DOCKET FILE COPY ORIGINAL

STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL
120 BROADWAY, NEW YORK, NEW YORK 10271

ELIOT SPITZER
Attorney General

RECEIVED & INSPECTED
APR 15 2004
FCC - MAILROOM

DIVISION OF PUBLIC ADVOCACY

SUSANNA M. ZWERLING
Bureau Chief
Bureau of Telecommunications and Energy

KEITH H. GORDON
Assistant Attorney General
E-mail Keith Gordonon@OAG State NY US
Vox (212) 416-8320
Fax (212) 416-8877

April 12, 2004

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street S.W. Suite TW-A325
Washington, D.C. 20554

Re: RM-10865 - In the Matter of United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Agency Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act.

Dear Ms. Dortch:

Pursuant to the Commission's March 12, 2004 Notice (DA No. 04-700), please find enclosed the Comments of New York State Attorney General Eliot Spitzer. Enclosed with this letter are the original executed brief and affidavit of John Christopher Prather (Exhibit A) which were e-filed in unsigned form.

Sincerely,

Keith H. Gordon
Assistant Attorney General

Enclosure: Comments of NYS Attorney General and Exhibits

cc: Natek, Inc.
9300 East Hampton Drive
Capitol Heights, MD 20743

No. of Copies rec'd 0
List ABCDE

RECEIVED & INSPECTED
APR 15 2004
FCC - MAILROOM

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

In the Matter of	)	
	)	
United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Agency	)	
	)	RM-10865
Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act.	)	

Comments of Eliot Spitzer
Attorney General of the State of New York

Terryl Brown Clemons
Acting Deputy Attorney General
Public Advocacy Division

Susanna M. Zwerling
Assistant Attorney General in Charge
Telecommunications and Energy Bureau

Keith H. Gordon
Assistant Attorney General
of counsel

Peter B. Pope
Deputy Attorney General
Criminal Division

Carrie H. Cohen
Assistant Attorney General in Charge
Public Integrity Unit

New York State Attorney General's Office
120 Broadway
New York, NY 10271
(212) 416-6343, Fax (212) 416-8877
keith.gordon@oag.state.ny.us

April 12, 2004

TABLE OF CONTENTS

SUMMARY 1

BACKGROUND 2

INTEREST OF THE ATTORNEY GENERAL OF THE STATE OF NEW YORK 6

ARGUMENT 8

I. Ambiguous CALEA Requirements Lead To Carrier Delay, Confusion and Resistance, And Thereby Impair Law Enforcement. 8

A. Law Enforcement Requires Immediate Carrier Compliance With Court-Approved Intercepts 8

B. Regulatory Gridlock Results in Industry Confusion and Impairs Law Enforcement. 9

1. The FCC's inconclusive CALEA rulings cause industry confusion . 9
2. Criminals are currently exploiting regulatory delay 10

II. Congress Authorized the FCC to Identify Services Subject to CALEA and, to Protect Vital Public Interest, the FCC Expeditiously Should So Act 11

A. CALEA History 11

B. Applicability of CALEA Does Not Need to be Determined by a Service's Classification as an Information Service or Telecommunications Service Under the 1996 Act 12

C. The Commission Should Expedite its Decision on the Joint Petition Independent of Other Pending Proceedings 15

D. The Commission Should Apply CALEA to Broadband Technologies 16

1. Subject VoIP and other broadband services to CALEA 16
2. Subject multimedia messaging services to CALEA 17
3. Subject push-to-talk services to CALEA 18

III. The FCC Should Adopt And Enforce Deadlines For Compliance. 18

IV. The FCC Should Regulate Which Costs Carriers May Impose On Law Enforcement. 19

A. Many Carriers' Intercept Fees Are Unreasonable 20

B. Procedures Are Needed to Resolve Carrier Intercept Provisioning Fee Disputes 23

CONCLUSION 24

Exhibit A:

AFFIDAVIT OF J. CHRISTOPHER PRATHER sworn to April 12, 2004

SUMMARY

The Office of New York State Attorney General Eliot Spitzer ("NY OAG") hereby submits these comments pursuant to the Federal Communications Commission's ("FCC" or "Commission") request for comments on the Joint Petition for Expedited Rulemaking submitted by the United States Department of Justice ("DOJ"), Federal Bureau of Investigations ("FBI") and Drug Enforcement Agency ("DEA") (collectively "Joint Petitioners"), dated March 10, 2004 ("Joint Petition").[1]

The FCC has not yet determined whether packet-mode or Internet protocol ("IP") services are subject to the provisions of the Communications Assistance to Law Enforcement Act ("CALEA") These services permit wireless carriers to offer the general public wireless phones with features such as Push-to-Talk, and multimedia messaging services such as picture messaging and video messaging, as well as future offerings of new, enhanced features.[2] Due to regulatory uncertainty, certain packet mode or internet protocol ("IP") services cannot be wiretapped by law enforcement agencies pursuant to a valid warrant.[3] As Joint Petitioners have written, "the ability of federal, state and local law enforcement to carry out critical electronic surveillance *is being*

---

[1] *See also* New York Criminal Procedure Law Article 700; Prather Aff. ¶ 5.

[2] *See e g.* PR Newswire Apr. 12, 2004, Monday ("Last spring, Cingular announced the New England launch of its next generation network using Global System for Mobile (GSM) technology for voice, and General Packet Radio Service (GPRS) for high-speed wireless data. More than 921 million people in 200 countries use this technology, which delivers a superior network...instant messaging and picture messaging.")

[3] Public Law 103-414, 108 Stat. 4279 (1994), 47 U.S.C. § 1001 As Joint Petitioners state, "implementation of CALEA for packet mode technologies has been largely unsuccessful." *See Joint Petition* at 34. Many carriers roll out new services with minimal if any interception capabilities." *Id* at 8. Indeed.most carriers "have not implemented their own carrier-specific CALEA-compliant solutions." They state they "do not have a CALEA solution available." Thus "extensions have become the rule rather than the exception for packet-mode compliance." *Id* at 35-38.

compromised today . . . ."[4]

There can be no more delay. The FCC must rule promptly so that these new services are accessible to law enforcement on the same basis as analog telephones. In a post-September 11 world, the commercial interests of telecommunications carriers can no longer trump law enforcement's use of court-authorized intercepts to protect the public.

BACKGROUND

Court-authorized intercepts of telephone communications have been, and continue to be, an essential investigative tool used by State and Federal law enforcement. New York State law enforcement, especially the NY OAG's Statewide Organized Crime Task Force ("OCTF") use such intercepts to solve major crimes and obtain convictions of organized crime leaders and member of international drug cartels.[5]

With passage of the Omnibus Crime Control and Safe Streets Act of 1968 ("Crime Control Act") and its subsequent amendment in 1970, Congress recognized the need for telecommunications carriers to provide law enforcement with technical and other assistance so that court-authorized intercepts could be effected.[6] Title III of the Crime Control Act specifies a finite number of serious crimes for which law enforcement can eavesdrop on telephone conversations and then sets strict standards and procedures that law enforcement must follow in order to obtain court authorization

---

[4] *Joint Petition* at 8 (emphasis in original).

[5] Exhibit A, Affidavit of John Christopher Prather, sworn to April 12, 2004 ("Prather Aff.") ¶ 11.

[6] 18 U.S.C 2510 *et seq.* In 1986, Congress amended the Crime Control Act to include electronic communications such as e-mail, data transmissions, faxes, cellular telephones, and pagers. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §2701, *et seq.*

for a wiretap.

By the early 1990's, technological and competitive changes in the telecommunications industry were beginning to cause serious problems for law enforcement: the new digital voice and data networks could not be tapped using the technology of the analog era. Solely because of technological changes, court-ordered wiretap warrants were being reduced to useless pieces of paper. In 1994, the FBI reported to the Congress that at least 183 eavesdropping investigations had been impaired because of such factors as lack of access to wireless carriers' systems, inability to obtain switch-based features used by subscribers of wireline carriers (such as call forwarding, call waiting, voice dialing, and speed dialing), and inaccessible voice mail.[7]

In response to these and other policy concerns, in 1994, Congress enacted CALEA.[8] When Congress drafted CALEA in 1994, it was deeply concerned about the 1993 terrorist bombing of the World Trade Center that killed six victims and demonstrated the ability of foreign terrorists to bring their violent attacks to America's doorstep.[9] Today, in the aftermath of the 9/11 terrorist attacks, the risk of terrorism is more acute than ever. As the nation engages in a global war against terror, federal, state and local public safety agencies are working to detect, identify, prevent and capture those who threaten America's safety. Interception of wire and electronic communications is an

---

[7] *CALEA Legislative History*, H.R. Rep. No. 103-827(I), 1994 U.S.C.C.A.N. 3489, 3495.

[8] *Id.* at 3489.

[9] Senator Patrick Leahy, CALEA's sponsor, stated that the bill was needed because, "We have recently experienced the terrorist bombing of the World Trade Center, the exposure of a foreign spy within the upper echelons of our intelligence agency, and the incessant reports of violent crime in virtually every town, city and rural area in the country." *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services,* Senate Joint Judiciary/Technology and Law and Civil and Constitutional Rights Police Access to Advanced Communications Systems, 103rd Cong., 1994.

essential tool in this effort.

Law enforcement's national security and public safety concerns are not merely theoretical. When Congress drafted CALEA, FBI witnesses testified:

> the nation's telecommunications networks are routinely used in the commission of serious criminal activities. Terrorists, violent criminals, organized crime groups, and drug trafficking organizations . . . rely heavily upon telecommunications to plan and execute their criminal activities and hide their illegal profits.[10]

In the decade after CALEA's passage, the results have been mixed at best. Compliance has improved in some areas such as wireline and wireless phone service. While some individual carriers have demonstrated their commitment to cooperate with law enforcement's efforts against erosion of its capabilities, this hardly has been universal. Far too often, the steps taken by carriers have been piecemeal, inconsistent, and incomplete.

While the FCC initiated a number of proceedings to implement CALEA,[11] tentative and inconclusive findings have left ambiguities concerning which packet-mode and IP services are subject to CALEA. Segments of the industry continue to maintain that CALEA does not apply to new service offerings, especially those employing packet-mode technologies and IP. Under CALEA, Congress directed the FCC to determine which technologies and services would be subject to CALEA and to enforce its provisions. The regulation of these services has been the subject of

---

[10] Before the House Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, 103rd Cong., May 3, 1994 (statement of James F. Kallstrom, Special Agent in Charge of the Special Operations Division, New York Field Division of the FBI).

[11] *See* CC Docket No. 97-213 - *In the Matter of Communications Assistance for Law Enforcement Act, Notice of Proposed Rulemaking,* released Oct. 10, 1997, 13 FCC Rcd 3149; *Further Notice of Proposed Rulemaking*, released Nov. 5, 1998, 13 FCC Rcd 22632 (1998); *Report and Order*, released Mar. 15, 1999, 14 FCC Rcd 4151 (1999), *Second Report and Order*, released Aug. 31, 1999, 15 FCC Rcd 7105 (1999); and *Third Report and Order*, released Aug. 31, 1999, 14 FCC Rcd 16794 (1999).

lengthy, and as yet unresolved, proceedings by the FCC. As Joint Petitioners point out, during this regulatory delay telecommunications carriers have introduced new services freely to the marketplace without the CALEA technology, increasingly crippling law enforcement and endangering the public.[12]

A decade after CALEA's passage, terrorists' continuing reliance on modern telecommunications recently was demonstrated by the March 11, 2004 use of cell phones to trigger bombs on Spanish commuter trains.[13] According to public reports, the terrorists' use of a prepaid cell phonecard and government wiretap recordings of wireless phone calls were key sources of evidence used by Spanish authorities to identify and arrest those charged with plotting and carrying out these heinous terrorist acts.[14]

The FCC has both the authority and duty under CALEA to ensure compliance by all providers. The FCC must, without further delay, resolve the CALEA issues that have been pending since 1997. The FCC should declare that packet-mode and other IP services, including Voice over Internet Protocol[15] ("VoIP") services, Push-to-Talk ("PTT"), and multimedia messaging services

---

[12] *Joint Petition* at 21-22.

[13] Indeed, wireless phones have become a standard method for terrorists to remotely detonate bombs, according to police investigations in Paris, Bali, Jakarta, and Saudi Arabia, as well as Madrid. *Newsday* (New York), *Cellphones Jury-Rigged To Detonate Bombs*, Mar. 15, 2004.

[14] According to news reports, a cell phone and prepaid phone card found on a Madrid train with an unexploded bomb was linked to one of the suspects who was arrested. *Toronto Star* (Canada), *Spain Knew Suspects' Terror Ties*, Mar. 17, 2004.

[15] There are a number of versions of VoIP services. Some transmit voice calls from one computer using broadband Internet access to another such computer, bypassing entirely the traditional public switched telephone network ("PSTN"). Other VoIP services combine the Internet with the PSTN to transmit calls. In a separate NPRM, the FCC has requested public comment on rules that would classify VoIP pursuant to the 1996 Act and thereby determine a host of regulatory issues other than CALEA coverage. WC Docket No. 04-36, *In the Matter of IP-*

such as picture messaging and video messaging, must become CALEA compliant now. Finally, the FCC should punish firmly and quickly any carriers that fail to comply.

Law enforcement is not seeking by the Joint Petition to broaden its powers to intrude on individuals' privacy rights. The type of telephone service available is rapidly changing in form and content due to technological advances. Messages are transmitted over alternate networks or enhanced with features such as pictures. Therefore, the FCC must enforce CALEA to realize the statute's goal: to keep law enforcement from slipping backward by dint of technological change. Too much is at stake for continued indecision.

Finally, too many carriers appear to be treating CALEA as a profit center by imposing unreasonably high fees to effect intercepts. The FCC thus should regulate the charges that carriers may bill law enforcement in provisioning intercepts.

INTEREST OF THE ATTORNEY GENERAL OF THE STATE OF NEW YORK

As the home of one of the world's most important financial sectors, as well as the victim of two terrorist attacks on the World Trade Center in 1993 and 2001, New York is a major focus of state and federal law enforcement anti-terrorism activity. In addition, New York long has been a key center for the investigation, interruption, and prosecution of narcotics trafficking and other major organized crime activities. These efforts account for roughly 30% of all wiretaps conducted nationally.[16]

Enabled Services, released Mar. 10, 2004 (initial and reply comments are due May 28 and June 28, 2004 respectively); 69 FR 16193, Mar. 29, 2004. The NPRM on VoIP notes the Joint Petition and states that the FCC will "closely coordinate" its efforts on the CALEA and VoIP dockets. *Id.* ¶ 50 n.158.

[16] *2002 Wiretap Report* at Table 2; Exhibit A, Prather Aff. ¶ 3.

The NY OAG is the chief law enforcement officer for the State of New York. As such, the NY OAG falls within the definition of "government" as set forth in CALEA.[17] A core mission of the NY OAG is investigating sophisticated criminal enterprises, cases that often rely on court-authorized intercepts. A major bureau within the NY OAG's criminal division is the Statewide Organized Crime Task Force ("OCTF") which investigates and prosecutes multi-county, multi-state, and multi-national organized criminal activities occurring within New York State.[18] The NY OAG's facilities, particularly OCTF's wiretap plants, routinely are used to assist other state, local, and federal law enforcement agencies.[19]

Further, the NY OAG represents New York State's interest in numerous federal and state court trials and regulatory proceedings, including many FCC dockets.

---

[17] *See* 47 U.S.C. § 1001(5)

[18] *See* N.Y. Exec. Law § 70-a. OCTF works closely with local, state and federal law enforcement agencies to investigate and prosecute organized criminal activities such as loan sharking, gambling rings, narcotic trafficking, racketeering, and money laundering. OCTF's investigations of traditional organized crime are too numerous to catalogue, however, the most notable have included electronic surveillance of associates of the Colombo and Gambino crime families. Prather Aff. ¶9. OCTF is a leading partner in narcotics task forces throughout New York, providing legal, investigative and technical expertise. Sheriff's offices, district attorneys, and municipal police officers from different counties participate in these task forces. *Id.* ¶3. A cooperative effort between the State Police and OCTF on the Cali Cartel Project, which ran from 1986 to 2003, is undoubtedly the paragon of interagency partnerships in New York State, having resulted in the arrest of nearly 450 major narcotics trafficker and the seizure of more than eleven tons of cocaine and over $60 million in cash. In addition to OCTF, the NY OAG's Criminal Prosecutions Bureau is responsible for the investigation and prosecutions of criminal actions within the jurisdiction of the Attorney General. The NY OAG's Medicaid Fraud Control Unit investigates and prosecutes health care crime in New York State. The NY OAG's Public Integrity Unit handles complex investigations into government corruption, fraud and abuse of authority. Among other statutes, the Public Integrity Unit enforces the "Tweed Law." N.Y. Exec. Law § 63-c. As New York State's chief legal officer, the NYOAG represents the New York State Police and other state agencies.

[19] Exhibit A, Prather Aff. ¶ 3.

ARGUMENT

I. Ambiguous CALEA Requirements Lead To Carrier Delay, Confusion and Resistance, And Thereby Impair Law Enforcement.

A. Law Enforcement Requires Immediate Carrier Compliance With Court-Approved Intercepts.

Court-ordered wiretaps need to be implemented as quickly as possible. Investigations of terrorist cells, narcotics dealers, kidnappers, racketeers, and other such dangerous criminals are extremely time sensitive, and delays in provisioning a wiretap can cause loss of lives as well as frustrate efforts to locate and apprehend fugitives or suspects before they escape jurisdictional reach.

Timeliness is critical not only for investigatory reasons, but for legal reasons as well. Legally, the court order granting an application for a wiretap sets strict time limits for carrying out the intercept, usually thirty days or less. Once thirty days have passed, an application for an extension for an additional period of up to thirty days must be presented to and granted by a judge based on a finding that the surveillance is still needed and justified. Accordingly, a request to extend a warrant must describe the results of the initial intercept "or provide a reasonable explanation of the failure to obtain such results," and such extensions are limited to a maximum of thirty days.[20] If weeks pass between approval of a wiretap and installation by a carrier, the resulting loss of surveillance might prevent law enforcement from making the showing necessary to justify an extension.

[20] New York Criminal Procedure Law § 700.40.

B. Regulatory Gridlock Results in Industry Confusion and Impairs Law Enforcement.

1. The FCC's inconclusive CALEA rulings cause industry confusion.

In Section 102 of CALEA, Congress specified which entities and services are required to comply with the statute's intercept capability requirements and authorized the Commission to implement the statutory definitions.[21] In the decade after CALEA was enacted, the Commission has undertaken numerous administrative proceedings intended to implement the Act. The FCC has not, however, settled a number of vital issues. Among them is whether CALEA applies to packet-mode technology. This issue has been the subject of proceedings pending before the FCC since 1997.[22]

As the Joint Petition demonstrates, such delay has allowed telecommunications firms to deploy untappable technology with impunity. The Commission must rule promptly.

One example of the confusion this regulatory uncertainty has caused is seen in wireless PTT services. PTT services are offered by some wireless carriers to enable customers to speak directly with other PTT users in a fashion similar to a walkie-talkie. The question of whether Nextel's PTT service -- not offered through packet mode technology -- is subject to CALEA's compliance requirements has been settled since 1999. Then the Commission decided:

> ... [P]ush-to-talk "dispatch" service is subject to CALEA to the extent it is offered in conjunction with interconnected service, because in such case it is a switched service functionally equivalent to a combination of speed dialing and conference calling, but

[21] 47 U S.C. §§1001(6) and (8) *et seq.*

[22] *Notice of Proposed Rule Making,* On Administrative Implementation of CALEA, FCC 97-356 (1997). Most recently, on November 19, 2003, the Commission extended, until January 30, 2004, the preliminary extension previously granted to wireline and wireless carriers who filed for extensions of packet-mode surveillance capability requirements. Public Notice - DA-03-3722, Nov., 2003. http://hraunfoss.fcc.gov./edocs_ public/attachmatch/DA-03-3722A1.pdf. More than two months past the January 30, 2003 deadline, no Order has been adopted or released.

otherwise not.[23]

Nextel's compelled compliance with CALEA has had no effect on carriers using packet-mode technology to offer PTT service.[24] In essence, they have argued that, because they are offering the same service through a different technology, they need not comply. It is far past time for the Commission to come to closure on this issue.

2. Criminals are currently exploiting regulatory delay

The growing CALEA compliance gap provides terrorists and criminals with the means to conduct their conspiracies free of monitoring by law enforcement agencies. Recently, FBI supervisory agent Richard Thompson described this danger, "[t]hose that would do our nation harm will migrate to the new technology if they have any idea or any regard that these cannot be surveilled."[25]

This prediction has already been fulfilled. OCTF head Deputy Attorney General J. Christopher Prather described how, "criminal organizations, to avoid interception, purposefully conducted criminal conversations over what was then an untappable Point to Point feature."[26] Yet firms continue to roll out untappable functions. Anyone today easily can obtain wiretap-proof

---

[23] *Second Report and Order* ¶ 21.

[24] As discussed elsewhere herein, the NY OAG asserts that the FCC's PTT decision is based on the function of the service, not the technology employed to deliver it. Therefore, packet-mode wireless PTT should be required to comply with CALEA.

[25] Statement of FBI supervisory special agent Richard Thompson to the Voice on the Net Conference held Mar. 30, 2004 in Santa Clara, CA.

[26] Exhibit A, Prather Aff. ¶ 14.

phones and thereby exploit the gaps in law enforcement's ability to effect intercepts with impunity.[27]

II. Congress Authorized the FCC to Identify Services Subject to CALEA and, to Protect Vital Public Interest, the FCC Expeditiously Should So Act

A. CALEA History

Upon finding in 1994 that technological advances were preventing law enforcement agencies from lawfully intercepting communications of terrorists and members of organized crime, Congress passed CALEA. The statute was intended:

> to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced techniques such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services.[28]

CALEA established a four-year transition period during which carriers were to retrofit existing services to permit law enforcement to carry out authorized intercepts, and Congress gave carriers a half-billion dollars to do so.[29] Thereafter, the communications industry was required to ensure that new services were CALEA compliant, while law enforcement agencies were made responsible for the capacity costs of implementing intercepts. In addition, CALEA delegated to the FCC authority to establish rules to implement the statute, in consultation with law enforcement, including resolution of disputes over industry-based standard-setting bodies that were to draft compliance specifications that serve as safe harbors for manufacturers and carriers. Importantly, the

---

[27] Exhibit A, Prather Aff., ¶ 15.

[28] *CALEA Legislative History, supra* at 3489.

[29] CALEA built upon the statutory body of law established under Title III of the Crime Control Act and the Electronic Communications Protection Act.

FCC was authorized to determine which new technologies and services would be subject to CALEA's requirements.[30]

In general, CALEA succeeded in getting carriers to make many pre-1994 services accessible, such as conference calling, call forwarding, and analog wireless voice services. CALEA has failed, however, to make the various new telecommunications technologies accessible to law enforcement.

B. Applicability of CALEA Does Not Need to be Determined by a Service's Classification as an Information Service or Telecommunications Service Under the 1996 Act.

Part of the regulatory delay is attributable to arguments being advanced by some in the industry that conflate CALEA's definitions with those in the 1996 Telecommunications Act ("1996 Act").[31] In separate dockets, the Commission has been considering whether cable modem services,[32] wireline-based broadband services[33] and VoIP[34] ("broadband technologies") are "telecommunications services" or "information services." The 1996 Act determinations will have, among other things, profound impacts on fees and thus are the subject of much contention.

The simple answer for the purposes of the Joint Petition is that the 1996 Act and CALEA

---

[30] *See* § 102(8) of CALEA, 47 U.S.C. § 1001(8).

[31] 47 U.S.C. § 251, *et seq*

[32] *See In the Matter of Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities,* Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd 3019 (2002), *reversed in part and remanded, Brand X v FCC,* 345 F.3d 1120 (9th Cir. 2003), *rehearing en banc denied* __ F. 3rd__, (9th Cir. April 1, 2004).

[33] CC Docket 02-33 - *In the Matter of Appropriate Framework for Broadband Access to the Internet Over Wireling Facilities, et al*

[34] *See, e g*, WC Docket No. 03-45 - *In the Matter of Petition for Declaratory Ruling that pulver com's Free World Dialup is neither Telecommunications Nor a Telecommunications Service, Memorandum Opinion and Order*, released Feb. 19, 2004.

have different goals and, more importantly, different definitions. Thus, it would be entirely proper to find that a service is a telecommunications service under CALEA but not under the 1996 Act. The CALEA language should be applied to effect its goal: to prevent law enforcement from losing ground. Thus, the Commission was correct when it previously "conclude[d] as a matter of law that the entities and services subject to CALEA must be based on the CALEA definition . . . independently of their classification for the separate purposes of the Communications Act."[35]

Indeed, CALEA defines "telecommunications carrier" more broadly than the corresponding term contained in the 1996 Act. For CALEA purposes, a "telecommunications carrier" includes both an entity engaged in "the transmission or switching of wire or electronic communications as a common carrier for hire"[36] and an entity providing transmission service "to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such person or entity to be a telecommunications carrier for purposes of this subchapter."[37]

CALEA's use of both "wire or electronic communications" in the foregoing definitions goes beyond traditional voice telephony, and explicitly includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system."[38] Thus, wireless technologies that

---

[35] *Second Report and Order* ¶ 13.

[36] 47 U.S.C. § 1001(8)(A).

[37] *Id.* at § 1001(8)(B)(ii).

[38] Section § 1001(1) of CALEA incorporates the definition of "electronic communication" in 18 U.S.C. § 2510(12).

provide video messaging and picture messaging are subject to CALEA, regardless of how they might be classified for the very different purposes of the 1996 Act.

While the 1996 Act's use of the terms "telecommunications service" and "information service" are mutually exclusive, this is not so with CALEA. CALEA provides that a "telecommunications carrier" is relieved of its CALEA obligations only "insofar as they are engaged in providing information services."[39] Therefore, as the Commission already ruled, where "facilities are used to provide both telecommunications and information services . . . such joint-use facilities are subject to CALEA."[40] Accordingly, even if a telecommunications carrier combines wireless voice service with video messaging or picture messaging, and, assuming *arguendo* that these two latter features are determined to be "information services," such joint-use offerings must comply with CALEA.

In addition, CALEA's inclusion of the term "switching" is not limited to only circuit-mode switching. Instead, consistent with the broad intent of Congress to anticipate new technologies that may be used by law enforcement targets to plan criminal activities,[41] CALEA's general use of "switching" should be interpreted to include packet-mode switching as well.

Finally, CALEA authorizes the Commission to subject carriers to CALEA's requirements if they: (1) are "engaged in transmission or switching;" (2) are substitutes for "a substantial portion" of

---

[39] 47 U.S.C. § 1001(8)(C)(i).

[40] *Second Report and Order* ¶ 27.

[41] CALEA "requires telecommunications carriers to ensure that new technologies and services do not hinder law enforcement access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance." *CALEA Legislative History*, *supra* at 3496.

the public switched telephone network; and (3) if it is "in the public interest" to do so.[42] Packet-mode services, including VoIP telephony, clearly involve transmission or switching and are rapidly replacing traditional public switched telephone network ("PSTN") traffic, thus requiring CALEA compliance to preserve the public's interest in safety from terrorist and criminal activity.

C. The Commission Should Expedite its Decision on the Joint Petition Independent of Other Pending Proceedings

The NY OAG recognizes the seriousness of the debate over the interpretation and implementation of the 1996 Act. As significant as these proceedings are, however, the Commission should not hold off addressing the relief sought in the Joint Petition until those other items are settled.

The expedited resolution of the instant CALEA issues should be the Commission's highest priority. The motivating purpose of CALEA was to close the gaps in law enforcement's wiretap ability that result from advances in telecommunications technology. Despite the passage of ten years, the Commission has not resolved critical questions involving the scope of CALEA, and new communications technologies remain inaccessible to law enforcement. As Joint Petitioners have said, "the importance and urgency of this task cannot be overstated."[43]

---

[42] 47 U.S.C. § 1001(B)(ii).

[43] *See Joint Petition* at 8.

D. The Commission Should Apply CALEA To Broadband Technologies.

1. Subject VoIP and other broadband services to CALEA.

The NY OAG supports the Joint Petitioners' request for a Declaratory Ruling and final rules that clarify that CALEA applies to broadband technologies, including those that employ VoIP and other packet-mode technology.[44] In a recently released Notice of Proposed Rulemaking ("NPRM"),[45] the Commission recognized that VoIP is widely recognized as rapidly replacing substantial portions of the traditional circuit-mode switched industry.[46]

In adopting CALEA, Congress clearly intended that communications transmitted over the Internet are subject to CALEA:

> While the bill does not require reengineering of the Internet, nor does it impose prospectively functional requirements on the Internet, this does not mean that communications carried over the Internet are immune from interception or that the Internet offers a safe haven for illegal activity. Communications carried over the Internet are subject to interception under Title III [of the Crime Control Act] just like other electronic communications. That issue was settled in 986 with the Electronic Communications Privacy Act. [CALEA] recognizes, however, that law enforcement will most likely intercept communications over the Internet at the same place it intercepts other electronic communications: at the carrier that provides access to the public switched network.[47]

Where a target's phone calls have been subjected to court-authorized interception, the target's choice of an "Internet phone" service in place of a circuit-switched phone service should not

---

[44] *Id* at 15-33.

[45] WC Docket 04-36 - *In the Matter of IP-Enabled Services, Notice of Proposed Rulemaking*, FCC 04-28, released Mar. 10, 2004.

[46] *Id.* at ¶ 3.

[47] *CALEA Legislative History, supra* at 3503-04.

determine whether law enforcement can monitor the call. While Congress in 1994 could not have anticipated specific Internet-based communications applications, or the most effective means for facilitating an intercept for each of the multiple variations on VoIP that since have emerged,[48] this does not make such calls an "information service" instead of a "telecommunications service" for purposes of CALEA. This sort of technology change is precisely the sort of development that Congress intended to be addressed by CALEA.

The public interest is not only consistent with such action, but demands the Commission so act before even greater migration of telephony onto VoIP networks prevents law enforcement from intercepting all but those calls that remain on the circuit-mode switched network.

2. Subject multimedia messaging services to CALEA.

Wireless telecommunications that include multimedia messaging services should be declared subject to CALEA because they provide both telecommunications and information services. The Commission's prior declaration that "such joint-use facilities are subject to CALEA" should, consequently, govern here as well.[49] Therefore, multimedia messaging services are part of

---

[48] Thus far, there are several distinct forms of VoIP telephony that have been brought to market. At one end of the spectrum is Pulver.com's Free World Dialup, which is exclusively useable by end users who communicate via personal computers having broadband (either cable modem or wireline DSL) access. Such calls travel entirely over the Internet and never intersect with the public switched telephone network ("PSTN"). Carriers like Vonage, can communicate either between two broadband computer-enabled end users as above, or connect a broadband subscriber with customers of the PSTN by transferring the call from the Internet via a gateway provided by a CLEC (and converting from IP format to analog or digital multiplex format). Still another variation of VoIP is used by Cablevision, which transmits its Digital Voice subscribers' calls using IP format over a coaxial broadband network and then hands the call off to a CLEC (affiliate Lightpath) for transmission over the PSTN with non-IP format. At the opposite end of this VoIP spectrum are carriers like USA DataNet, which require their customers to dial an access phone number over the PSTN, and then transfer the call to IP format for transmission via the Internet, only to be reconverted at the other end for delivery over the PSTN.

[49] *CALEA Second Report and Order* ¶ 27.

the sort of joint-use facilities that fall under the purview of the statute.

3. Subject push-to-talk services to CALEA.

In response to Nextel's attempt to exempt its PTT "Direct-Connect" dispatch service, the Commission found in 1999 that such services offered in conjunction with its interconnected wireless service are subject to CALEA.[50] Identical services offered by other firms over packet-mode network should be treated identically for the purposes of CALEA.

III. The FCC Should Adopt And Enforce Deadlines For Compliance.

The NY OAG strongly endorses concrete deadlines for compliance by carriers offering both existing packet-mode technologies and future technologies that are covered by CALEA. Far too much time has been allowed to pass.

Given the competitive nature of the telecommunications industry and the industry's unsatisfactory record during the ten years since passage of CALEA, the NY OAG is pessimistic about the willingness of carriers to "voluntarily" take the high road. Too many carriers, fearing that they will be at a competitive disadvantage should they take steps to meet their CALEA obligations while others do not, will delay making the requisite investments. A decade of experience has demonstrated that there is no viable alternative but for the FCC to establish firm and extremely short deadlines for CALEA compliance.

The Commission thus should establish rules that provide for enforcement actions where necessary. There is no acceptable alternative in light of the industry's track record of delays in establishing compliance standards for existing and new technologies, failures to cooperate with law

---

[50] *Id* ¶ 21

enforcement, and foot-dragging in deploying technology needed to assist law enforcement with court authorized intercepts. A regulatory stalemate and business-as-usual industry placement of profits before public interest cannot continue.[51] The stakes simply are too high.

IV. The FCC Should Regulate Which Costs Carriers May Impose On Law Enforcement.

Congress established a compensation scheme in CALEA with three categories. For "equipment, facilities and services deployed before January 1, 1995" $500 million was appropriated to the U.S. Attorney General "to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed ... to establish the capabilities necessary to comply with Section 1002 of [Title 47, U.S.C.]."[52] Congress' distinction between "compliance capability" expenses as opposed to provisioning expenses (for purposes of pre-CALEA upgrades reimbursement) forms the foundation for CALEA's treatment of compliance investment costs for subsequent services.

For post-1995 facilities and services, section 109(b) of CALEA places the cost of implementing CALEA compliance on the carrier, except where the Commission makes a determination that compliance is not "reasonably achievable" because "compliance would impose significant difficulty or expense on the carrier or on the users of the service."[53] Congress listed

---

[51] While some policies may be best left to market forces, there is no basis for assuming that competition will bring about carriers' CALEA compliance. Most customers are unlikely to prefer those carriers that are CALEA compliant, and some who are engaged in criminal activity would have reason to seek out carriers that do not make law enforcement interception feasible. Indeed, the past decade of industry resistance to CALEA compliance during the blossoming of telecommunications competition in numerous markets indicates that regulation, not competition, is required to ensure law enforcement access to new services

[52] 47 U.S.C. § 1008(a).

[53] *Id* at § 1008(b)(1).

eleven factors in making such determinations of reasonable achievability, the first of which is "the effect on public safety and national security."[54] Congress intended that "industry will bear the cost of ensuring that new equipment and services meet the legislated requirements."[55]

Congress prescribed that only where the Commission finds that such services are not reasonably achievable, would a carrier have a basis under CALEA to apply to the U.S. Attorney General for funds to meet these obligations, and such grants are "subject to the availability of appropriations."[56] However, the Commission has not issued any "not reasonably achievable" findings under section 109(b),[57] so all carriers found subject to CALEA must comply if they do not obtain a § 109(b) exemption.

A. Many Carriers' Intercept Fees Are Unreasonable.

In 1999, the Commission anticipated that the wireless carriers would pay approximately $159 million and the wireline carriers would pay approximately $117 million to implement CALEA compliance with four of the FBI "punch-list" items.[58] These figures illustrate the scale of CALEA compliance costs. Recovery of all carriers' CALEA compliance capital costs through individual

---

[54] *Id* at § 1008(b)(1)(A). The other factors to be considered include, *inter alia*, the effect on rates for basic residential telephone service, protection of privacy for communications not authorized to be intercepted, the policy to encourage provision of new technologies and services, carriers' financial resources, and competition impacts

[55] *CALEA Legislative History*, *supra* at 3496.

[56] If no funds were awarded by the U.S. Attorney General, the carrier would be deemed in compliance without making the modifications to achieve CALEA capability. 47 U.S.C. §§ 1008(b)(2)(A) and (B).

[57] CALEA requires the Commission to issue its determination within one year of the filing of any carrier's § 109(b) petition. 47 U.S.C. § 1008(b)(1).

[58] CC Docket No. 97-213 - *In the matter of Communications Assistance for Law Enforcement Act, Third Report and Order*, 14 FCC Rcd. 16,794, Appendix B at n.2, released Aug. 31, 1999.

wiretap provisioning fees, therefore, could result in charges as great as $10,000 to $50,000 per intercept (depending on the amortization period applied) as there are approximately 1,500 court authorized intercepts annually.[59] Such a cost recovery scheme would make intercepts prohibitively expensive for virtually all law enforcement agencies, and result in depriving law enforcement of an essential crime fighting and anti-terror tool. There is no basis for concluding that Congress intended this result. Instead, CALEA was passed so as to restore law enforcement's access to court-authorized intercepts, not to price intercepts out of the realm of practicality.

The Crime Control Act authorizes carrier compensation for the costs incident to each wiretap order:

> Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant **for reasonable expenses incurred** in providing such facilities or assistance.[60]

The plain meaning of this statute limits carriers' provisioning fees to the reasonable expenses incurred in responding to individual wiretap warrants presented by law enforcement, not the costs of achieving capability as prescribed by CALEA. If Congress intended that carriers recover their CALEA compliance implementation costs through individual fees collected from law enforcement when wiretap warrants are executed, then the provisions of CALEA Section 109 discussed above would have no meaning.

Despite the clear statutory language, it is apparent that many carriers are charging the NY

---

[59] *2002 Wiretap Report* at Table 2.

[60] 18 U.S.C. § 2518(4)(emphasis added).

OAG and other law enforcement agencies far more than their "reasonable expenses incurred in providing facilities and assistance" to effect authorized intercepts. As fully set forth in the Affidavit of J.Christopher Prather, the fees many carriers charge the NY OAG are related neither to expenses incurred in provisioning a wiretap nor reasonable.[61] Wireless carriers charge from $1,500 to $4,400 to set up an intercept, plus between $250 and $2,200 monthly to maintain it.[62] The reasonable wireless carrier expenses incurred to execute a warrant are not significantly more than the same carriers' normal fees to provide basic wireless services to business customers (ranging from $135 to $400 monthly),[63] and probably much less (since the intercept is effected with a few keystrokes at a computer terminal).[64] In general, wireline carriers (including ILECs and CLECs) charge the NY OAG much less for installing an intercept than do wireless carriers, and the charges are for the most part comparable to the fees charged for installation and maintenance of single line business telephone service.[65]

The foregoing examples demonstrate that the fees many carriers' charge to the NY OAG for

---

[61] *See* Exhibit A ¶¶ 16-22.

[62] *Id.* ¶ 18.

[63] For example, AT&T Wireless charges $299 per month for 3000 local/long distance minutes to small business customers. http://www.attwireless.com/business/plans/overview.jhtml. At Sprint PCS, a similar small business plan with 2,500 minutes (plus unlimited minutes to other PCS phones or during off-peak hours) costs $135 per month http://www.sprint.com/pcsbusiness/plans/voice/free_clear.html. Nextel charges $100 for 2,000 minutes (plus unlimited off-peak usage). Cingular charges $250 for 4,500 monthly anytime minutes (plus 5,000 off-peak minutes). Verizon Wireless offers 3,500 monthly minutes (plus unlimited off-peak minutes) for $200. http://www.verizonwireless.com/b2c/store/controller?item=planFirst&action=viewPlanDetail&sortOption=priceSort &catId=323. T-Mobile's 4,000 minutes per month (plus unlimited off-peak and mobile-to-mobile minutes) costs $200.

[64] Exhibit A, Prather Aff., ¶ 17.

[65] *Id.* ¶ 19.

provisioning intercepts exceed the carriers' reasonable expenses incurred in providing the intercept as permitted by 18 U.S.C. § 2518(4). It appears, moreover, that some carriers are attempting to collect from law enforcement the capital and other costs of meeting CALEA implementation capacity requirements and not just the incremental expenses of provisioning individual intercepts.

B. Procedures Are Needed to Resolve Carrier Intercept Provisioning Fee Disputes.

The NY OAG and other law enforcement agencies have experienced major increases in expenditures for intercept provision fees charged by some carriers. Such fees cost the NY OAG between $400,000 and $500,000 annually.[66] As burdensome as this expense is for New York State, other smaller-scale law enforcement agencies simply cannot afford to pay the fees many carriers are demanding, and instead must forego using wiretaps entirely.[67]

Prompt Commission action is necessary to delineate clear standards controlling what carrier costs may be included in intercept provisioning fees. The NY OAG and other law enforcement agency personnel are engaged in crucial investigations that protect the public from terrorist attacks, illegal weapons trafficking, kidnapping, drug smuggling, and organized crime. It is beyond their financial and temporal time resources to seek court review of every questionable carrier charge claimed by various carriers. The time taken up by such bill disputes would interfere with more critical public safety activities.

Competition is of no help in controlling carriers' provisioning fees billed to law enforcement. As the NY OAG is forced to use whatever carrier is being used by the target, law

---

[66] *Id.* ¶ 16.

[67] *Id.* ¶ 17

enforcement is unable to shop for the best intercept price charged by competing carriers. If subscribers ever considered such matters, their price signal would be a perverse incentive to choose the carrier with the highest intercept provisioning fees, since the charges are paid by law enforcement, not the subscriber.

The Commission, therefore, should exercise its authority under § 229(a) of the 1996 Act[68] and promulgate regulations that define those costs carriers may properly recover from law enforcement through provisioning fees, as well as require all other CALEA compliance expenses be collected from ratepayers generally.

CONCLUSION

The first ten years' experience with CALEA demonstrates that while it has succeeded in assisting law enforcement with access to some services provided by wireline and wireless carriers, substantial confusion remains regarding the statute's applicability. This lack of clarity and certainty has created large gaps in interception capability and contravenes Congress' intent in enacting CALEA and puts the public at great risk.

Too much is at stake for regulatory gridlock. The Commission must act now. It should assure that as new services are developed, carriers and manufacturers will deploy eavesdropping capability and that it will punish those who do not.

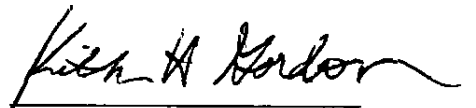
April 12, 2004

Respectfully submitted,

ELIOT SPITZER
Attorney General of the State of New York

[68] 47 U.S.C. § 229(a).

By:



Keith H. Gordon
Assistant Attorney General

Terryl Brown Clemons
Acting Deputy Attorney General
Public Advocacy Division

Susanna M. Zwerling
Assistant Attorney General in Charge
Telecommunications and Energy Bureau

Keith H. Gordon
Assistant Attorney General
of counsel

Peter B. Pope
Deputy Attorney General
Criminal Division

Carrie H. Cohen
Assistant Attorney General In Charge
Public Integrity Unit

New York State Attorney General's Office
120 Broadway
New York, NY 10271
(212) 416-6343
Fax (212) 416-8877
keith.gordon@oag.state.ny.us

Exhibit A

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

In the Matter of	)	
	)	RM-10865
United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Agency	)	AFFIDAVIT OF J. CHRISTOPHER PRATHER
Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act.	)	

STATE OF NEW YORK)
) ss.:
COUNTY OF NEW YORK)

J. Christopher Prather, being duly sworn, deposes and says:

1. I am an employee of the Office of the Attorney General of the State of New York ("OAG"), jointly appointed by New York's Attorney General and the Governor of New York to the position of Deputy Attorney General in Charge of the Statewide Organized Crime Task Force ("OCTF"). I have held this position since September 2002.[1] I am fully familiar with the facts stated herein.

[1]Prior to taking charge of OCTF, from March 1999 to September 2002, I served as Assistant Deputy Attorney General in the OAG's Criminal Division. Prior to my employment with the OAG, I was employed by the New York City School Construction Authority, Inspector General's Office, as First Assistant Inspector General and Counsel to the Inspector General. I began my career as a prosecutor for the Manhattan District Attorney's Office where I worked as a trial assistant to the Career Criminal Prosecutions Bureau, as Senior Investigative Counsel in the Rackets Bureau, and as Deputy Chief of the Frauds Bureau. Prior to moving to New York, I was employed by the North Carolina Attorney General's Office. I earned my juris doctorate from the University of North Carolina School of Law in 1977, and am admitted to practice in the States of New York and North Carolina.

The Organized Crime Task Force

2. OCTF was established in 1970 by the enactment of Section 70-a of the New York Executive Law. OCTF has broad powers to investigate organized criminal activity occurring in more than one county in New York State or occurring both within and outside of New York State.

3. OCTF has offices across the State of New and conducts long-term investigations into narcotics trafficking, gambling, money laundering, smuggling, labor racketeering, prostitution, grand larceny, official corruption, and fraud. OCTF provides assistance, as requested and whenever possible, to local district attorneys' offices, especially technical assistance with wiretaps. OCTF also provides assistance and intelligence to various federal law enforcement agencies with whom it works, including the United States Federal Bureau of Investigation ("FBI"), Drug Enforcement Agency, Secret Service, Department of Labor-Inspector General, Bureau of Alcohol, Tobacco and Firearms, and the U.S. Attorneys' offices. More than one-third of all court-approved wiretaps in the nation are done in New York.

4. The Deputy Attorney General in charge of OCTF, or one of his assistant deputies, may conduct investigative hearings, compel the production of documents and other evidence, apply for search warrants, and, with the consent of the Governor and the appropriate district attorney, appear before grand juries, conduct criminal and civil actions, and exercise the same powers as the local district attorney.

Court-Authorized Wiretaps Are Essential To OCTF

5. Article 700 of New York's Criminal Procedure Law governs court-authorized eavesdropping in New York by state and local prosecutors and complies with the Federal

eavesdropping standards set forth in Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq*. In Article 700, the State Legislature specifically enumerated the serious offenses, such as kidnapping and narcotics trafficking, for which an eavesdropping warrant may be authorized.

6. As the Deputy Attorney General in charge of OCTF, I am authorized by statute and the Attorney General to determine when it is necessary and appropriate to seek court authorization to use wiretaps and pen registers and to personally apply to the appropriate court for an eavesdropping warrant. Wiretap warrants are issued for thirty days, and a new application is required to obtain an extension warrant for each additional thirty days. If a carrier delays provisioning and thus prevents the interception of useful evidence in the initial warrant period, it can be very difficult to obtain an extension beyond the initial warrant period.

7. In the past two years, OCTF has secured court orders for pen registers and/or eavesdropping warrants on more than 440 instruments.

8. One hallmark of any organized group is the need of its members to communicate. This is true of organized criminal enterprises too, whether they be members of a Mafia family, a narcotics trafficking conspiracy, or a terrorist cell. Especially where a criminal organization has a hierarchical structure, the "street level" offenders too often are the only visible targets for law enforcement. In the narcotics model, for example, only those persons selling small amounts on street corners, within view of the police, are likely to be arrested. Through the use of court-authorized wiretaps, evidence can be gathered against the upper echelon of the organization and criminal responsibility properly can be affixed for all members of the enterprise.

9. OCTF has investigated numerous sophisticated criminal enterprises through the use of court-authorized wiretaps. The evidence obtained through such wiretaps has led to convictions in recent significant prosecutions of organized crime members. OCTF court-authorized wiretaps on wireless phones of Gambino organized crime family associates produced key evidence that led to the RICO conviction of Gambino boss Peter Gotti. *See U.S. v. Gotti*, No. 02-CR-606(FB) (EDNY). Similarly, OCTF taps on the wireless phones of the associates of Joel Cacace, the boss of the Colombo organized crime family, resulted in evidence that led to Cacace's indictment. *See U.S. v. Cacace*, No. 03-CR-191(SJ) (EDNY).

10. On the non-traditional organized crime front, court-authorized wiretaps have proven critical as well. For example, OCTF's wiretaps on land lines and wireless phones of individuals associated with the Cali drug cartel resulted in the conviction of more than 450 upper-level drug dealers and the seizure of more than eleven tons of cocaine and more than $60 million cash.

11. Since the events of September 11, 2001, OCTF has undertaken new types of investigations designed to combat terrorism. Accordingly, OCTF currently is using its wiretap capability and authority to investigate certain types of crimes that commonly are used to finance terrorist activities, including cigarette smuggling, cellular phone fraud, and narcotics money laundering.

Changes In Technology Are Thwarting OCTF

12. A decade ago, most pen register orders and eavesdropping warrants were executed on traditional "land line" telephones. To do this, the carrier identified the copper wire pair and pole location so that a law enforcement technician could attach a device to route call data and/or

conversations occurring over the target line to the eavesdropping "plant," where call data was collected. Monitoring officers then listened to and recorded the target's conversations. The transmission from pole to plant occurred over a "plain old telephone service" or "POTS" line, the bill for which was part of law enforcement's cost for the eavesdropping.

13. For electronic surveillance, the advent of wireless telephones and other mobile communication devices eliminates the wires and the telephone pole, and changes the job of the technician from "wire man" to computer specialist. Within minutes of receipt of the court order, warrants for the interception of wireless devices can be implemented by the communications carriers. With just a few computer key strokes, the connection is made directly between law enforcement's computerized listening stations and the telephone service provider's computerized switches. These connections occur over expensive, high-speed data lines, leased by OCTF.

14. As a result of the evolution from land lines to wireless phones, the OAG has spent more than $4 million in the past three years to upgrade its eavesdropping technology. Despite such investment, we continue to fall behind. Each of the major wireless carriers currently offers wireless communication services that cannot be tapped, and which can be purchased for only a few hundred dollars. This is not lost on the criminals. OCTF has encountered instances where criminals, to avoid interception, purposefully conducted criminal conversations over what was then an untappable Point to Point feature. Indeed, in one such case, a suspect told another that he had inside information about an impending law enforcement action and instructed his co-conspirator to disconnect the phone call and go point-to-point so he could securely share the specifics.

15. I have no doubt that technologically savvy culprits will continue to utilize the newest, untappable technologies in an effort to thwart electronic surveillance. These wiretap-proof phones and services are available to anyone with a modest amount of funds. Most troubling, in my estimation, is that the most technologically adept criminal groups (terrorists) are the ones for whom we most need to have viable eavesdropping capabilities.

Wireless Carriers Appear To Be Making Electronic Eavesdropping A Profit Center

16. Collectively, the phone companies charge OCTF between $400,000 and $500,000 annually for the cost of implementing interception court orders. This charge is over and above the monthly connection charges ($110 for in-state and $200 for out-of-state) for maintaining high speed data lines connecting the phone companies' facilities to OCTF's equipment.

17. In the past few years, the fees charged to law enforcement by telephone service providers for implementing lawful pen register and wiretap warrants have skyrocketed, to the point that many prosecutor's offices across New York State simply do not have the funds to pay for this crucial investigative tool. The increased costs associated with replacing POTS lines with leased, high speed data lines are only a small part of the overall increase. Over and above those line costs, each telephone service provider assesses its own "provisioning fees." These fees are needlessly excessive as only minimal effort is required on behalf of a wireless carrier to provision an intercept, which is achieved entirely through electronic coding.

18. Set forth below is a description of the provisioning fees charged to OCTF by the major carriers:

a. Nextel charges OCTF $1,500 per target number to set up an intercept, plus a $250 monthly service fee for the duration of the intercept. If the target subscribes to Nextel's PTT service (Direct Connect℠), an additional $1,500 setup fee plus $250 monthly service fee is

imposed;

b. Sprint PCS charges OCTF $250 per "market area" as a setup fee (New York is one market area), plus $25 per day. When OCTF questioned Sprint about the basis of its provisioning fee amount, the response given was that it was comparable to the fee charged by other carriers;

c. T-Mobile applies yet another formula. Connections to ten or more switches are typically needed to implement a pen register or wiretap warrant on a T-Mobile wireless phone. T-Mobile charges OCTF $250 per switch for each pen register and/or wiretap for the initial 30 days (up to a maximum of $2,500) for each target phone number, plus a $100 "bridging fee" per target phone number. Extensions are assessed a $50 per switch fee (up to a maximum of $500), plus the bridging fee, per target number. (Additionally, Voice mailbox "cloning" costs $150 for each 90-day period, per target number.) In practical terms, these fees equate to a charge of $2,600 per wireless phone tap for the initial 30 days, and $600 per wireless phone for each additional 30 day extension;

d. Cingular Wireless charges a flat $600 processing fee per target;

e. AT&T Wireless charges OCTF double for most intercepts. Separate New York criminal procedure statutes govern pen registers and wiretaps. Accordingly, OCTF typically must apply for simultaneous authorizations and the court issues a separate eavesdropping warrant and pen register order. Even though OCTF serves AT&T Wireless with both the warrant and order together and no extra effort required, AT&T Wireless insists on charging OCTF separate fees of $2,200 each for provisioning the pen register and the warrant, for a total of $4,400. If the pen register and wiretap were combined in a single court order, AT&T Wireless would charge a single fee. At one time, Nextel maintained a similar double billing policy, but changed it when questioned by OCTF, and acknowledged that there was no justification for billing additional amounts for wiretap warrants and pen register orders when they are served together; and

f. For each target line to be intercepted, Verizon Wireless charges OCTF a $50 "administrative fee" plus a $25 per switch set-up fee, in addition to a $800 per switch "service and maintenance" fee (or a $2,000 monthly service and maintenance fee for three or more switches). Monthly extensions for each intercept cost an amount similar to the initial setup, even though there is no significant effort or cost incurred by Verizon for not de-provisioning the intercept.

19. The intercept provisioning charges of wireline carriers are much less than for wireless carriers, and are comparable to fees such carriers charge for installation and maintenance of single line business service.

20. When challenged for what OCTF has come to view as exorbitant charges for implementing lawful pen register orders and eavesdropping warrants, the phone companies have proffered various justifications for their fees. One company at first claimed money was owed for time spent by its legal staff reviewing the warrant, and even went so far as to request that copies of the eavesdropping application and supporting affidavits, upon which the issuing judge found probable cause, be furnished to it for inspection and review. No such fee was required in the days of POTS lines and the orders and warrants are the same now as they were then. Moreover, applications and supporting affidavits are sealed as a matter of law and have never been available for telephone company review. When OCTF explained this, there was no diminution in the eavesdropping fee. Instead, the company claimed to OCTF that the fee schedule represented an amortization of its costs for CALEA compliant switches.

J. Christopher Prather

The foregoing affidavit was signed before me by J. Christopher Prather, known by me to be the person identified above, on this 12th day of April, 2004.

Keith H. Gordon
notary public

KEITH H. GORDON
Notary Public, State of New York
No. 4841690
Qualified in Westchester County
Commission Expires July 31, 2004