DOCKET FILE COPY ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

RECEIVED ORIGINAL

APR 14 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket 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 Docket No. 96-149

REPLY COMMENTS OF MCI TELECOMMUNICATIONS CORPORATION

MCI TELECOMMUNICATIONS CORPORATION

Frank W. Krogh
Mary L. Brown
1801 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
(202) 887-2372

Its Attorneys

Dated: April 14, 1998

No. of Copies rec'd 0+6
List A B C D E

TABLE OF CONTENTS

Summary ii

A. Additional Customer Restrictions on CPNI Use 2

B. Carrier Proprietary Information 7

1. The ILEC's Comments Underscore the Need for Clear Rules Protecting Carrier Proprietary Information 7

2. Clear Rules Protecting Billing Data Are Needed . . 12

3. Once Clear Rules Are Established, No Additional Safeguards Should be Necessary 17

C. Foreign Storage of Domestic CPNI 19

D. Conclusion 22

SUMMARY

The overwhelming majority of commenters from all segments of the industry are in agreement with MCI that the Commission should reject the proposals to allow a customer to bar her carrier's use of her customer proprietary network information (CPNI) for any marketing purposes and to prohibit carriers from storing domestic CPNI abroad.

Various parties point out that allowing customers to bar any marketing use of CPNI would upset the balance between privacy and competitive goals struck by Congress in Section 222 and would do little to protect customers' interest in being left alone. To the contrary, prohibiting any use of CPNI would likely result in greater intrusions, as carriers would not be able to rationally exclude customers from marketing campaigns on the basis of their CPNI, thereby subjecting customers to more marketing, not less.

Several commenters echo MCI's point that denial of any use of CPNI would have anticompetitive consequences, since it would make marketing less effective. Anything that makes marketing less effective will disproportionately burden smaller carriers, since they cannot afford mass marketing campaigns, and tend to favor incumbents. Such results would defeat rather than further the goals of Section 222.

Comments on the issue of the application of Section 222(a) and (b) to carrier proprietary information range from ILEC assertions that no rules are needed to protect such information

to the request of the TRA that the Commission impose certain database access restrictions.

ILEC interpretations of Section 222(a) and (b) reveal the necessity of Commission rules implementing those provisions. US West, for example, tries to distinguish between "proprietary" information covered by Section 222(a) and "competitively sensitive" information, which allegedly is not covered. It will obviously be necessary for the Commission to define "proprietary" so that carriers understand the competitive significance of proprietary information and its misuse. It is especially important that the Commission take steps to halt the abuses of IXC billing information by LECs, which attempt to avoid their duties under Section 222(a) to protect the confidentiality of such data by soliciting customer authorizations to use such data for marketing purposes.

Every party commenting on the issue of foreign storage of domestic CPNI agrees with MCI that there should be no restrictions on foreign storage of or foreign access to "domestic" CPNI, and carriers should not be required to keep a copy of all U.S.-based customers' CPNI in the United States. Other parties agree that there is nothing in Section 222 that supports the FBI's requested restrictions. Additionally, such restrictions would not accomplish their stated goals, would impose undue burdens on carriers and might spur retaliatory measures by foreign administrations.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket 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 Docket No. 96-149

REPLY COMMENTS OF MCI TELECOMMUNICATIONS CORPORATION

MCI Telecommunications Corporation (MCI), by its undersigned counsel, submits this reply to other parties' comments filed in response to the Further Notice of Proposed Rulemaking (Further Notice) issued with the Second Report and Order in these dockets (Order).[1] The weight of the comments on the three additional issues related to the application of Section 222 of the Communications Act of 1934, added by the Telecommunications Act of 1996 (1996 Act),[2] supports MCI's views.

---

[1] Second Report and Order and Further Notice of Proposed Rulemaking, FCC 98-27 (released Feb. 26, 1998). The Second Report and Order, which comprises paragraphs 1-202 of this release, will be referred to throughout as the Order. The Further Notice is contained in paragraphs 203-10.

[2] Pub. L. No. 104-104, 110 Stat. 56 (1996), codified at 47 U.S.C. §§ 151 et seq.

In the case of the first and third issues -- whether a customer may bar her carrier's use of her customer proprietary network information (CPNI) for any marketing purposes and whether carriers should be prohibited from storing domestic CPNI abroad -- opinion in all segments of the industry is virtually unanimous that both proposed restrictions should be rejected. As to the second issue, namely, whether any additional protections are necessary for carrier proprietary information to implement Section 222(a) and (b), opinion is more varied. As explained below, MCI disagrees with those parties who cavalierly dismiss the need for any rules at all as well as those desiring excessively burdensome mechanical database restrictions.

A. Additional Customer Restrictions on CPNI Use

With one exception, every party commenting on this issue agrees that customers should not be permitted to restrict carriers' use of their CPNI to any greater extent than is already provided in Section 222. Service providers in various segments of the industry point out that such restrictions would upset the balance between privacy and competitive goals struck by Congress in Section 222 and would not do much to protect customers' interest in being left alone. Congress already determined all of the situations in which customers could and could not restrict the use or disclosure of CPNI in Section 222(c) and (d). Congress thus intended carriers to be able to use CPNI in certain

situations without customer approval.[3] As Vanguard Cellular Systems, Inc. states, the Commission found in the Order that it must interpret Section 222 "'to permit some use of CPNI for marketing purposes.'"[4] Thus, those specific provisions in Section 222 allowing the use of CPNI without customer approval override the general duty to protect CPNI in Section 222(a), which the Further Notice suggests might support a customer's total ban on the use of CPNI.[5] Any decision to change that balance should be left to Congress.[6]

Moreover, the Commission found in the Order that denying the use or disclosure of CPNI only outside the customer's total service relationship maximizes the customer's control and convenience.[7] A customer might not learn of additional services, promotions or upgrades that she might want or more economical service arrangements if the carrier were denied all use of CPNI.[8]

Customers who do not want to be subjected to marketing can be placed on "Do Not Call/Do Not Mail" lists and thereby take

---

[3] See Sprint Spectrum Comments at 1-4; Intermedia Comments at 3-5.

[4] Vanguard Comments at 3 (quoting Order at ¶ 36). See also, AT&T Comments at 4-5.

[5] See Sprint Spectrum Comments at 3; Intermedia Comments at 4-5.

[6] See SBC Comments at 8.

[7] See id. at 5-6.

[8] See Sprint Spectrum Comments at 4-5; Intermedia Comments at 5-6; Vanguard Comments at 5.

care of the problem directly.[9] As other parties point out, prohibiting any use of CPNI would not only fail to ensure customers' desires to be left alone but would likely result in greater intrusions, since carriers would not be able to target marketing appeals without the use of CPNI.[10] Without a customer's CPNI, a carrier would not be able to rationally exclude the customer from any marketing campaign, thereby subjecting the customer to more marketing.[11]

Some of the commenters also echo MCI's point that denial of any use of CPNI will have anticompetitive consequences, since it makes marketing less effective. Carriers cannot compete effectively if they cannot make a customer aware of a promotion or new features related to the customer's existing services, which, of course, requires the carrier's marketing personnel to be familiar with the customer's existing services.[12] Anything that makes marketing less effective will disproportionately burden smaller carriers, which tend to rely more than larger carriers on "surgical marketing efforts targeted to specific customer preferences," since they cannot afford mass marketing campaigns.[13] To the extent that carriers do undertake more mass

---

[9] See SBC Comments at 6; AT&T Comments at 2.

[10] See BellSouth Comments at 3 n. 13.

[11] See Bell Atlantic Comments at 2.

[12] See Intermedia Comments at 5.

[13] Vanguard Comments at 6-7.

marketing to make up for their inability to review CPNI, the additional costs of such campaigns would be passed on to consumers.[14]

The only dissenting opinion is that of the Consumers' Utility Counsel Division of the Georgia Governor's Office of Consumer Affairs (CUCD), which takes the position that because of the unusual privacy implications of telecommunications usage data, customers should be given the right to ban the use of their CPNI completely. The CUCD argues that Section 222 made no explicit provision for such a restriction because it has always been "assumed" that customers have such a right.[15]

Where a statute sets out a detailed regime such as in the case of Section 222, however, it cannot be "assumed" that an inconsistent rule survives because the statute did not address it. Any statutory scheme could be eviscerated by supposed pre-existing rights that were so obvious that they were not addressed in, but are implicit exceptions to, the statute. It would be especially destructive to invent such a rule of statutory construction in this instance, since Section 222 "established a comprehensive new framework ... which balances principles of privacy and competition in connection with the use and disclosure of CPNI and other customer information."[16] If pre-existing, but

---

[14] AT&T Comments at 6-7.

[15] CUCD Comments at 4.

[16] Order at ¶ 14.

legislatively unaddressed, privacy rights could carve out exceptions to this "comprehensive new framework," the balance created by Congress would be upset, and the "uniform national CPNI policy"[17] established by Section 222 would be thwarted.

As explained above, the initial comments demonstrate that competition would suffer if customers could prohibit all uses of CPNI. Marketing would be less effective, which would injure small carriers and tend to favor incumbents. Such a detrimental impact on competition would defeat, rather than further, the goals of Section 222. Thus, Section 222 is not really silent on the restriction in question, as the Further Notice suggests.[18] Rather, such a restriction would conflict with the statute. The CUCD's contention that the proposed restriction can be inferred from prior practice and somehow survives the statute thus must be rejected. Moreover, as also explained above, the initial comments also show that privacy interests would not be significantly advanced by such a restriction. Thus, there is no statutory basis for the restriction suggested in the Further Notice and no policy justification for such an extra-statutory right.[19]

---

[17] Id.

[18] Further Notice at ¶ 204.

[19] See AT&T Comments at 5-8.

B. Carrier Proprietary Information

1. The ILECs' Comments Underscore the Need for Clear Rules Protecting Carrier Proprietary Information

Comments on the issue of the application of Section 222(a) and (b) to carrier proprietary information range over a wide spectrum, from incumbent local exchange carriers (ILECs), dismissing the notion that any implementing rules are needed, to the Telecommunications Resellers Association (TRA), which reiterates its previous requests for certain database access restrictions. In some cases, the ILECs' assertions that no rules are needed to protect carrier proprietary information reveal the necessity of such rules. For example, BellSouth seems to believe that the issue is whether obligations should be imposed "beyond the duties set forth in the Act."[20] That formulation begs the question, since the issue is actually whether specific rules are necessary to implement the protections that are already in Section 222(a) and (b). Some of the ILECs' interpretations demonstrate a clear need for such rules.

Thus, US West seems to discern a distinction between "proprietary" information, which is covered by Section 222(a) and (b), and "competitively sensitive" information, which it claims is something else and is not covered. US West never explains the difference and, in suggesting why competitively sensitive information should not be covered by those provisions, states

---

[20] BellSouth Comments at 6.

only that what is competitively sensitive can change over time.[21]

That, of course, is true but hardly provides a justification for failing to consider the competitive impact of disclosure of information in determining whether it is proprietary. Commercial sensitivity is the touchstone for determining confidentiality under the Freedom of Information Act (FOIA),[22] which is the term used in the general provision of Section 222(a) -- i.e., carriers must protect the "confidentiality of proprietary information of, and relating to," other carriers and customers. (Emphasis added.) US West has provided no explanation as to why commercial harm should not be the criterion for determining the coverage of a statute protecting the "confidentiality of proprietary information." The changing nature of confidentiality does not make that aspect of FOIA unworkable, and it should not make the application of Section 222 unworkable.

Indeed, it is difficult to imagine what the goal of Section 222(b) -- and Section 222(a), to the extent it involves carrier information -- could possibly be other than the protection of information that is competitively sensitive. To the extent that a carrier might not be certain as to whether particular information of another carrier might qualify as proprietary under such a standard, it should always assume that the information is

---

[21] US West Comments at 7 n. 17.

[22] See National Parks and Conservation Ass'n. v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974).

proprietary until it can check with the other carrier. The fact that US West would raise such a question underscores the need for fairly detailed Commission guidance (more detailed than MCI had previously thought necessary) as to the coverage of Section 222(a) and (b). In addition to the points raised by MCI in its initial comments on this issue, it will obviously be necessary for the Commission to define "proprietary" for US West and other carriers so that they understand the competitive significance of proprietary information and its misuse.

US West also introduces the notion of "joint" proprietary information, which apparently is the data that is generated when one carrier provides a telecommunications service to another. US West asserts that such data is the joint proprietary information of both parties. It cites, as an example, data that is generated by the provision of service by a facilities-based carrier to a reseller. It states that such data is needed by the facilities-based carrier for such legitimate activities as network planning and design and financial management. Although US West seems to suggest that individual customer data would not be included within this concept, that is not clear.[23]

It is difficult to know how to respond to US West's joint proprietary data concept without more detail. Certainly, the Commission should not endorse this idea in its current embryonic state. It does not seem likely that individual customer call

---

[23] See US West Comments at 7-10.

detail data would serve any useful purpose for network planning or financial management. Moreover, it would also seem that there is a great deal of non-customer data that would be proprietary to the reseller in US West's example that US West should not be able to use for its own competitive purposes, such as the reseller's total service volume and geographic location of such services. That such data might be useful for legitimate purposes, such as network planning, should not open it up to other uses.

The Commission should make it clear that any proprietary data that one carrier derives from providing telecommunications services to another should not be used for marketing or other competitive purposes. If a carrier wishes to use such data for some purpose other than strictly providing service, it can always request permission to do so from the carrier whose proprietary information is sought.

One issue raised by some of the ILECs concerns what they view as the need for equivalence in any rules applicable to ILECs and competitive local exchange carriers (CLECs). BellSouth argues that if the Commission imposes rules on ILECs' access to information, the same rules should be imposed on the CLECs' access to the same information.[24] It is difficult to understand what issue BellSouth is trying to raise here. As MCI discussed in its initial comments, the only significant problems raising Section 222(a) and (b) issues that involve ILEC/CLEC

---

[24] BellSouth Comments at 6.

relationships have to do with the ILECs' misuse of the CLECs' proprietary information.[25] Why CLECs' access to their own information needs to be restricted is somewhat mystifying.[26]

Bell Atlantic argues that no rules implementing Section 222(b) are needed, since there is no record of the misuse of carrier proprietary information (or as Bell Atlantic mistakenly calls it, "carrier CPNI").[27] Bell Atlantic evidently has not been keeping up with MCI's filings in this proceeding and elsewhere. For example, MCI discussed Bell Atlantic's misuse of an MCI customer's billing information in an ex parte filing in this proceeding. When the MCI customer called Bell Atlantic to cancel his "Easy Voice" service, the Bell Atlantic representative referred to his MCI calling records in trying to sell him three-way calling as a way to reduce his long distance bills.[28] Those calling records are MCI's proprietary information, which Bell Atlantic may only use to provide billing services under Section 222(a).

MCI also referred, in its initial comments, to Pacific

---

[25] MCI Comments at 15-16.

[26] The Georgia CUCD, at 6-7, also addresses the supposed need to protect customer information that is being transferred from an ILEC to a CLEC that has won the customer. The CUCD does not appear to be focusing on Section 222(a) or (b) here, however; rather, its concern appears to relate solely to the CPNI protections of Section 222(c).

[27] Bell Atlantic Comments at 3.

[28] Letter from Frank W. Krogh, MCI, to William F. Caton, Acting Secretary, FCC, dated Oct. 8, 1997, at 8-9.

Bell's misuse of interexchange carrier (IXC) billing databases and discusses that issue further below.[29] Moreover, MCI filed a complaint against Pacific Bell raising its misuse of carrier proprietary information in targeting customers who have chosen another local carrier for its "winback" program.[30] There is more than enough of a record of abuse to justify the issuance of clear rules implementing Section 222(a) and (b).

2. Clear Rules Protecting Billing Data Are Needed

Sprint, like MCI, raises the issue of billing data that is disclosed by an IXC to a LEC in order for it to provide billing services to the IXC. Sprint notes that such data is protected under Section 222(a).[31] A recent decision involving this issue was recently issued in the long-running case involving Pacific Bell's "PB Awards Program," involving Pacific Bell's misuse of proprietary IXC billing data. There, the Court held that Pacific Bell's use of the IXCs' customer billing databases for its own marketing purposes misappropriated the IXCs' trade secrets under California law and granted the IXCs' motion for a permanent injunction.[32] The Court rejected the IXCs' argument, however,

---

[29] See MCI Comments at 14 & n. 10.

[30] MCI Telecommunications Corporation v. Pacific Bell, File No. E-97-11 (PacBell Winback).

[31] See Sprint Comments at 7-9.

[32] See AT&T Communications of California, Inc., et al. v. Pacific Bell, et al., No. C 96-01691 CRB (N. D. Cal. April 6, 1998), slip op. at 10-12.

that the obligation to protect carrier proprietary information in Section 222(a) also provided a basis for injuctive relief.

While MCI certainly welcomes the Court's vindication of its right to protect its trade secrets under state law, MCI also believes that the Court did not fully appreciate the intent of Section 222 and thus failed to apply the statute properly to the facts before it. Pacific Bell argued that the customer billing information contained in the databases constituted CPNI under Section 222(f)(1)(B) and that written authorizations obtained from customers required the IXCs to grant Pacific Bell access to the databases containing such information for its own use under Section 222(c)(2). The Court rejected Pacific Bell's argument as applied to the facts, but only because such authorization could only be used to compel the IXCs to turn over customers' billing information itself, not the electronic databases containing that data.

Accordingly, although Pacific Bell could not exploit Section 222(c)(2) customer authorizations to use the IXCs' billing databases, the Court concluded that the obligation to protect carrier proprietary data in Section 222(a) could not be the basis for the injunctive relief sought by the IXCs.

> Plaintiffs' electronic databases may contain customer information, but the databases themselves are not customer information. Just as section 222 does not compel plaintiffs to provide CPNI in electronic form, it does not explicitly bar Pacific Bell from accessing the data as such. Further, the court is reluctant to read such a restriction into a section which focusses on the privacy of customer information and does not

> contemplate the means of release of such data. Section 222 simply does not address this issue. Accordingly, plaintiffs may not use section 222(a) as the basis for justifying issuance of the permanent injunction.[33]

MCI respectfully disagrees and requests the Commission to correct the Court's error. In fact, Section 222(a) does address this issue. As the expert agency on this subject, the Commission is well aware that Section 222(a) and (b) protect carrier information, including information pertaining to their customers, just as Section 222(a) and (c) protect customers' information.[34] Although the IXCs' billing databases -- as opposed to the billing information contained therein -- might not be CPNI, they are certainly the IXCs' carrier proprietary information, for all of the reasons the Court found them to constitute trade secrets.[35] As such, those databases are covered by Section 222(a), and Pacific Bell had "a duty to protect the confidentiality of" such databases under that provision. Accordingly, injunctive relief should have been predicated on that ground as well, since customer approval under Section 222(c)(1) or written authorization under Section 222(c)(2) cannot allow or compel the use or disclosure of carrier proprietary information.

Moreover, even the billing information contained in the databases is carrier proprietary information, whether or not the

---

[33] Id. at 8.

[34] See Further Notice at ¶ 206.

[35] See AT&T Communications, slip op. at 10-12.

Commission determines that it is also CPNI. Customer billing information certainly meets all of the criteria for proprietary information that should be kept confidential, given its competitive sensitivity. Assuming that particular billing information could constitute both CPNI and carrier proprietary information, such dual status does not make it any less proprietary, nor should that dual status diminish the protection afforded by Section 222(a). Unlike Section 222(b), Section 222(a) is not limited to information that is "receive[d] or obtain[ed] ... from another carrier." It covers any "proprietary information of, and relating to, other telecommunication carriers," derived from any non-public source. Of course, if a particular customer's billing data were otherwise made public, it would lose its proprietary nature. Assuming, however, that certain IXC billing data were both its proprietary information and CPNI, a LEC should not be permitted to retroactively undermine the confidentiality of such data by seeking customer authorization to do so under Section 222(c)(2).

In light of Pacific Bell's conduct, and possible variations in state trade secret law, it is clear that Commission clarification is necessary in this area. MCI requests that the Commission find that billing databases provided to other carriers for the purpose of performing billing services, as well as the billing information contained therein, constitute carrier proprietary information under Section 222(a) that may not be used

for marketing or any other purposes by the carrier performing the billing service. Such status as carrier proprietary information, or the protection afforded by Section 222(a), should not be affected by the dual status of the information contained in such databases as CPNI, if any such information is also found to be CPNI. Accordingly, LECs, or any other carriers performing billing services for others, should be prohibited from soliciting customer authorizations under Section 222(c)(1) or (c)(2) to gain access to billing information or the databases containing such information, as such solicitations violate the "duty to protect the confidentiality of [such] proprietary information" mandated by Section 222(a).

Ordinarily, carriers' business self-interest in protecting customers', including carrier-customers', proprietary information in an increasingly competitive marketplace will facilitate compliance with clear rules in this area, especially where carriers find themselves on both sides of wholesale-reseller relationships.[36] That market-derived protection breaks down, however, when one party has undue bargaining power on account of its market dominance and is generally only on the underlying wholesale side of wholesale-reseller relationships. MCI is finding, for example, that some of the ILECs are demanding that MCI give up its proprietary rights in its billing information in renegotiating Billing and Collection agreements.

---

[36] See GTE Comments at 5.

Because the ILECs provide the access services for virtually all interexchange calls and are in a position to deny service for nonpayment, they are the only entities in a position to offer reasonably priced billing and collection services to the IXCs. This gives them enormous leverage in negotiating Billing and Collection agreements, which they are now beginning to exploit by demanding that MCI agree that customers may authorize the ILEC to use MCI's proprietary billing information for the ILEC's own marketing purposes. The Commission should take a firm position that ILECs and other carriers must not use their dominant market power to coerce other entities into waiving their rights under Section 222.

3. Once Clear Rules Are Established, No Additional Safeguards Should be Necessary

Once the Commission defines the coverage of Section 222(a) and (b) and states the principles implementing those protections, as MCI has requested herein and in its initial comments, there should not be a need for more detailed safeguards for carrier proprietary information. TRA emphasizes its demands for database access restrictions for resellers' customer information in the possession of underlying facilities-based carriers as well as strict liability standards and heavy financial penalties for violations of Section 222(a) and (b). TRA complains that, in spite of assurances to the contrary, database use restrictions and personnel training have not been enough to forestall abuses

of reseller customer information by facilities-based IXCs.[37]

Although MCI sympathizes with these problems, having experienced the misuse of its proprietary information by other carriers, it still believes that, once firm rules implementing Section 222(a) and (b) are in place, and their coverage is clearly defined, carriers will fall in line. The problem up to now has been the absence of a clear set of rules covering all of the relationships that give rise to abuses of carrier proprietary information. This lack of rules has required carriers to file individual complaint cases before the Commission and in federal and state courts to vindicate their rights.[38] A clear set of rules in this proceeding will be a much more effective enforcement tool than ad hoc litigation.

If the Commission believes that some additional safeguards, over and above the clear set of rules sought by MCI, are necessary for the protection of carrier proprietary information -- particularly information pertaining to resellers' customers -- the most logical approach would be to apply the same safeguards that the Commission imposed on CPNI in paragraphs 198-201 of the Order. Sprint suggested similar protections: personnel training in the application of use restrictions; required disciplinary processes; supervisory review; and an annual certificate of

---

[37] TRA Comments at 4-5, 11.

[38] See, e.g., PacBell Winback; AT&T Communications.

compliance to protect carrier proprietary information.[39] Application of the same safeguards to reseller customer data that carriers are required to apply to their own customers' CPNI would be less burdensome and confusing than a different, more stringent set of safeguards, as TRA advocates.

C. Foreign Storage of Domestic CPNI

Every party commenting on this issue agrees with MCI that there should be no restrictions on foreign storage of or foreign access to "domestic" CPNI, and carriers should not be required to keep a copy of all U.S.-based customers' CPNI in the United States, as the FBI requests. Indeed, MCI went the farthest in attempting to reach a compromise with the FBI on this issue by proposing that all domestic CPNI be readily accessible from the United States, so that it is immediately available to law enforcement personnel.

Other parties agree that nothing in Section 222 supports the FBI's requested restrictions. There is no indication of any legislative intent or language suggesting any law enforcement goals in Section 222 or any limitation on the location of CPNI, as long as it is properly protected. A statutory amendment would therefore be necessary to support these requests.[40]

---

[39] See Sprint Comments at 6-7.

[40] See GTE Comments at 7-8 & n. 9; Iridium Comments at 3-4.

At the same time, the CPNI restrictions adopted in the Order meet all of the goals of the FBI request, to the extent practicable.[41] The implementation of the protections of Section 222 in the Order restrict foreign access, or any third party access, to CPNI.[42] The location of CPNI does not affect the application of Section 222 obligations to such data.[43] Requiring domestic storage of all domestic CPNI would not provide any greater protection and would impose increased data transfer and maintenance burdens, including an increased risk of interception.[44] Indeed, hackers can access data anywhere, even in the Pentagon's secure databases.[45]

Other parties also agree with MCI that the location of data is a largely meaningless concept and has little bearing on how and when it can be used. The Internet shows that one system can be constructed of piece parts located throughout the world.[46] Parties also point out that the goals of the requested restrictions would be easily frustrated, since customers can always access foreign Internet sites or call foreign service providers, thereby making their CPNI available to foreign

---

41 Iridium Comments at 4.

42 Intermedia Comments at 10-11.

43 GTE Comments at 8.

44 Iridium Comments at 4-5.

45 GTE Comments at 8 & n. 10.

46 See id. at 7.

entities, irrespective of any foreign storage or access restrictions.[47]

As illustrated by Ameritech, carriers often contract with foreign firms for information systems development and production support. Such activities might involve software maintenance and troubleshooting in connection with databases containing CPNI and in connection with billing systems. Such foreign contractors thus would have incidental access to CPNI. As Ameritech and others point out, however, carriers have a substantial business interest in protecting CPNI from misuse.[48] Ameritech states that it contracts only with reputable foreign firms and has established several layers of network security to ensure that its CPNI and other data remain fully protected.[49]

Omnipoint suggests that, if the Commission is concerned about the security of CPNI stored or accessed abroad, it should require strict database security measures, rather than locational restrictions. Omnipoint also warns that if the Commission does impose such data storage restrictions, foreign administrations may retaliate, leading to roadblocks in the way of the developing

---

[47] Intermedia Comments at 11. As Omnipoint notes, at 7, n. 5, there also appears to be some tension among the FBI's stated goals, since its concern for privacy is overridden by its desire for access to all domestic or U.S.-based customer CPNI.

[48] Omnipoint Comments at 9 & n. 8.

[49] Ameritech Comments at 1-2.