DOCKET FILE COPY ORIGINAL

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

RECEIVED

OCT 25 1999

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of:	CC Docket No. 97-213
Communications Assistance for Law Enforcement Act	

PETITION FOR RECONSIDERATION OF SECTION 105 REPORT AND ORDER

On March 15, 1999, the Commission released a Report and Order (SSI Order) implementing the systems security and integrity provisions contained in § 105 of the Communications Assistance for Law Enforcement Act of 1994 (CALEA).[1] The Department of Justice/Federal Bureau of Investigation (the Department) appreciates the close attention that the Commission has given to the various concerns implicated by § 105, and believes that the SSI Order will be largely effective in furthering this provision's important objectives. However, the Department believes that in a few important respects, the SSI Order omits obligations that are essential to the mandate of § 105.

The Department believes that to ensure the full achievement of Congress's purposes in enacting § 105, the SSI Order must be amended to include: (i) more effective personnel security obligations, including mechanisms for ensuring that law enforcement agencies will be able to

[1] In the Matter of Communications Assistance for Law Enforcement Act, *Report and Order*, CC Docket No. 97-213 (rel. Mar. 15, 1999), *modified by* In the Matter of Communications Assistance for Law Enforcement Act, *Order on Reconsideration*, CC Docket No. 97-213 (rel. Aug. 2, 1999); *summary published in* 64 Fed. Reg. 51,462 - 51,470 (Sep. 23, 1999).

No. of Copies rec'd 0+4
List ABCDE

conduct background checks on designated carrier employees who are heavily involved in electronic surveillance; (ii) a requirement that carriers generate an automated message that would enable law enforcement agencies to verify that unauthorized electronic surveillance is not occurring; (iii) a modification of the language establishing the timeliness with which security breaches must be reported; and (iv) a modification of the recordkeeping requirement pertaining to the commencement of interceptions. The Department suggests corresponding revisions to the rules accompanying the SSI Order in an appendix to this petition, and sets forth below its reasons for seeking reconsideration on these points.

1. Personnel Security Obligations

No effort to ensure systems security and integrity can be fully effective unless carriers and law enforcement agencies can have confidence in the trustworthiness of the people responsible for implementing interceptions. In the "Plain Old Telephone Service" environment, the people who conducted interceptions were law enforcement officials — individuals who were (and are) subject to extensive and rigorous background checks.[2] In the digital environment, however, employees of private telecommunications carriers increasingly must assist the law enforcement entities that have the legal authority (18 U.S.C. § 2518) to conduct electronic surveillance. In this new environment,

[2] Candidates to become agents of the Federal Bureau of Investigation must undergo a background check that includes (i) a polygraph test, (ii) a drug test, (iii) a credit check, (iv) a criminal records check, and (v) interviews with the candidate's references — who must include all of the candidate's previous employers, the management of places of residence occupied by the candidate during the prior ten years, three unrelated people who have known the candidate for over five years, three unrelated people who have known the candidate within the prior five years, the candidate's neighbors and friends, and administrators at schools attended by the candidate. This check is updated every five years. Other federal agencies that conduct electronic surveillance, as well as State and local law enforcement agencies, also conduct background checks upon candidates for employment. While these tests vary, they generally include at least a credit check and a criminal records check.

careful oversight is essential to § 105's purpose of ensuring that interceptions are activated "only in accordance with a court order or other lawful authorization" and only by individuals who are "acting in accordance with regulations prescribed by the Commission." 47 U.S.C. § 1004. Without effective oversight, there is a great danger that a carrier employee who is regularly involved in sensitive electronic surveillance activities might conduct unauthorized interceptions, assist others in doing so, or make improper disclosures of information pertaining to investigative activities. Obviously, any of these actions would infringe severely upon the privacy and security interests that Congress enacted § 105 to protect.

Because it is crucial to the purposes of § 105 to have some mechanism for verifying the trustworthiness of carrier employees regularly involved in implementing electronic surveillance, the Department asked the Commission to include in its implementing regulations provisions that would ensure that appropriate background checks are conducted on these employees. See FBI Dec. 12, 1997 Comments ("FBI Comments") 19. Notably, multiple commenters, including an industry association speaking on behalf of "tens of thousands of licensees" (PCIA Comments 1 n.1), concurred with the Department's position that background checks were necessary — and even went so far as to demand that the Commission expressly acknowledge that the carriers should either conduct these checks or cooperate with law enforcement agencies in having them performed.[3]

---

[3] See Omnipoint Comments 6 ("federal and state law should authorize a carrier, in an effort to discharge its responsibility, to furnish personal identifying information about designated employees to law enforcement officials as part of conducting a background check"); PCIA Comments 12 ("it is important that carriers be able to check the criminal records of their security personnel"); PCIA Reply Comments 13 ("the Commission could enhance its self-certification regime by permitting carriers to check the criminal records of their security personnel").

The Department also requested regulations that would require carriers to designate their employees authorized to conduct electronic surveillance and require these employees to sign appropriate non-disclosure agreements. See FBI Comments 24-25. Again, numerous commenters either stated that they supported an employee designation requirement, or indicated that such a requirement would necessitate no substantial departure from their existing practices.[4] To the extent that the commenters raised any serious opposition to the idea of maintaining a list of designated employees,[5] they primarily raised concerns regarding the requirement's apparent scope, suggesting that it would be unduly burdensome to designate all employees who might in the future become involved, to any degree, in any interception. See BellSouth Comments 11; Teleport Communications Group Comments 3; Bell Atlantic Mobile Comments 7-8; SBC Comments 19. The commenters raised very little opposition to the request that the designated employees execute non-disclosure agreements.

---

[4] See BellSouth Comments 11 ("BellSouth agrees that it is sound practice for carriers to designate specific employees, officers or both to assist law enforcement officials in the implementation of lawful interceptions"); U S West Comments 24 n.47 ("U S West incorporates the notions of designated versus non-designated employees in its daily operations"); AirTouch Comments 23 ("the same group of designated employees handle all interceptions"); AT&T Comments 32 ("AT&T * * * has certain identified personnel that are responsible for electronic surveillance"); Bell Atlantic Mobile Comments 7 ("[Bell Atlantic Mobile's] internal procedures ensure that only those employees who are fully trained in the obligations imposed by federal and state wiretap laws participate in surveillance efforts"); Teleport Communications Group Comments 3 ("[Teleport Communications Group] recommends that the 'designated employee' obligations be applied to a core group of key contact point personnel who have the primary responsibility of carrying out a lawful interception request").

[5] A few carriers argued that, despite the fact that they made it a practice to designate employees authorized to conduct interceptions, it would be unduly burdensome for them to create and maintain a *list* of the designated employees. See AirTouch Comments 24-25; Bell Atlantic Mobile Comments 7-8; BellSouth Comments 13. Of course, it is not possible for a carrier to designate the employees who will conduct electronic surveillance, and ensure that only those employees do so, without maintaining the functional equivalent of a list of the employees so designated.

The SSI Order rejected the Department's suggestions. The Order acknowledged that the background check and non-disclosure agreement provisions "may ensure a greater level of internal carrier systems security," but nevertheless concluded that carriers "will take necessary actions" without such requirements. SSI Order ¶ 26. The Order rejected the designation request as "impractical" and "invasive." *Id.* ¶ 25.

In light of the importance of these requests to the purposes of § 105, and the impressive degree of consensus between law enforcement and carriers that these measures are necessary, the Department respectfully requests that the Commission reconsider this portion of the SSI Order. The fact that many carriers are already conscientious about these matters demonstrates that the requested regulation would impose no new burdens on much of the industry, and in no way undermines the need for the regulation: Carriers that have not submitted comments, do no yet exist, or are destined to undergo changes in management may well need firm oversight from the Commission to ensure that their practices are fully consistent with § 105.

At the same time, the Department is prepared to modify and limit this request in light of the concerns about its scope that were raised by some carriers and referenced in the Order. Accordingly, the Department here requests that the Commission require carriers to include in their lists of designated employees only those employees who, as a regular part of their job duties, are exposed to information identifying the individuals whose communications are being intercepted pursuant to lawful electronic surveillance. Cf. Ameritech Comments 7 ("while some individuals will understand they are doing work to implement an intercept, these individuals will not have full knowledge regarding the line, the persons, the timing, the authorization, etc."). The Department believes that this limitation answers concerns regarding the scope of the designation requirement, while providing

an acceptable cutoff point defining the group of employees whose trustworthiness and reliability must be verified through background checks.

The Department also notes that it seeks to conduct only limited background checks for employees who are designated to facilitate general criminal (*e.g.*, Title III) intercepts, and more thorough background checks for employees who will facilitate electronic surveillance pursuant to the Foreign Intelligence Surveillance Act ("FISA"), which commonly involves exposure to information the improper dissemination of which could severely impair the national security. The background checks for employees designated to facilitate general criminal surveillance would normally involve simply a credit check and a criminal records check, requiring that law enforcement be provided only with the same sort of information that individuals routinely disclose when engaging in such commonplace activities as applying for video club memberships and department store credit cards. The proposed limited background checks would be scarcely more intrusive than the checks routinely conducted by landlords deciding whether to rent out an apartment, yet would play an important role in protecting the privacy and security interests that § 105 was enacted to protect. The background checks for employees designated to facilitate FISA surveillance would be more thorough, and would require the designated employees to cooperate directly with the law enforcement agencies conducting the checks by providing references and other necessary information.

a. List Of Limited Group Of Designated Employees

Therefore, the Department requests that the Commission modify the SSI Order to provide that carriers must maintain a list of employees designated to facilitate electronic surveillance, limited to those employees who, as a regular part of their job duties, are exposed to information identifying

the individuals whose communications are being intercepted pursuant to lawful electronic surveillance. The list would include the names, dates of birth, social security numbers, and workplace telephone numbers of these designated employees, and would be made available upon request to law enforcement agencies in order that they may conduct appropriate background checks on these employees.

b. Non-Disclosure Agreements Signed By Designated Employees

The Department also requests that the Commission require carriers to require these designated employees to sign agreements whereby they acknowledge the sensitivity of the information involved in electronic surveillance activities, agree to make no improper disclosures of this information, and agree to cooperate with law enforcement agencies as necessary to conduct appropriate background checks.

It remains unclear what persuasive objection could be raised to such a requirement. The execution of these agreements could hardly be thought to represent an oppressive administrative burden (particularly in light of the narrowed scope of the employee designation provision that the Department is now requesting), nor does the fact that such agreements may replicate obligations imposed under existing laws render them unreasonably duplicative; indeed, the overlap only reinforces the conclusion that the agreements would place no substantial new burdens upon the carriers. At the same time, such agreements would serve important functions that the mere existence of laws on the books would not, by ensuring that each designated employee is fully *aware* of these important non-disclosure obligations, and acknowledges her duty to protect sensitive information and to cooperate with law enforcement as necessary to the completion of appropriate background checks.

2. Surveillance Status Message

In its petition for a rulemaking to implement the "assistance capability" mandate set forth in § 103 of CALEA, the Department asked the Commission to require carriers to provide a "surveillance status message" capability that would permit law enforcement agencies to confirm periodically that the software used to conduct an interception is working correctly and is accessing the equipment, facilities, or services of the correct subscriber. See DOJ/FBI Joint Petition For Expedited Rulemaking ¶¶ 99-100; *id.* Appendix 1 at 13-14. In its Third Report and Order in that proceeding, the Commission ruled that neither this capability nor the other two requested capabilities collectively referred to as "surveillance integrity" items were part of the mandate placed upon telecommunications carriers by § 103. Third Report and Order ¶¶ 101, 106, 111. The Department does not here seek to challenge that ruling, or to suggest that the "continuity check tone" or "feature status message" capabilities fall within the mandate of § 105. However, the Department does believe that the surveillance status message capability falls squarely within the mandate of § 105, and should be incorporated in the Commission's rules implementing that provision.

When an intercept is, through inadvertence or design, implemented on, or transferred to, the wrong subscriber's facilities, it constitutes an "interception * * * effected within [the carrier's] switching premises" that is not activated "in accordance with a court order or other lawful authorization" (47 U.S.C. § 1004) — *i.e.*, precisely what § 105 was enacted to prevent. The surveillance status message capability is specifically designed to minimize such unauthorized interceptions, and thus to protect the interests that underlie § 105.

The fact that the Department initially requested this capability pursuant to § 103 should not prevent the Commission from incorporating it into its rules implementing § 105. The Department

initially requested this capability pursuant to § 103 because it believed that the capability fell within the mandate of that section (see 47 U.S.C. § 1002(a)(4)(A) (requiring carriers to be able to "facilitat[e] authorized communications interceptions * * * in a manner that protects * * * the privacy and security of communications * * * not authorized to be intercepted")), and also because the capability appeared to fall into the same "surveillance integrity" category as the other two capabilities that the Department placed under this heading in its § 103 filings. But considering whether this capability is required pursuant to § 105 would introduce no unfairness into this proceeding. An extensive record examining the various technical and cost-related issues connected with the surveillance status message was developed in the § 103 proceeding, and the Commission's reason for declining to require this capability pursuant to § 103 did not derive from technical or cost concerns, but from the Commission's conclusion that the language of § 103 did not require it. Third Report and Order ¶ 101. Thus, the only new question to be addressed here is whether the capability would implement the language of § 105, and an adequate record on this discrete question of statutory interpretation can be developed through the comment cycle connected with the instant petition.

3. Maximum Time To Report Suspected Compromise Of System Security

Even a well-constructed protocol of systems security and integrity cannot guarantee that no security breaches will occur. In order to minimize threats to the safety and privacy of informants, witnesses, and members of the public, it is necessary to ensure that such breaches are corrected with a degree of urgency appropriate to the weighty interests involved. For this reason, the Department asked the Commission to require carriers to report breaches (or suspected breaches) in the security or integrity of their systems to law enforcement no more than two hours after they have either

discovered the breaches or developed the reasonable suspicion that the breaches have occurred. See FBI Comments 20-21.

Although the SSI Order required carriers to report security breaches to the appropriate law enforcement agency, it rejected the Department's requested timing requirement, requiring only that breaches be reported "within a reasonable period of time upon discovery." SSI Order ¶ 38.

The Department has serious concerns as to the effectiveness of the "reasonable period of time" language included in the Commission's rule. Because the rule does not specify what family of concerns underlie the "reasonableness" criterion, carriers can be expected to read it with an eye to the concerns that seem most immediate to them, and thus to report breaches only as quickly as they feel is appropriate in light of their own business necessity or convenience. Should a carrier's promptness in reporting a compromise be challenged, it would likely seek to justify any delay by reference to such factors, and the challenger would not have access to the information about the carrier's internal operations that would be needed to refute the carrier's assertions. Such an outcome would undermine the language and purposes of § 105, which is designed, not to maximize the convenience of telecommunications carriers, but to minimize the privacy and security threats that result from compromises to the security and integrity of electronic surveillance.

The Department therefore requests that the Commission modify the language of its rule to require carriers to report breaches "as soon after discovery as is reasonable in light of privacy and safety concerns and the needs of law enforcement." This language would put carriers on notice that they may not effectively read the prompt reporting requirement out of the Commission's rule by assuming that delays may be justified by reference to their perceived business necessity.

4. Recording Of The Date And Time Of The "Opening Of The Circuit" For Law Enforcement

In its Notice of Proposed Rulemaking (SSI NPRM), the Commission proposed to implement 47 U.S.C. § 229(b)(2)'s requirement that carriers "maintain secure and accurate records of any interception" by requiring carriers to record (among other information) "the start date and time of [an] interception." SSI NPRM (rel. Oct. 10, 1997) ¶ 32. The SSI Order, however, modified this portion of the reporting obligation by requiring carriers to record "the start date and time of the *opening of the circuit* for law enforcement." SSI Order ¶ 44; *id.* App. A § 64.2104(a)(1)(ii) (emphasis added).

The Department believes that this language should be modified to exclude a construction that would enable carriers to evade the clear obligation in § 229(b) requiring carriers to maintain records of "any interception" — *i.e.*, of any *individual* interception. The SSI Order's reference to the start date and time of the "opening of the circuit" to law enforcement might be susceptible to an interpretation whereby, if a circuit to law enforcement were to be kept open for the duration of multiple intercepts, the carrier's records of these various intercepts would all show the same "start date and time." For example, some carriers keep a circuit to law enforcement open continuously, and for such carriers, the date and time of the "opening of the circuit" to law enforcement obviously would not correspond to any individual intercept. To avoid such an anomalous interpretation, the Department requests that this portion of the recordkeeping obligation be modified to require carriers to maintain records of the "date and time at which the interception of communications or access to call-identifying information was enabled."

With these modifications, the Commission's SSI Order will constitute a substantially more effective means of ensuring that Congress's objectives in enacting § 105 will be fully realized. The Department urges the Commission to make these modifications, and looks forward to working with the Commission and the telecommunications industry in implementing this important legislation.

DATE: October 25, 1999

Respectfully submitted,

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530

APPENDIX - PROPOSED MODIFICATIONS TO FINAL RULES

(Requested Modifications Shown in ***Boldface Italics***)

AMENDMENTS TO THE CODE OF FEDERAL REGULATIONS

PART 64 - MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

Part 64 of the Code of Federal Regulations (C.F.R.) is amended as follows:

* * * * *

§ 64.2102 Definitions

* * * * *

(d) Surveillance Status Message. Capability that permits a law enforcement agency to confirm periodically that the interception software is working correctly and accessing the equipment, facilities, or services of the correct subscriber.

§ 64.2103 Policies and Procedures for Employee Supervision and Control.

A telecommunications carrier shall:

* * * * *

(e) report to the affected law enforcement agencies, ***as soon after discovery as is reasonable in light of privacy and safety concerns and the needs of law enforcement***:

(1) any act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities; and

(2) any act of unlawful electronic surveillance that occurred on its premises.

* * * * *

(g) maintain a list of its employees who, as a regular part of their job duties, are exposed to information identifying the individuals whose communications are being intercepted pursuant to lawful electronic surveillance. This list should include each designated employee's (i) name, (ii) date of birth, (iii) social security number, and (iv) workplace telephone number.

(h) require its employees who are designated to be regularly involved in the facilitation of electronic surveillance and who, as a regular part of their job duties, are exposed to information identifying the individuals whose communications are being intercepted pursuant to lawful electronic surveillance, to sign non-disclosure agreements whereby they acknowledge the

sensitivity of the information involved in electronic surveillance activities, agree to make no improper disclosures of this information, and agree to cooperate with law enforcement agencies as necessary to conduct appropriate background checks.

§ 64.2104 Maintaining Secure and Accurate Records.

A telecommunications carrier shall:

(a) maintain a secure and accurate record of each interception of communications or access to call-identifying information, made with or without appropriate authorization, in the form of single certification.

(1) This certification must include, at a minimum, the following information: (i) the telephone number(s) and/or circuit identification numbers involved; (ii) the ***date and time at which the interception of communications or access to call-identifying information was enabled***;

* * * * *

(new) ***§ 64.2105 Ensuring the Prompt Termination of Unauthorized Electronic Surveillance.***
(existing §§ 64.2105 and 64.2016 to be redesignated §§ 64.2106 and 64.2107)

As of September 30, 2001 a telecommunications carrier shall provide to a law enforcement agency the surveillance status message capability.

Certificate of Service

I, Myla R. Saldivar-Trotter, Federal Bureau of Investigation, hereby certify that a true copy of the foregoing **Petition for Reconsideration of Section 105 Report and Order** was served via hand delivery (indicated by *) or by mail to the following parties:

Myla R. Saldivar-Trotter

Myla R. Saldivar-Trotter

The Honorable William E. Kennard*
Chairman
Federal Communications Commission
445 Twelfth Street, S.W., Room 8B201
Washington, D.C. 20554

Ari Fitzgerald*
Legal Advisor to Chairman Kennard
Federal Communications Commission
445 Twelfth Street, S.W., Room 8B201
Washington, D.C. 20554

The Honorable Harold Furchtgott-Roth*
Commissioner
Federal Communications Commission
445 Twelfth Street, S.W., Room 8A302
Washington, D.C. 20554

The Honorable Susan Ness*
Commissioner
Federal Communications Commission
445 Twelfth Street, S.,W., Room 8B115
Washington, D.C. 20554

The Honorable Michael Powell*
Commissioner
Federal Communications Commission
445 Twelfth Street, S.W., Room 8A204
Washington, D.C. 20554

The Honorable Gloria Tristani*
Commissioner
Federal Communications Commission
445 Twelfth Street, S.W., Room 8C302
Washington, D.C. 20554

Mark Schneider*
Legal Advisor To Commissioner Ness
Federal Communications Commission
445 Twelfth Street, S.W., Room 8B115B
Washington, D.C. 20554

Bryan Tramont*
Legal Advisor to
Commissioner Furchtgott-Roth
Federal Communication Commission
445 Twelfth Street, S.W., Room 8A302B
Washington, D.C. 20554

Peter Tenhula*
Legal Advisor to Commissioner Powell
Federal Communications Commission
445 Twelfth Street, S.W., Room 8A204F
Washington, D.C. 20554

Karen Gulick*
Legal Advisor To Commissioner Tristani
Federal Communications Commission
445 Twelfth Street, S.W., Room 8C302F
Washington, D.C. 20554

Christopher J. Wright*
General Counsel
Federal Communications Commission
445 Twelfth Street, S.W., Room 8C755
Washington, D.C. 20554

Thomas Sugrue*
Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Kent Nilsson *
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Jim Burtle*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Rodney Small*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W., Room 7A121
Washington, D.C. 20554

Charlene Lagerwerff*
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street, S.W., Room 4A124
Washington, D.C. 20554

Tejal Mehta*
Wireless Telecommunciations Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Lawrence E. Strickling*
Chief
Common Carrier Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Anna Gomez*
Chief
Network Services Division
Common Carrier Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Charles Iseman*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Julius Knapp*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Geraldine Matise*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

James F. Green*
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street, S.W., Room 4A237
Washington, D.C. 20554

David O. Ward*
Network Services Division
Common Carrier Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Dale Hatfield *
Chief
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Susan Aaron*
Office of General Counsel
Federal Communications Commission
445 Twelfth Street, S.W., Room 8A522
Washington, D.C. 20554

Diane Conley*
Wireless Telecommunications Bureau
445 Twelfth Street, S.W., 4th Floor
Washington, D.C. 20554

David Krech*
Wireless Telecommunications Bureau
445 Twelfth Street, S.W., Room 4A223
Washington, D.C. 20554

Matthew J. Flanigan
President
Telecommunications Industry Association
Suite 300
2500 Wilson Boulevard
Arlington, VA 22201-3834

Stewart A. Baker
Tom Barba
Steptoe & Johnson, LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795

Thomas Wheeler
President & CEO
Cellular Telecommunications Industry
Association
Suite 200, 1250 Connecticut Avenue, N.W.
Washington, D.C. 20036

Albert Gidari
Perkins Coie
1201 Third Avenue
40th Floor
Seattle, Washington 98101

Mark J. Golden
Senior Vice President, Industry Affairs
Robert Hoggarth
Senior Vice President, Paging/Messaging
Personal Communications Industry Association
Suite 700
500 Montgomery Street
Alexandria, VA 22314-1561

Roy Neel
President & CEO
United States Telephone Association
Suite 600
1401 H Street, N.W.
Washington, D.C. 20005-2164

Alliance for Telecommunication Industry
Solutions
Suite 500
1200 G. Street, N.W.
Washington, D.C. 20005

Jerry Berman
Executive Director
Center for Democracy and Technology
Suite 1100
1634 Eye Street, N.W.
Washington, D.C. 20006

Mark C. Rosenblum
Ava B. Kleinman
Seth S. Gross
Room 3252F3
295 North Maple Avenue
Basking Ridge, NJ 07920

Pamela J. Riley
David A. Gross
AirTouch Communications, Inc.
1818 N Street, N.W.
Washington, D.C. 20036

James P. Lucier, Jr.
Director of Economic Research
Americans for Tax Reform
Suite 200
1320 Eighteenth Street, N.W.
Washington, D.C. 20036

Anita Sheth
Director, Regulatory Policy Studies
Citizens for a Sound Economy
Suite 700
1250 H Street, N.W.
Washington, D.C. 20005

Eric W. DeSilva
Stephen J. Rosen
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006

Michael Altschul
Vice President and General Counsel
Randall S. Coleman
Vice President, Regulatory Policy and Law
Cellular Telecommunications Industry Association
Suite 200, 1250 Connecticut Avenue, N.,W.
Washington, D.C. 20036

William L. Roughton, Jr.
Associate General Counsel
PrimeCo POersonal Communications, L.P.
Suite 320 South
601 Thirteenth Street, N.W.
Washington, D.C. 20005

Joseph R. Assenzo
4900 Main Street, 12th Floor
Kansas City, MO 64112

Lisa S. Dean
Director, Center for Technology Policy
Free Congress Foundation
717 Second Street, N.E.
Washington, D.C. 20002

James X. Dempsey
Senior Staff Counsel
Daniel J. Weitzner
Deputy Director
Center for Democracy and Technology
Suite 1100
1634 Eye Street, N.W.
Washington, D.C. 20006

Lawrence E. Sarjeant
Linda Kent
Keith Townsend
Suite 600
1401 H Street, N.W.
Washington, D.C. 20005

John Pignataro
Senior Technical Advisor
Police Department, City of New York
Fort Totten Building 610
Bayside, NY 11359

Barbara J. Kern
Counsel
Ameritech Corporation
4H74
2000 Ameritech Center Drive
Hoffman Estates, IL 60196

James D. Ellis
Robert M. Lynch
Durward D. Dupre
Lucille M. Mates
Frank C. Magill
175 E. Houston, Room 4-H-40
San Antonio, TX 78205

Robert Vitanza
Suite 1300
15660 Dallas Parkway
Dallas, TX 75248

M. Robert Sutherland
Theodore R. Kingsley
BellSouth Corporation
Suite 1700
1155 Peachtree Street, N.E.
Atlanta, GA 30309-3610

Michael P. Goggin
BellSouth Cellular Corp.
Suite 910
1100 Peachtree Street, N.E.
Atlanta, GA 30309-4599

Michael W. White
BellSouth Wireless Data, L.P.
10 Woodbridge Center Drive, 4th Floor
Woodbridge, NJ 07095-1106

J. LLoyd Nault, II
BellSouth Telecommunications, Inc.
4300 BellSouth Center
675 West Peachtree Street, N.E.
Atlanta, GA 30375

Charles M. Nalbourne
Suite 400
3353 Peachtree Road, N.E.
Atlanta, GA 30326

Kurt A. Wimmer
Gerard J. Waldron
Alane C. Weixel
Ellen P. Goodman
Erin Egan
Covington & Burling
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566

William T. Lake
John H. Harwood, II
Samir Jain
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420

Kathryn Marie Krause
Edward M. Chavez
1020 Nineteenth Street, N.W.
Washington, D.C. 20036

John M. Goodman
Attorney for Bell Atlantic telephone companies
1300 I Street, N.W.
Washington, D.C. 20005

Martin L. Stern
Lisa A. Leventhal
Preston Gates Ellis & Rouvelas Meeds LLP
Suite 500
1735 New York Avenue, N.W.
Washington, D.C. 20006

Cheryl A. Tritt
James A. Casey
Morrison & Foerster LLP
Suite 5500
2000 Pennsylvania Avenue, N.W.
Washington, D.C 20006

Sylvia Lesse
Marci Greenstein
Kraskin, Lesse & Cosson, LLP
2120 L Street, N.W.
Suite 520
Washington, D.C. 20037

Henry M. Rivera
Larry S. Solomon
J. Thomas Nolan
Shook, Hardy & Bacon LLP
Suite 900
1850 K Street, N.W.
Washington, D.C. 20006

John T. Scott, III
Crowell & Moring LLP
1001 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Carole C. Harris
Christine M. Gill
Anne L. Fruehauf
McDermott, Will & Emery
600 Thirteenth Street, N.W.
Washington, D.C. 20005

Francis D. R. Coleman
Director of Regulatory Affairs
- North America
ICO Global Communications
Suite 550
1101 Connecticut Avenue, N.W.
Washington, D.C. 20036

Joel M. Margolis
Corporate Counsel-Regulatory
Nextel Communications, Inc.
Suite 100
1505 Farm Credit Drive
McLean, VA 22102

Robert M. Lynch
Roger K. Toppins
Hope E. Thurrott
One Bell Plaza, Room 3023
Dallas, TX 75202

Colette M. Capretz
Fisher Wayland Cooper
Leader & Zaragoza LLP
Suite 400
2001 Pennsylvania Avenue, N.W.
Washington, D.C. 20006

Lon C. Levin
Vice President and Regulatory Counsel
American Mobile Satellite Corporation
10802 Park Ridge Boulevard
Reston, VA 20191

Edward J. Wisniefski
Deputy Assistant Administrator
Office of Investigative Technology
Drug Enforcement Administration
8198 Terminal Road
Lorton, VA 22079

Peter M. Connolly
Koteen & Naftalin, LLP
1150 Connecticut Avenue, N.W.
Washington, D.C. 20036

L. Marie Guillory
Jill Canfield
National Telephone Cooperative Association
4121 Wilson Boulevard, 10th Floor
Arlington, VA 22203-1801

Colonel Carl A. Williams
Superintendent, New Jersey State Police
P.O. Box 7068
West Trenton, NJ 08628-0068

Dudley M. Thomas
Director, Texas Department of Public Safety
5805 N. Lamar Boulevard
Box 4087
Austin, TX 78773-0001