PIPER & MARBURY
L.L.P.
1200 NINETEENTH STREET, N.W.
WASHINGTON, D.C. 20036-2430
202-861-3900
FAX: 202-223-2085

BALTIMORE
NEW YORK
PHILADELPHIA
EASTON
LONDON

WRITER'S DIRECT NUMBER
202-861-3938
FAX: 202-223-2085
jhalpert@pipermar.com

DOCKET FILE COPY ORIGINAL

March 30, 1998

RECEIVED
MAR 31 1998
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

HAND DELIVERY

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
1919 M Street, N.W.
Room 222
Washington, DC 20554

Re: Comments of Omnipoint Communications Inc.

Dear Ms. Salas:

Enclosed please find an original and eleven (11) copies of the Comments of Omnipoint Communications Inc., and Motion for Leave to File Late-Filed Comments filed in the above-captioned matter.

If you have any questions, please feel free to contact me.

Sincerely,

James J. Halpert

JJH/spj
Enclosure

No. of Copies rec'd 0+11
List A B C D E

WASH01A:122829:1:03/30/98
22489-1

DOCKET FILE COPY ORIGINAL

RECEIVED

MAR 31 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Before the
Federal Communications Commission
Washington, D.C.

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Dkt. No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended	)	CC Dkt. No. 97-149

MOTION FOR LEAVE TO FILE LATE-FILED COMMENTS

Omnipoint Communications Inc. ("Omnipoint"), by its attorneys, hereby moves for leave to file the attached late-filed comments in the above-captioned proceeding.

In support of its motion, Omnipoint submits: (1) that it attempted to deliver its comments at the Commission at 5:33 p.m. on March 30, 1998; (2) acceptance of the comments will not prejudice any party to this proceeding because the comments are being filed in the Commission Secretary's Office at 9:00 a.m. on March 31st, will be hand-delivered to International Transcription Services, and an electronic copy of the comments was delivered to the Common Carrier Bureau for web posting on March 30th; and (3) that this is a Notice and Comment proceeding for which an eighteen hour filing delay will not materially affect any party's rights.

WHEREFORE, good cause having been shown, Omnipoint asks that the Commission grant the relief requested.

James J. Halpert

Piper & Marbury L.L.P.
1200 19th Street, N.W.
Seventh Floor
Washington, D.C. 20036
(202) 861-3900

Its Attorney

Before the
Federal Communications Commission
Washington, D.C.

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Dkt. No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended	)	CC Dkt. No. 97-149

COMMENTS OF OMNIPOINT COMMUNICATIONS INC.

Mark J. O'Connor
James J. Halpert

Piper & Marbury L.L.P.
1200 19th Street, N.W.
Seventh Floor
Washington, D.C. 20036
(202) 861-3900
Its Attorneys

Date: March 30, 1998

TABLE OF CONTENTS

Page

I. INTRODUCTION AND SUMMARY 1

II. ALLOWING A BROAD CUSTOMER OPT-OUT TO "TOTAL SERVICE" CPNI WOULD IMPOSE MAJOR COSTS AND SEVERE OBSTACLES TO INTEGRATED CMRS PROVIDERS 2

III. THE COMMISSION SHOULD REJECT THE FBI'S REQUESTS TO IMPOSE RESTRICTIONS ON FOREIGN STORAGE OF DOMESTIC CPNI AND CALEA-LIKE MANDATES OF RETENTION OF U.S.-BASED CPNI 6

A. The Commission Should Reject the FBI's Request to Prohibit Foreign Storage and Access to Customer CPNI 7

B. The Commission Should Reject the FBI's Request for Additional Record-Keeping Requirements for U.S. Carriers 10

IV. CONCLUSION 11

I. INTRODUCTION AND SUMMARY

Omnipoint Communications Inc. ("Omnipoint"), by its attorneys, files these comments in response to the Commission's Further Notice of Proposed Rulemaking in its CPNI proceeding.[1] Omnipoint, through its affiliates, holds the New York MTA Block A license, 18 Block C PCS licenses for which it bid a net price of $509 million, and 108 Block D, E and F licenses for which it bid a net price of $181 million (including 50 Block F licenses at a net price of $74 million). Omnipoint currently operates PCS systems in a number of markets, including New York City, Philadelphia, Boston and Miami.

The PCS technology used by Omnipoint, Global System for Mobile communications ("GSM"), developed and deployed internationally before passage of the 1996 Act,[2] provides customers with an innovative, integrated service that delivers basic and adjunct-to-basic CMRS voice telephony, as well as a range of information services through a single handset. Through Omnipoint's GSM encrypted service, all Omnipoint customers have access through their handset to voice mail, brief two-way e-mail text messages, faxing, paging, news headlines, sports scores, stock quotes and weather information on demand for any city. Each handset also includes a unique Internet address.

The ability to market and to deliver integrated digital services is one of the chief advantages of PCS technology, and the value of such integration contributed to the success of the Commission's auctions of PCS spectrum. It is critical to PCS providers' ability to break into and succeed in markets occupied by large incumbent wireless providers. However, the regulatory categories set forth in the Second Report and Order

---

1 Second Report and Order and Further Notice of Proposed Rulemaking, CC Dkt. 96-115 & 97-149 (rel. Feb. 26, 1998) (hereafter "the FNPRM").

2 P.L. 104-104.

and FNPRM pose unique difficulties for Omnipoint and similarly situated CMRS providers who have provided integrated service offerings since the inception of their service.

Because of the unique burden that CPNI restrictions impose on integrated CMRS offerings, Omnipoint asks the Commission not to apply customer opt-out rules to CMRS providers. At a bare minimum, the Commission should make clear that customer opt-outs do not apply to information relating to customer subscription to information services, and that the statutory exceptions set forth in subsection 222(d) apply to CMRS providers' use of data they obtain concerning subscribers' use of information services.

Furthermore, Omnipoint urges the Commission to reject the FBI's requests to prohibit foreign storage of and access to domestic CPNI, and to mandate domestic storage of U.S.-based customer CPNI. These requests are incompatible with the statutory scheme, are enormously overbroad, and would create serious obstacles to provision of international and domestic GSM roaming service.

II. ALLOWING A BROAD CUSTOMER OPT-OUT TO "TOTAL SERVICE" CPNI WOULD IMPOSE MAJOR COSTS AND SEVERE OBSTACLES TO INTEGRATED CMRS PROVIDERS

The FNPRM asks whether the Commission should establish rules giving customers "a right to restrict all marketing uses of CPNI" through an opt-out from "use of CPNI for all marketing purposes, even within the customer's total service offering." Id. at ¶ 205. In Omnipoint's view, it should not, but if it does create such a right, it should exempt CMRS providers who provide integrated services.

Section 222 of the Act provides important protections for customer privacy, and the Commission has already interpreted these protections in a very robust way, mandating opt-in requirements and burdensome internal compliance procedures for all individually identifiable information other than that exempted by subsections 222(c)(1)(A) and (B). To add to this regime an opt-out requirement for CPNI within the total service offering

would be contrary to the structure of the statute. It would also pose an unjustifiable barrier to competition by CMRS providers, such as Omnipoint, whose technology is specifically designed to offer integrated telecommunications and information services.

Neither subsections 222(a) nor (c) supports such an opt-out requirement, much less require its imposition on CMRS providers who already offer integrated total service offerings. Subsection 222(c) is the statutory provision addressing the information at issue. It sets forth in specific terms the categories of individually identifiable CPNI that telecommunications carriers *may* make use of, disclose or permit access to without customer request. 47 U.S.C. § 222(c)(1). While the language of this provision limits these categories, it imposes no restrictions whatsoever on use of the information falling with the defined range of CPNI that carriers may use.

Subsection 222(a) provides only the most general support for an additional opt-out requirement, and in any event is outweighed by the specific language of § 222(c)(1). Subsection 222(a) is a very general provision, and does not even use the term CPNI. Instead, it refers to telecommunications carriers' amorphous duty to protect the confidentiality of "proprietary information" belonging to or relating to other carriers, equipment manufacturers and customers. 47 U.S.C. § 222(a). This duty is then specified in the remaining subsections of the statute. Because § 222(c)(1) is the more specific section, and deals expressly with the very category of CPNI that would be subject to an opt-out, it should govern the Commission's decision on this question.

Having already established robust customer privacy protections in the Second Report and Order, the Commission has already created far-reaching privacy protections, and should regulate no further.

Restricting use of CPNI obtained through the provision of integrated PCS total service offerings is a special case posing unique difficulties. Under the language of Section 222, information services listed on a telecommunications bill constitute CPNI.

47 U.S.C. § 222(f)(1)(B). However, the statutory exceptions expressly permitting use of CPNI to bill, collect, or prevent fraudulent use or misappropriation apply only to telecommunications services. See 47 U.S.C. §§ 222(d)(1) and (2). As a result, if an opt-out rule were to apply, customers would be able to opt out of *any* use of CPNI concerning bundled information services, *even for* billing, collection or prevention of fraud or misappropriation of the providers' information services. Accordingly, the Commission should decline to create an opt-out for integrated PCS offerings.

Through a statutory anomaly,[3] the fact that data concerning use of these information services happens to appear on "bills pertaining to" telephony services may bring data concerning use of bundled PCS information services within the sweep of the CPNI statute. See 47 U.S.C. § 222(f)(1)(B) (defining CPNI as including "information contained in the bills pertaining to telephone exchange service or telephone toll service"). Therefore, imposing an opt-out from PCS total service offerings would sweep in information service usage data that would not otherwise be part of CPNI.

Furthermore, imposing an opt-out from PCS total service offerings would risk precluding use of information service data for important statutory purposes that are expressly permitted under § 222(d) for telecommunications service data. Section 222(d) exceptions override the other privacy provisions of the statute to permit use of CPNI for initiating, rendering, billing and collecting "for telecommunications service," and for preventing fraud and unauthorized use of "such services." 47 U.S.C. §§ 222(d)(1) and

---

3 This statutory problem occurred because Section 222 was the product of a compromise between incumbent local exchange carriers (ILECs), inter-exchange carriers (IXCs) and resellers. The authors of this language had little or no awareness of the nature of integrated service offerings in the fledgling PCS industry. Cf. H. Rep. No. 104-458, Joint Explanatory Statement of the Committee of Conference, at 203-05.

(2). However, these exceptions do *not* permit use of CPNI for the same functions with respect to "information services."

For this reason, applying an opt-out rule to integrated PCS offerings would produce the bizarre result that CMRS customers could opt out of use of information service-related CPNI for billing and collection and for fraud prevention.

The inability to use bundled CPNI would be particularly problematic for Omnipoint and other similarly situated PCS carriers because a critical feature of this service is the ability to bundle information service features with CMRS voice telephony. The GSM standard that Omnipoint uses was developed and deployed before passage of the 1996 Act and the commencement of this rulemaking. It provides customers with the ability to receive telecommunications, adjunct-to-basic and a range of voice and text information services through the customer's handset. For example, as stated above, Omnipoint offers its CMRS customers bundled information services, including voice messaging, transmission and receipt of short e-mail messages and a package of news headlines, sports scores, weather information, and stock quotes. For both customer and carrier convenience, these services are included as charges in the customer's phone bill. The ability to deploy and to market all these services as part of an integrated service offering is critical to PCS providers' ability to break into and to succeed in highly competitive markets occupied by large incumbent wireless providers.

This bundling of traditional telephony functions with enhanced features is precisely the sort of innovation that Congress sought to reward when it passed the provisions of the Omnibus Budget Reconciliation Act of 1993 addressing CMRS services, as well as in Section 222. Moreover, the Commission's Second Report and Order itself supports such offerings. See id. at ¶¶ 58, 64 (expressing support for permitting use of CPNI for innovation and for total service offerings).

The Commission should make clear that customers may not opt out of use of data concerning their usage of PCS information services even if such data happen to appear on a telephone bill, and that such data may be used for all the purposes set forth in § 222(d).

III. THE COMMISSION SHOULD REJECT THE FBI'S REQUESTS TO IMPOSE RESTRICTIONS ON FOREIGN STORAGE OF DOMESTIC CPNI AND CALEA-LIKE MANDATES OF RETENTION OF U.S.-BASED CPNI.

The Commission also seeks comment on the FBI's effort to conjure up from Section 222 two inconsistent requirements: first, a prohibition against foreign storage of and foreign direct access to domestic CPNI, and second, a mandate to maintain copies of the CPNI of all U.S.-based customers. FNPRM at ¶¶ 208-10.

These proposed requirements would impose burdensome obstacles to PCS international calling and roaming services to the detriment of consumers.[4] Like its more extreme demands in the CALEA negotiating process, the FBI's proposed prohibitions against foreign storage of and foreign direct access to CPNI require a wholesale change in the law and should be addressed to Congress, not the Commission. The FBI's proposed domestic CPNI record-keeping requirement risks imposing burdensome, undefined obligations on carriers. In Omnipoint's view, if the Commission is inclined to grant these requests, it should narrow them greatly, and specify that the rules should not apply to information exchanged between a foreign carrier and a domestic carrier providing international long distance or roaming service.

---

4 Omnipoint presently has roaming agreements for its customers with over 70 CMRS providers, including international roaming agreements in 28 countries.

A. The Commission Should Reject the FBI's Request to Prohibit Foreign Storage and Access to Customer CPNI

First, the FBI requests that carriers be prohibited from storing abroad or allowing direct foreign access to the CPNI of "U.S. Customers who only subscribe to domestic telecommunications services." Although characterizing the scope of its request as covering CPNI that is "essentially intra-U.S. in nature," the FBI actually seeks to apply its storage and direct access requirements to U.S. "long distance service where international calls may be placed." FBI Ex Parte, at 1 n.1.

Section 222(a) provides no support for special obligations relating to foreign access to CPNI. The statute and conference report make no mention whatsoever of any of the policy concerns raised by the FBI's Ex Parte submission, with the exception of privacy.[5] Furthermore, they do not reveal any concern whatsoever with the question of foreign access to CPNI. Indeed, § 222(a) simply applies generically to "[e]very telecommunications carrier," and § 222(d) applies to "a telecommunications carrier." The plain language of the statute simply does not leave room for special burdens or restrictions on carriers who provide international service.

Nor do other statutes support the FBI's request. The closest candidate is Section 220, which grants the Commission authority to prescribe the "forms of" and to obtain "access to" carriers' accounts, records and memoranda. 47 U.S.C. §§ 220(a) and (c). However, this statute does not encompass the authority to prescribe the *location* of such information or to *limit others' access* to these records. Accordingly, the FBI's proposed storage and access restrictions would be contrary to law.

---

5 The FBI's stated concern with the privacy of U.S. customer information, Ex Parte at 3-4, is called into question by its obvious desire to ensure that the information is stored within the U.S. so as to afford ready access for investigations. Id. at 4-9.

From a policy perspective, the FBI's proposal risks presenting serious obstacles to the provision of international CMRS and CMRS roaming services. As the Commission recognized in its Foreign Participation Order,[6] foreign carriers terminating international calls collect U.S. customer calling information on the foreign end of the international route. Id. at ¶ 175. Under the broad formulation of the FBI's request, foreign carriers who terminate international calls might be prohibited from receiving CPNI for U.S.-originated traffic. Any restriction would have to provide in clear terms exceptions for effecting settlements and billing international services.

Applying the FBI's prohibitions in the context of GSM roaming is even more problematic. For example, when American GSM customers use their handsets internationally, some of the customers' CPNI, including information regarding the services that the customer is authorized to receive, is transferred automatically to the foreign carrier. A rule prohibiting foreign carriers from obtaining direct access to CPNI used in roaming would make international GSM roaming nearly impossible.

With respect to foreign warehousing and processing of CPNI, the FBI's proposal is likewise overbroad. It is based upon a sweeping, unsubstantiated assumption that such information would not be secure in any foreign location, and that encryption and other security measures would be insufficient to prevent access by foreign intelligence agencies. Omnipoint respectfully submits that if any restriction were consistent with the statute, which we believe it is not, a better approach would be to establish security requirements, rather than the outright ban suggested by the FBI.

The FBI's proposed restrictions would doubtless trigger retaliation from foreign countries, creating major obstacles to the provision of international service. It would be

---

6 Report and Order, In the Matter of Foreign Participation in the U.S. Market, IB Dkt. Nos. 97-142 and 95-22 (rel. Nov. 25, 1997).

particularly unwise to impose such a restriction now, at the dawn of international competition under the WTO Basic Telecommunications Agreement and months before the effective date of the E.C. Data Protection Directive (October, 1998). If the United States were to impose such a restriction, the result would be corresponding restrictions making it more difficult for U.S. companies to take advantage of opportunities under the WTO accord to penetrate foreign markets.[7]

Finally, the FBI's proposed prohibition against the transborder flow of domestic CPNI would set an enormously negative precedent for the global information economy generally, in which services must be rendered and billed across national boundaries.

Concerns that the FBI, CIA, DOD and others may have about storage and access to the CPNI of their employees can be addressed through targeted legislation, as well as through the government's exercise of its considerable contracting powers to obtain special arrangements for its employees.[8] However, the FBI's request is not permitted by existing law and the request is framed so sweepingly as to have major detrimental effects on other important policy goals.

---

[7] The Commission should also be mindful of the effect of the FBI's proposal on negotiations that the Commerce Department is engaged in with the European Commission over a somewhat similar European data transfer restriction. The E.C. Data Protection Directive would impose extensive, burdensome regulation of individually identifiable information concerning European citizens. Article 25 of the Directive prohibits data transfers to non-E.U. countries that lack "adequate" privacy protections. The Department of Commerce is in the midst of prolonged negotiations with the European Community to avert a trade war over the Directive. If the FCC were to issue regulations adopting the FBI's proposal for similar restrictions on transborder flows of CPNI, it would risk undercutting the United States' negotiating position in Europe.

[8] Moreover, even without government intervention, market forces help to protect the confidentiality of CPNI. CPNI is extremely valuable information that U.S. carriers have every interest in keeping safe from foreign intrusion and economic espionage.

B. The Commission Should Reject the FBI's Request for Additional Record-Keeping Requirements for U.S. Carriers

The FBI asserts without any supporting legal authority that the Commission must require that U.S. carriers maintain copies of the CPNI of all U.S.-based customers, including the CPNI of customers who make international calls pursuant to special contracts, tariff arrangements or volume discount arrangements.

The FNPRM does not provide sufficient notice to comment in detail on this request. Neither the FBI's request nor the FNPRM itself specifies what records would be stored, the form of storage, or the length of time the copies would have to be retained.

To the extent that the FBI seeks records that companies store in the ordinary course of business, or that must be available under existing law for purposes of complying with the Commission's existing regulations issued under Section 220, Omnipoint has no objection to the FBI's proposal.

However, the Bureau's request appears to suggest that it wants considerably more. Omnipoint notes that its proposal would be particularly burdensome for CPNI relating to calls by customers of other carriers who roam within a GSM-provider's network. Billing information and call detail records for such customers' usage is retained for a limited amount of time, conveyed through a clearinghouse to the billing carrier, and removed from the GSM roaming provider's billing systems. To require the carriers providing roaming service to retain such information would present a major burden on these carriers' systems, and have a particularly negative effect on smaller providers.

If the FBI wants carriers to expand their record-keeping of CPNI, it should compensate carriers for this service, rather than attempting to use Section 220 or other statutory provisions to force these costs on providers. In preserving and expanding its surveillance capabilities, the FBI has already made extensive demands on the telecommunications industry as part of the CALEA negotiating process. Congress has followed the CALEA process closely, and taken an active role in oversight of FBI-

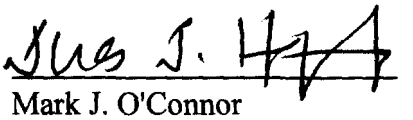
industry negotiations. Acting on the FBI's latest request would be inappropriate in that it would circumvent the general principle under CALEA that carriers are compensated for changes to their operations made solely to accommodate government surveillance requests. Acting on the FBI's request in this proceeding would be particularly inappropriate because the congressional statute on the subject, Section 222, nowhere *requires* storage of CPNI, and instead establishes a series of limits upon what carriers may do with such information if they store it.

Conclusion

Omnipoint urges that opt-out rules not be applied to integrated PCS total service offering CPNI because Section 222 would prevent these PCS providers from using bundled information service CPNI for billing, collecting, fraud prevention and other important statutory purposes. In addition, Omnipoint asks the Commission to reject the FBI's call to impose record storage, access and maintenance requirements on CPNI that are incompatible with Section 222 and would seriously impede PCS international and roaming service.

Respectfully submitted,

OMNIPOINT COMMUNICATIONS INC.

By: 

Mark J. O'Connor
James J. Halpert
Piper & Marbury L.L.P.
1200 19th Street, N.W.
Seventh Floor
Washington, D.C. 20036
(202) 861-3900
Its Attorneys

Date: March 30, 1998