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

In the Matter of IP-Enabled Services	))))	WC Docket No. 04-36

COMMENTS OF
THE UNITED STATES DEPARTMENT OF JUSTICE

Laura H. Parsky
Deputy Assistant Attorney General
Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 2213
Washington, D.C. 20530
(202) 616-3928

Patrick W. Kelley
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
U.S. Department of Justice
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.,
Room 7427
Washington, D.C. 20535
(202) 324-8067

Michael L. Ciminelli
Deputy Chief Counsel
Office of Chief Counsel
Drug Enforcement Administration
U.S. Department of Justice
Washington, D.C. 20537
(202) 307-8020

TABLE OF CONTENTS

SUMMARY

In the IP NPRM, the Commission recognizes the importance of ensuring that law enforcement's surveillance requirements are fully addressed, including that CALEA can and should apply to voice over Internet protocol ("VoIP") and Internet protocol ("IP")-enabled service providers. Furthermore, the Commission stated that the IP NPRM would not prejudice the outcome of the Commission's separate CALEA rulemaking proceeding and that it would closely coordinate its efforts between these two dockets.

DOJ appreciates the Commission's recognition of the importance of CALEA and its applicability to VoIP and IP-enabled services. As the Commission proceeds with its categorization of IP-enabled services to determine whether a particular regulatory requirement is needed to further critical national policy goals, DOJ urges that, for purposes of CALEA, the Commission take into account the following points:

- DOJ has no position on whether IP-enabled services need to be subject to economic regulation. DOJ agrees with the Commission that fencing off IP-enabled services from economic regulation does not require fencing them off from regulations intended to address important public safety and other public policy concerns.

- The Commission should be mindful not to adopt a classification scheme that would inhibit the ability of law enforcement to conduct court-ordered surveillance of communications via IP-enabled services.

- In order not to undermine the Commission's ability to classify an IP-enabled service provider as a "telecommunications carrier" in the CALEA rulemaking proceeding, the Commission should distinguish its ruling with respect to pulver.com from other VoIP services that do provide transmission and switching.

- DOJ believes that forbearance, waivers, and rule modifications are appropriate mechanisms for reducing burdens on IP-enabled service providers that the Commission deems unnecessary or inappropriate.

In addition, as the Commission evaluates the specific regulatory mandates it may choose to apply to IP-enabled services, the Commission should keep in mind that prior experience has demonstrated that relying on mere voluntary compliance -- for a statutory mandate such as CALEA -- is inadequate for ensuring implementation of and compliance with CALEA.

The Commission has also requested comments on whether providers of VoIP or other IP-enabled services should have the same obligations to protect customer proprietary network information ("CPNI") as other telecommunications carriers. DOJ has the same concerns regarding CPNI for IP-enabled services as it has previously stated to the Commission with respect to traditional telecommunications services -- *i.e.*, law enforcement must have speedy and secure access to such CPNI, and providers should protect CPNI from inappropriate disclosure.

Finally, as the Commission has recognized, the Section 214 authorization process provides an opportunity for Executive Branch agencies to review applications for, *inter alia*, law enforcement and national security concerns. The law enforcement and national security concerns are often the same whether a carrier provides traditional telecommunications service or IP-enabled service. The ability of a service provider to damage law enforcement and national security interests is created by its control over access to the communications, not by the protocol it employs.

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

In the Matter of IP-Enabled Services	))))	WC Docket No. 04-36

COMMENTS OF
THE UNITED STATES DEPARTMENT OF JUSTICE

I. Introduction

The United States Department of Justice ("DOJ")[1] hereby submits comments on the Commission's notice of proposed rulemaking released in the above-captioned docket (hereinafter the "IP NPRM").[2] In the IP NPRM, the Commission seeks to "examine issues relating to services and applications making use of Internet Protocol (IP), including but not limited to voice over IP (VoIP) services (collectively, 'IP-enabled services')" and requests comment on "how [the Commission] might distinguish among

---

[1] In past Commission proceedings, certain DOJ filings have been captioned as joint filings of the United States Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Administration. This and future filings, however, will be captioned in only the name of the Department of Justice, which, of course, includes all of its constituent components. This change is a matter of style only, and no substantive inference should be drawn from it.

[2] *In re IP-Enabled Services*, WC Docket No. 04-36, Notice of Proposed Rulemaking, 19 FCC Rcd 4863 (rel. March 10, 2004).

such services, and on whether any regulatory treatment would be appropriate for any class of services."[3]

DOJ (including the FBI and the DEA) recently filed a petition for rulemaking that asks the Commission to determine which services, including IP-enabled services, and entities are subject to the Communications Assistance for Law Enforcement Act ("CALEA").[4] Many of the subjects and questions raised by the Commission in the IP NPRM have the potential to impact CALEA implementation in the CALEA rulemaking proceeding. Therefore, DOJ submits these comments on the IP NPRM to assist the Commission's development of rules for IP-enabled services, particularly to the extent such rules may impact CALEA's applicability to IP-enabled services.

II. The Commission's Actions in the IP NPRM Proceeding Should Be Consistent With and Not Prejudice the Outcome of the CALEA Rulemaking Proceeding

The Commission has recognized the importance of the CALEA rulemaking proceeding in the IP NPRM and the "importance of ensuring that law enforcement's requirements are fully addressed."[5] Furthermore, the Commission stated that the IP NPRM "does not prejudice the outcome of our proceeding on CALEA, and we will

---

[3] IP NPRM at ¶¶ 1, 2.

[4] *In the Matter of United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act*, RM No. 10865 (filed Mar. 10, 2004) (hereinafter "CALEA Rulemaking Petition").

[5] IP NPRM at ¶ 50 n.158.

closely coordinate our efforts in these two dockets."[6] Chairman Powell's statement that "CALEA requirements can and should apply to VoIP and other IP enabled service providers, even if these services are 'information services' for purposes of the Communications Act" further demonstrates the Commission's commitment to ensure that federal, state, and local law enforcement have the ability to lawfully surveil criminals' communications when they utilize IP-enabled services.[7]

DOJ appreciates the Commission's recognition of the importance of CALEA and its applicability to VoIP and IP-enabled services. As the Commission considers whether, as to IP-enabled services, "a particular regulatory requirement is needed to further critical national policy goals,"[8] we urge that, for purposes of CALEA, the Commission take into account several points:

---

[6] *Id*.

[7] *See* Statement of Chairman Michael Powell on the IP NPRM. Other Commissioners also recognized the importance of preserving the ability of law enforcement to conduct surveillance of communications. Commissioner Abernathy stated that "we will need to find solutions to guarantee . . . the ability of law enforcement agencies to conduct surveillance." Statement of Commissioner Kathleen Abernathy on the IP NPRM. Commissioner Martin stated that "we need to carefully consider and address any questions and concerns regarding the obligations to provide traditional public safety services such as . . . the ability to comply with law enforcement requirements." Statement of Commissioner Kevin Martin on the IP NPRM. Commissioner Adelstein stated that "we must also understand how IP-enabled services will affect . . . the ability of our law enforcement officials to rely on CALEA to protect public safety and national security . . . ." Statement of Commissioner Jonathan Adelstein on the IP NPRM.

[8] IP NPRM at ¶ 35.

First, DOJ has no position on whether IP-enabled services need to be subject to economic regulation.[9] Moreover, we agree with the Commission that fencing off IP-enabled services from economic regulation does not require fencing them off from regulations raising important "public safety" and "other public policy concerns."[10] In fact, if the Commission decides to minimize economic regulation on IP-enabled services, it may find that the remaining public safety obligations, including law enforcement access under CALEA "for authorized wiretapping purposes,"[11] are entirely manageable.

Second, the IP NPRM clearly provides that issues of CALEA coverage are distinct and reserved for the CALEA rulemaking proceeding.[12] Nonetheless, as the Commission proceeds to categorize specific types of IP-enabled services, it should be mindful not to adopt a classification scheme that could inhibit the ability of law enforcement to conduct court-ordered surveillance of communications occurring via IP-enabled services.

Third, in order not to undermine the Commission's ability to classify an IP-enabled service provider as a "telecommunications carrier" in the CALEA rulemaking proceeding, the Commission should not adopt an overly narrow approach to

---

9 *Id.* at ¶ 5.

10 *Id*.

11 *Id*.

12 *Id.* at ¶ 50 n.158.

determining whether a service is engaged in "transmission or switching." A finding that an IP-enabled service does not involve "transmission or switching" would have serious consequences for the application of CALEA to such service. Such a finding could also improperly prejudice the CALEA rulemaking proceeding.[13]

In this context it is also important to note that the case of pulver.com, where the Commission found that the service did not involve transmission or switching, is distinguishable from other categories of broadband IP telephony service providers. Unlike some other IP telephony service providers, pulver.com has no managed network, does not connect to public telecommunications networks, offers limited service features, does not intend to offer carrier-grade quality of service, is limited to only a small number of members who have downloaded the software, and is offered for free to the public.[14]

In contrast, other broadband IP telephony service providers, including cable operators, local exchange carriers ("LECs"), competitive LECs, interexchange carriers, and VoIP providers offering telephony over broadband Internet access, such as Vonage, do engage in "transmission or switching of wire or electronic communications"; operate, manage, lease, or control facilities and networks to help ensure quality of service;[15]

---

[13] *Id.*

[14] pulver.com Declaratory Ruling at ¶¶ 4-6.

[15] In the IP NPRM, the Commission discussed IP telephony service providers that do not own extensive facilities, or any facilities at all, to provide their IP telephony service. IP NPRM at ¶ 15. If the Commission were to apply a narrower "ownership of

connect to public networks to allow for the termination of users' calls; offer their services to the public for a fee; and have larger established customer bases. These other broadband IP telephony providers are clearly distinguishable from pulver.com and should be CALEA-compliant.

Fourth, the Commission has asked, if the default regulatory framework associated with the legal classification accorded to a given service is inappropriate, whether the Commission should use its forbearance authority to modify that framework.[16] As DOJ stated in the CALEA Rulemaking Petition, the Commission has ample authority under the Communications Act of 1934, as amended (the "Communications Act") to forbear from, waive, or modify its rules, and to forbear from applying provisions of the Communications Act to telecommunications carriers.[17] Forbearance is an appropriate mechanism for eliminating regulations on IP-enabled services that the Commission deems unnecessary or inappropriate. After conducting a

---

facilities test," it would create a major loophole that is inconsistent with current Commission regulation of non-facilities-based wireless and wireline carriers. In determining whether an IP telephony provider is providing telecommunications services for purposes of CALEA, the proper question for the Commission to consider is not whether such provider "owns" facilities, *per se*, but whether it owns, leases, manages or otherwise controls facilities used to provide the IP telephony services. *See, e.g.*, *Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets*, Report and Order and Further Notice of Proposed Rulemaking, 18 FCC Rcd 24,817 (2003) (lessees of CMRS spectrum rights are subject to Title III where they have management control over another wireless carrier's facilities).

16 IP NPRM at ¶ 49.

17 *See* CALEA Joint Petition at 26 n.49, 32 n.58; IP NPRM at ¶ 49.

forbearance analysis with respect to IP-enabled services, the Commission could effectively impose only a small number of especially important and competitively neutral mandates that it determines would not pose undue burdens or hinder the deployment of IP-enabled services.

III. The Commission Should Not Rely on Title I to Apply the Mandates Required by CALEA

The Commission should not rely on Title I to apply the mandates required by CALEA. If the Commission utilizes its ancillary jurisdiction under Title I to apply mandates required by CALEA, such action could be challenged in court and result in delays and prolonged regulatory uncertainty, which is not in the interest of industry or of law enforcement. The Commission is correct that Congress generally has not imposed any specific Title II requirements under the Communications Act on information services.[18] That is because Congress followed the Commission's lead in the *Computer I, II, and III* decisions[19] and excluded information services from common carrier regulation under Title II. However, where the Commission has applied regulations to "information services" using its Title I ancillary authority,[20] it has done so in a very limited way.

---

[18] IP NPRM at ¶¶ 25-27.

[19] *See* 47 U.S.C. § 230(b)(2); IP NPRM at ¶ 25 n.82 (citing to *Computer I, II, and III* decisions).

[20] IP NPRM at ¶ 27 n.95.

In the face of the Congressional mandates of CALEA, requiring full and effective regulation, the Commission should not rely on Title I and instead should use its authorized powers under Section 229 of the Communications Act.[21] Section 229 of the Communications Act authorizes the Commission to "prescribe such rules as are necessary to implement the requirements of the Communications Assistance for Law Enforcement Act."[22]

IV. In Categorizing IP-Enabled Services, the Commission Should Not Prejudice the CALEA Rulemaking Proceeding

In the IP NPRM, the Commission solicits comment regarding "how, if at all, we should differentiate among various IP-enabled services to ensure that any regulations applied to such services are limited to those cases in which they are appropriate."[23]

Consistent with the Commission's commitment in the IP NPRM to closely coordinate its efforts in the IP-Enabled Services proceeding and the CALEA rulemaking proceeding,[24] it is important that whatever classifications the Commission adopts in this proceeding not preclude the Commission from making the findings necessary to conclude that CALEA applies to the services described in the CALEA Rulemaking

---

[21] 47 U.S.C. § 229. Section 229 of the Communications Act authorizes the Commission to "prescribe such rules as are necessary to implement the requirements of the Communications Assistance for Law Enforcement Act." *Id*.

[22] 47 U.S.C. § 229(a).

[23] IP NPRM at ¶ 35.

[24] *See id.* at ¶ 50 n.158.

Petition. The Commission has signaled its intent to further "critical national policy goals" by creating requirements that are "tailored as narrowly as possible."[25]

The Commission should be mindful of CALEA's broad scope[26] and the applicability of CALEA's public safety mandate to IP-enabled services as it classifies the different categories of such services. In addition, DOJ recommends that the Commission revisit the categories often enough to stay current with changing technologies as they emerge and evolve.

V. Appropriate Legal and Regulatory Framework for IP-Enabled Services

A. The Commission Should Ensure that Any Statutory Classifications Applied to IP-Enabled Services Are Consistent with Other Statutory Mandates

The Commission has requested comment on the appropriate statutory classification for the IP-enabled services identified by commenters in response to Section III of the IP NPRM.[27] The classification issues with respect to CALEA's applicability to broadband telephony and broadband access service are specifically

---

[25] *Id*. at ¶ 35. The Commission recognized the concern that the IP NPRM "does not prejudice the outcome of our proceeding on CALEA." *Id*. at ¶ 50 n.158.

[26] *In The Matter of Communications Assistance for Law Enforcement Act,* Notice of Proposed Rulemaking, 13 FCC Rcd 3149, 3161 ¶ 17 (1997) ("We conclude that Congress intended the obligations of CALEA to have broad applicability, subject only to the limitations in scope explicitly contained in the statute."); *In The Matter of Communications Assistance for Law Enforcement Act*, Second Report and Order, 15 FCC Rcd 7105, 7109 ¶ 7 (1999) (hereinafter the "CALEA Second Report and Order").

[27] *See id.* at ¶ 43.

reserved to the CALEA proceeding;[28] therefore, DOJ does not comment on the appropriate statutory classification for the IP-enabled services identified in this proceeding for purposes of their classification under the Communications Act -- other than to repeat the caution that the Commission be mindful not to create any classifications in this proceeding that would have the effect of undermining either the CALEA proceeding or CALEA's applicability to such services in general.

The Commission has also asked for comment on whether new and evolving technologies and services raise the possibility that a single IP-enabled communication might comprise both an "information service" and a "telecommunications service" component.[29] A dual-classification situation may already currently exist -- *e.g.*, for broadband Internet access services -- or will in the future exist for other IP-enabled services.

Accordingly, DOJ asks the Commission to make clear in this proceeding or the CALEA rulemaking proceeding that where an IP-enabled service contains both a telecommunications service and an information service component, the IP-enabled service provider is subject to CALEA with respect to, at a minimum, the telecommunications service component. A finding that the telecommunications service component of the service is subject to CALEA is consistent with the Commission's *CALEA Second Report and Order*, in which the Commission concluded that "[w]here

---

[28] CALEA Rulemaking Petition at Section II.C.

[29] IP NPRM at ¶ 43.

facilities are used to provide both telecommunications and information services, . . . such joint-use facilities are subject to CALEA in order to ensure the ability to surveil the telecommunications services."[30]

B. The Commission Has Authority to Update Prior Interpretations of Statutory Terms

The Commission has asked about the extent to which its previous interpretations of statutory terms are suitable to proper classification of IP-enabled services.[31] In connection with that request, the Commission has asked whether there are legal constraints on the Commission's authority to revise its prior interpretations.[32]

We believe that, within the confines of the Administrative Procedures Act, the Commission has the authority to revisit and revise the regulatory interpretations to reflect changes in existing services and to account for the introduction of new services into the marketplace. The Commission can use this authority to revisit its prior interpretations of various statutory terms -- including those discussed in the Stevens

---

30 CALEA Second Report and Order at ¶ 27.

31 IP NPRM at ¶ 44.

32 *Id*.

Report[33] -- many of which are outdated and unsuitable to properly classify IP-enabled services.[34]

C. Specific Regulatory Requirements and Benefits

1. Public Safety

The Commission should continue to recognize that the public interest includes public safety, law enforcement, and national security.[35] These interests must not be subordinated to business and economic interests. In fact, in considering business and economic interests, the Commission should recognize that advancing the interests of public safety, law enforcement, and national security makes for a more secure and stable business environment — the very type of environment that fosters creative innovation and a competitive market economy.

---

[33] *In the Matter of Federal-State Joint Board on Universal Service*, Report to Congress, 13 FCC Rcd 11,501 (1998) (hereinafter the "Stevens Report").

[34] For example, the DOJ believes the Commission should no longer apply the term "enhanced services" to any service that employs computer processing, because virtually all of the telecommunications systems of today employ such processing. Future telecommunications systems will likewise employ such processing.

[35] *See, e.g.*, *In the Matter of General Motors Corporation and Hughes Electronics Corporation, Transferors, and the News Corporation Limited, Transferee, for Authority to Transfer Control*, Memorandum Opinion and Order, 19 FCC Rcd 473, 492-93 ¶¶ 35-37, 628 ¶ 374 (2004); *1998 Biennial Regulatory Review -- Review of International Common Carrier Regulations*, Report and Order, 14 FCC Rcd 4909, 4915 ¶ 15 (1999); *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*, Report and Order and Order on Reconsideration, 12 FCC Rcd 23,891, 23,918 ¶ 59 (1997); *Market Entry and Regulation of Foreign-Affiliated Entities*, Report and Order, 11 FCC Rcd 3873, 3897 ¶ 62 (1995).

The Commission would be justified in considering the consequences to these interests of a decision classifying IP-enabled services as telecommunications services, information services, or otherwise. However, in the case of CALEA, the question of whether CALEA's requirements should apply is defined by the CALEA statute itself, which establishes a simple rule: If an entity is a telecommunications carrier as defined in Section 102(8) thereof,[36] then it is legally obligated to meet CALEA's assistance-capability requirements under Section 103,[37] unless it establishes pursuant to Section 109(b)[38] that compliance is not reasonably achievable. Economic burdens and alleged adverse impacts on market innovation may be taken into account only to the extent that CALEA itself so provides. While Section 109(b) permits those considerations to be taken into account in the context of "determinations of reasonably achievable," nothing in CALEA permits the Commission to rely on them when it is determining the general scope and applicability of CALEA to classes of market participants. Scope and applicability of CALEA are determined solely by reference to CALEA's unique definition of "telecommunications carrier," which is inclusive of and broader than the definition in the Communications Act.

The IP NPRM also asked whether voluntary agreements entered into by providers of IP-enabled services might serve the purpose of regulation in the context of

---

[36] 47 U.S.C. § 1001(8).

[37] 47 U.S.C. § 1002.

[38] 47 U.S.C. § 1008(b).

the legacy circuit-switched network.[39] CALEA is a statutory mandate. Thus, to the extent that CALEA applies to a given service, there is no issue of voluntary compliance. Neither the Commission nor industry has the authority to replace the mandatory compliance mechanisms specified in the statute with a scheme of voluntary agreements. Voluntary compliance was never considered adequate for accomplishing the statutorily mandated CALEA implementation and compliance for circuit-mode networks, and there is likewise no justification for deeming voluntary compliance with CALEA to be adequate for IP networks.[40] As to public safety mandates that the Commission finds are not applicable to particular services, the Commission should consider imposing requirements under some other authority -- at least in cases where consumers are unlikely to choose one service or provider over another on the basis of its voluntary adoption of public safety measures. In such cases, market forces are unlikely to address the lack of voluntary adoption of such measures.

---

[39] IP NPRM at ¶¶ 48, 56.

[40] As a clear recognition that voluntary compliance can be inadequate even where appropriately applied, the Commission recently proposed to make wireless network outage reporting mandatory after discovering the failings of voluntary reporting. *In re New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, ET Docket No. 04-35, Notice of Proposed Rule Making, 19 FCC Rcd 3373 (rel. February 23, 2004).

2. Effect of Title III of the Communications Act

The IP NPRM asks what effect Title III and, in particular, Section 332 may have on IP-enabled services offered over a wireless platform.[41] To the extent that a carrier offers an interconnected mobile service to the public for profit, it is engaged in providing a commercial mobile radio service ("CMRS"), regardless of whether it offers IP-enabled services. Further, pursuant to Section 102(8)(B)(i) of CALEA, any CMRS provider is subject to CALEA obligations, therefore, the Commission should consider the impact on CALEA of any decision not to classify an IP-enabled service offered over a wireless platform as CMRS.

If a CMRS carrier upgrades its wireless network to offer VoIP, it continues to meet the definition of a CMRS carrier because it still offers an interconnected service to the public for a profit.[42] Accordingly, the carrier would remain subject to all the same regulatory mandates of Titles II and III of the Communications Act and would hence remain covered by CALEA as a "person or party engaged in providing commercial mobile radio service."[43]

---

41 IP NPRM at ¶¶ 68, 69.

42 47 U.S.C. § 332(d).

43 47 U.S.C. § 1001(8)(B)(i). The Commission should confirm that CMRS-based Internet access service also meets the definition of CMRS and therefore remains subject to Titles II and III of the Communications Act, as well as CALEA. Indeed, the Commission has not even opened a rulemaking to reclassify CMRS-based Internet access service as an information service, as it has done with Internet access services offered over other communications platforms.

If the same CMRS carrier were to leverage its network upgrade to provide some other IP-enabled service, the carrier should similarly be required to bring the service into compliance with CALEA, as long as such IP-enabled service is part of the CMRS service offering and not exempt from CALEA as an "electronic messaging service."[44] In fact, the Commission has already ruled that one non-VoIP IP-enabled service, namely digital dispatch ("push-to-talk") service, was covered by CALEA because it was offered "in conjunction with" the rest of the carrier's CMRS service.[45]

Further, any conclusion in this proceeding about the regulatory status of non-CMRS wireless IP-enabled services should be closely coordinated with the outcome of the pending CALEA rulemaking proceeding, where the Commission will address the issue of CALEA applicability in more detail.[46]

Finally, certain wireless entities not currently classified as CMRS may offer IP-enabled services. One example would be WiFi-based VoIP. Although these service providers may currently have no obligations under Titles II or III, they may still be subject to CALEA based on CALEA's unique definition of "telecommunications carrier."

---

[44] *See* 47 U.S.C. § 1001(4).

[45] CALEA Second Report and Order at ¶ 21.

[46] *See* CALEA Rulemaking Petition at Section II.C.

VI. Other Regulatory Requirements

A. Law Enforcement and National Security Concerns Regarding Improper Handling of Sensitive and Personal Customer Proprietary Network Information Are the Same for Providers of IP-Enabled Services to the Public as for Traditional Telecommunications Carriers

The Commission has also requested comments on whether providers of VoIP or other IP-enabled services should have the same obligations to protect CPNI as other telecommunications carriers.[47] The concerns DOJ has expressed with regard to CPNI concerning traditional telecommunications services are equally pertinent to sensitive and personal network information associated with IP-enabled services offered to the public.[48] For each type of service, law enforcement must have speedy and secure access to such records. At the same time, inappropriate disclosure of such information can be a boon to criminals, terrorists and spies. Thus, the appropriate handling of CPNI, whether associated with traditional telecommunications services or with new methods of communicating, is vital to preserving the privacy of subscribers, to effectively enforcing United States law, and to preventing damage to United States national security.

---

47 IP NPRM at ¶ 71.

48 *See* Reply Comments of the United States Department of Justice and the Federal Bureau of Investigation, In the matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Docket No. CC-96-115, at 2; *see also* Comments of the Federal Bureau of Investigation in the matter of 1998 Biennial Regulatory Review of International Common Carrier Regulations, IB Docket 98-118. DOJ hereby incorporates the comments referenced above herein.

Congress has recognized that the personal and highly sensitive nature of CPNI requires that providers protect it from inappropriate disclosure.[49] As the Commission itself has noted, "Congress recognized . . . that the new competitive market forces and technology ushered in by the 1996 Act had the potential to threaten consumer privacy interests. Congress, therefore, enacted Section 222 to prevent consumer privacy protections from being inadvertently swept away along with the prior limits on competition."[50] This statutorily mandated protection is necessary because CPNI:

> consists of highly personal information, particularly relating to call destination, including the numbers subscribers call and from which they receive calls, as well as when and how frequently subscribers make their calls. This data can be translated into subscriber profiles containing information about the identities and whereabouts of subscribers' friends and relatives; which businesses subscribers patronize; when subscribers are likely to be home and/or awake; product and service preferences; . . . and subscribers' social, medical, business, client, sales, organizational, and political telephone contacts.[51]

DOJ has observed in other proceedings before the Commission that, in addition to the potential to harm individuals' privacy, inappropriate handling of CPNI can harm

---

49 *See* 47 U.S.C. § 222.

50 *In the Matter of the Implementation of the 1996 Act*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 ("Second CPNI Report") at ¶ 1.

51 Second CPNI Report at ¶ 61.

law enforcement and national security interests as well.[52] As described in DOJ's previous comments concerning CPNI, speedy and secure access to CPNI by law enforcement pursuant to lawful authority is critical to all kinds of criminal investigations and intelligence operations. At the same time, improper access to CPNI can be extremely useful to the adversaries of law enforcement. To provide just one example of the serious consequences that can flow from improper access to CPNI, DOJ is aware of instances where information from a common carrier outside of the United States was used by an international drug cartel to murder individuals whom the information suggested were cooperating with law enforcement.[53]

The concerns discussed above result from access to the communications data, regardless of how such communications are transmitted. Thus, the same set of concerns that DOJ has expressed with regard to CPNI handled by traditional telecommunications carriers apply to CPNI associated with IP-enabled services provided to the public. Just like traditional telecommunications carriers, many IP-enabled service providers have

---

[52] *See* Reply Comments of the United States Department of Justice and the Federal Bureau of Investigation, In the matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket 96-115, at 2 (filed Nov. 19, 2002); *see also* Comments of the Federal Bureau of Investigation in the matter of 1998 Biennial Regulatory Review of International Common Carrier Regulations, IB Docket 98-118 (filed Aug. 28, 1998).

[53] *See* Letter of May 24, 1995 from Louis J. Freeh, Director of the Federal Bureau of Investigation to the Honorable John D. Dingell, U.S. House of Representatives (attached to the Comments of the Federal Bureau of Investigation in the matter of 1998 Biennial Regulatory Review of International Common Carrier Regulations, IB Docket 98-118).

access to highly personal information about their customers' communications, including, *inter alia,* when, how often, and with whom a customer communicates. As explained above, such information must be available to United States law enforcement and not available to those who seek to cause harm.

B. Carriers Who Provide International IP-Enabled Services Present Many of the Same Law Enforcement and National Security Concerns as Traditional International Telecommunications Carriers

The Commission has also asked "whether the growing use of IP-enabled services presents any foreign policy or trade issues."[54] In particular, the Commission has noted that common carriers must obtain Section 214 authorization before commencing international service, and that this process provides an opportunity for Executive Branch agencies to review applications for, *inter alia*, law enforcement and national security concerns.[55] As with many other public safety regulations, the law enforcement and national security issues with which DOJ is concerned when a carrier seeks to provide international communications service are often the same whether a carrier provides traditional telecommunications service or IP-enabled service.

The Commission currently provides notice of Section 214 applications to Executive Branch agencies prior to allowing any entity to provide international

---

54 IP NPRM at ¶ 76.

55 *Id.* at n. 225.

telecommunications services.[56] This notice requirement serves the important function of allowing appropriate Executive Branch agencies, with responsibility for such areas as national security, law enforcement, foreign policy, and trade policy, to consider whether a particular application implicates any of these interests before service has commenced. In recognition of each agency's primacy in its area of responsibility, where an Executive Branch agency raises a concern within its area of expertise, "the Commission defers to Executive Branch agencies on national security, law enforcement, foreign policy, and trade policy concerns raised in an application."[57]

As the FBI explained in its comments filed in the 1998 Biennial Regulatory Review of International Common Carrier Regulations, IB Docket No. 98-118, there are numerous ways in which an international communications provider could harm United States law enforcement and national security. To reiterate just a few of the possible harms described more fully in the comments and the letters attached thereto, an international communications provider hostile to United States law enforcement or national security could frustrate or compromise lawful electronic surveillance, could learn and disclose law enforcement targets and technical capabilities, and could perform unlawful interceptions without detection. In other words, the company could provide criminals, terrorists and spies a wiretap-free line, could tip off targets of

---

[56] *See* 47 U.S.C. § 214(b) (requiring notice to the Secretaries of Defense and State); *see also* 2002 *IB Biennial Regulatory Review Staff Report*, 18 FCC Rcd at 4237-38, ¶ 22 (listing other Executive Branch agencies the Commission notifies).

[57] See *2002 IB Biennial Regulatory Review Staff Report*, 18 FCC Rcd at 4237-38, ¶ 22.

investigations, could learn what United States law enforcement can and cannot do, and could access United States commercial and state secrets virtually without detection. As recently as this month, DOJ and the Department of Homeland Security again stressed the vital importance of Section 214 review when it filed comments opposing new exceptions to the authorization requirement.[58]

The Commission has repeatedly recognized that the serious risks to law enforcement and national security presented by international communication service providers require Commission action. In proceedings where DOJ has noted such concerns, the Commission has conditioned approval of Section 214 applications on compliance with network-security agreements negotiated between DOJ and the applicants.[59]

The ability of an international communications provider to damage law enforcement and national security interests is created by the provider's control over access to the communications, not by the particular protocol the provider employs to provide the communications capability. Thus, many of the same concerns apply regardless of whether or not the communications service being provided is enabled by the Internet protocol. An IP-enabled service provider receiving a lawful electronic

---

[58] *See* Comments of the Departments of Justice and Homeland Security, In the matter of Amendment of Parts 1 and 63 of the Commission's Rules, IB Docket No. 04-47 (filed May 6, 2004).

[59] *See e.g.*, *Global Crossing Ltd. and GC Acquisition Limited*, Memorandum Opinion, Order and Authorization, 18 FCC Rcd 20,301 (2003); *Bell Atlantic New Zealand Holdings, Inc. and Pacific Telecom, Inc.*, Order and Authorization, 18 FCC Rcd 23,140 (2003).

surveillance order could disclose the existence of an investigation to a target just as easily as a traditional telecommunications carrier could compromise such an operation. Likewise, an IP-enabled service provider could monitor private communications just as freely as a traditional telecommunications service provider, and communications could contain anything from details of government business to commercially valuable trade secrets. So long as the provider has control over the communications conduits vital to the conduct of both government business and private commerce, it has the power to damage not only personal privacy and the U.S. economy, but law enforcement and national security as well.

VII. Conclusion

While DOJ recognizes that issues of CALEA applicability are distinct and reserved for the separate CALEA Rulemaking Petition, we urge that the Commission consider implications of actions in this proceeding to its ability to effect its stated goal that CALEA apply expansively -- *i.e.*, to VoIP and other IP-enabled services. We appreciate the Commission's recognition and support for law enforcement's important mandate to maintain public safety.

Respectfully submitted,

THE UNITED STATES DEPARTMENT OF JUSTICE

/s/ Laura Parsky

Laura H. Parsky
Deputy Assistant Attorney General
Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 2113
Washington, D.C. 20530
(202) 616-3928

and

/s/ Patrick Kelley

Patrick W. Kelley
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
U.S. Department of Justice
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.
Room 7427
Washington, D.C. 20535
(202) 324-8067

and

/s/ Michael L. Ciminelli

Michael L. Ciminelli
Deputy Chief Counsel
Office of Chief Counsel
Drug Enforcement Administration
U.S. Department of Justice
Washington, D.C. 20537
(202) 307-8020

Dated: May 28, 2004