Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	**)**	
	)	
Implementation of the	**)**	**CC Docket No. 96-115**
Telecommunications Act of 1996:	**)**	
	)	
Telecommunications Carriers'	**)**	
Use of Customer	**)**	
Proprietary Network Information	**)**	

REPLY COMMENTS OF
THE ELECTRONIC PRIVACY INFORMATION CENTER

November 21, 2002

Pursuant to the Commission's request for public comment[1] and notice[2] and in accordance with the Commission's rules[3] the Electronic Privacy Information Center (EPIC) submits the following reply comments regarding the regulation of foreign storage and access to domestic customer proprietary network information (CPNI).

EPIC urges the Commission to meet its fundamental responsibility to protect the privacy rights of those using the nation's telecommunications system by implementing regulatory safeguards towards the foreign storage of and access to the CPNI of United States customers who subscribe to domestic telecommunications services, pursuant to section 222 of the Communications Act of 1996. In promulgating section 222, Congress addressed a

[1] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002) (*Third CPNI Order*).

[2] 67 Fed. Reg. 59236 (Sept. 20, 2002)

[3] 47 C.F.R. § 1.415.

particular privacy concern: "protecting the confidentiality of proprietary information."[4] EPIC opposes the request of the Federal Bureau of Investigation (the Bureau) to mandate the limited retention of CPNI data. These reply comments address the danger of adopting a CPNI retention regime, and requests that the Commission carefully balance the privacy rights of United States telecommunications customers with the needs of law enforcement. Minimizing the collection of CPNI is one of the best privacy safeguards available, and we ask the Commission to proceed with this in mind.

These reply comments also incorporate by reference our previous comments, urging the Commission to adopt safeguards in order to protect CPNI when a carrier goes out of business or seeks to sell CPNI as a business asset.

I. Mandating CPNI Data Retention Raises Serious Privacy Risks

These comments are in response to the Federal Bureau of Investigation's (the Bureau's) July 1997 ex parte letter to the Commission, in which the Bureau asked the Commission to implement a limited data retention scheme related to the foreign access and storage of domestic CPNI.[5] Specifically, the Bureau requested the Commission to promulgate regulations requiring domestic carriers to retain copies of CPNI in the United States, in circumstances under which carriers are permitted by current regulations to store domestic CPNI in foreign countries. In addition, the Bureau asked the Commission to require carriers to retain copies in the United States of the CPNI of domestic customers using non-domestic telecommunications services.[6] We agree with the Bureau that it is necessary to

[4] 47 United StatesC. § 222(a).

[5] *See* Letter from John F. Lewis, Jr, Federal Bureau of Investigation, to William F. Caton, Acting Secretary, Federal Communications Commission, CC Docket No. 96-115 (filed July 8, 1997) (the Bureau Letter).

[6] *Id.* at 5, n. 8.

limit foreign retention of CPNI, and agree that foreign storage of domestic CPNI should be permitted only upon informed written customer approval.[7] However, there should not be a United States data retention scheme, as any data retention regulations—even the limited regulations requested by the Bureau—would be a move toward outright CPNI data retention.

Any federal CPNI data retention would be a blow to the privacy expectations of telecommunications customers. The Bureau proposal focuses on the purported needs of law enforcement, and while we understand that law enforcement needs to be able to effectuate lawful investigations of criminal activity, a regulatory regime that establishes the retention of CPNI data on all customers simply goes too far, and could lead to the permanent surveillance of all citizens. Careful distinctions must be drawn between data retention—the routine storage by all covered providers of large categories of data for a specified period—and data preservation—the storage for a specified period of time of specific data related to a particular criminal investigation of a specified individual, accessed according to legal and constitutional safeguards and subject to judicial review.[8] Only the latter is permitted under United States law. Furthermore, any data retained under law enforcement data retention schemes in the United States is subject to statutory minimization requirements, limiting the data collected and the uses to which such information can be put.[9] It would therefore be inconsistent with other surveillance systems if the Bureau proposals were adopted by the Commission, as the data retention scheme the Bureau requests does not discriminate between innocent citizens and those engaged in or suspected of criminal activities.

---

[7] *See id.* at 2 (noting that, "the prospect of direct foreign access to the CPNI of United States Domestic Customers would have the unintended effect of seriously undermining, legally and practically,…privacy-based protections that are afforded to CPNI under international and bilateral treaties...and other international legal assistance procedures."); *see also* Third CPNI Order, at ¶ 144.

[8] *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 USC § 2510 *et seq.*

[9] *See id.* § 2518(5).

Requiring CPNI data retention as part of the 1996 act would be an extraordinary regulatory action by the Commission. Telecommunications consumers have a legitimate and significant expectation of privacy with respect to sensitive personal information such as which telephone numbers they have dialed.[10] In its report on the legislation that was eventually enacted as the Telecommunications Act of 1996, the House Commerce Committee explained that the purpose of the protections contained in section 222 of the 1996 Act was to balance "the need for customers to be sure that personal information that carriers may collect is not misused."[11]

Congress has recognized the importance of a citizen's privacy interest by enacting an elaborate statutory scheme to protect the privacy of telephone communications,[12] and has specifically prohibited the use of pen registers without a court order.[13] Thus, Congress has determined that people have a legitimate expectation of privacy with respect to the phone numbers they dial and has decided that this information is so sensitive that it has developed an entire statutory scheme governing law enforcement's ability to collect such data. Indeed, the Bureau proposal appropriately recognizes the sensitive nature of CPNI,[14] as the Commission itself has previously done on numerous occasions.[15] With this in mind, we believe that the adoption of any data retention system would be beyond the scope of the

---

[10] *See id.*

[11] H.R. Rep. No. 104-204, pt. 1, at 90 (1995).

[12] *See* 18 U.S.C. §§ 2510-2522 (2000).

[13] *See* 18 U.S.C. § 3121 (2000).

[14] *See* the Bureau Letter at 3 (noting that CPNI "comprehends detailed and sensitive proprietary information about a customer's use of network services; his/her calling patterns; social, medical, organizational, and political telephone contacts; and much more.")

[15] *See, e.g*, Third CPNI Order at 25 ("the government's interest in protecting consumers from unexpected and unwanted disclosure of their personal information in CPNI is a significant one.")

Commission's authority, and should be properly left to Congress to debate. In addition, we note that the purpose of section 222 is the protection of customers' privacy rights, not the authorization or assistance of law enforcement in information collection.

The United States government has always vehemently opposed data retention.[16] While many providers routinely retain limited traffic data for billing and other business purposes on a short-term basis, there are currently no government-imposed data retention requirements in any of the major industrialized countries.[17] One critical concern underlying any Commission mandate of CPNI data retention is the potential for the data to be misused by law enforcement, for example, the risk that law enforcement authorities might use such authority to conduct broad and arbitrary "fishing expeditions."

We also note that the practical realities do not support the Bureau's assertions that absent a CPNI data retention mandate, law enforcement's power to conduct a lawful criminal investigation will be inhibited. Carriers faced with a subpoena generally go to great lengths to provide law enforcement with the information needed to effectuate a lawful criminal investigation, and the Bureau fails to present evidence to the contrary. Further, section 222 of the 1996 Act recognizes that disclosure to law enforcement will occur "as required by law."[18] Finally, while the Bureau wants the Commission to regulate the storage of CPNI, we

---

[16] Comments of the United States on the European Commission Communication on Combating Computer Crime, presented at the European Union Forum on Cybercrime at Brussels, (Nov. 27, 2001) at <http://www.usdoj.gov/criminal/cybercrime/intl/MMR_Nov01_Forum.doc> ("The United States has serious reservations about broad mandatory data retention regimes and has articulated these reservations in multilateral fora such as the Council of Europe Cybercrime Convention negotiations and the G8.")

[17] *See*, *e.g.*, Council of Europe, Convention on Cybercrime, ETS no. 185, *opened for signature* Nov. 23, 2001, available at <http://conventions.coe.int/Treaty/EN/cadreprincipal.htm> (permitting only preservation, not retention, of traffic data). Although the Convention is not yet in force, as it has not yet been ratified by five countries, the United States signed the Convention in November of 2001.

[18] 47 U.S.C. § 222(c) (1).

note that CPNI data retention is not mandated under the Patriot Act,[19] presumably because neither the Bureau nor the Department of Justice thought it necessary to their law enforcement capabilities.[20]

Additionally, CPNI data retention has the real possibility of threatening users' confidence in the telecommunications network as a whole. Technology has given consumers the ability to conduct many activities over the phone (check payments, make bank account balance inquiries, etc.), and a data retention regulation could seriously erode consumer confidence in the telecommunications network. Furthermore, as has been discussed in length in other comments submitted in this proceeding, the costs for telecommunications carriers of the proposed data retention requirement could be staggering.[21]

While we must be mindful of law enforcement authorities' legitimate need to combat and prevent crime, the adoption of a regulation that so easily allows the retention and surveillance of domestic and non-domestic telecommunications traffic undermines fundamental principles of privacy and democracy. We respectfully urge the Commission to reject the Bureau's proposed data retention scheme.

II. CPNI Must be Protected When a Carrier Goes Out of Business

We again urge the Commission to adopt an opt-in requirement for a carrier's use of CPNI when a carrier goes out of business or seeks to sell CPNI as a business asset. While we believe that an opt-out approach to the use of CPNI in a carrier transfer is less preferable from a privacy perspective than an opt-in approach, we are not asking the Commission to "do

---

[19] USA-PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

[20] *See* http://www.epic.org/privacy/terrorism/hr3162.html.

[21] *See e.g*, Comments of Nextel, (CC Docket No. 96-115) at 2-3; Comments of Verizon, (CC Docket No. 96-115) at 3-4.

an abrupt about-face," as AT&T has suggested in its reply comments.[22] Despite AT&T's assertion to the contrary, EPIC's comments do not argue that section 222(c)(1) approval *requires* opt-in approval.[23] Rather, EPIC's comments acknowledge and operate within the CPNI sharing approach the Commission adopted in the *Third Report and Order*, to allow for opt-out for carriers' affiliated parties and opt-in when the carrier is "engaging in transactions with unaffiliated third parties or affiliates not providing communications services."[24] Our argument is simply that commercial use of CPNI transferred from an exiting carrier to an acquiring carrier should be opt-in because the safeguards the Commission has relied on regarding a carrier's incentive not to abuse CPNI may not always be present when a customer is transferred to another carrier and lacks the competitive choice to choose a different carrier.[25] Practically, this safeguard may only be in jeopardy of disappearing when the transferring carrier is a Local Exchange Carrier (LEC), which we clearly note in our comments.[26]

III. Conclusion

For the foregoing reasons, the Commission should (1) refrain from adopting any data retention regulations with regard to the foreign storage of or access to CPNI, (2) adopt regulatory safeguards to protect CPNI when a carrier goes out of business or seeks to sell

---

[22] AT&T Reply Comments at 5.

[23] *Id.* The portion of the EPIC comments AT&T refers to was simply intended by EPIC to illustrate that opt-in approval is preferable, from a privacy perspective, to an opt-out approach, because opt-in requires an affirmative "approval" from the customer. If AT&T had understood this point, they may not have concluded that, "None of EPIC's contentions…has any basis in law or logic." AT&T at 4.

[24] EPIC Comments at 2.

[25] *Id.* at 4-5.

[26] *Id.* at 5.

CPNI as an asset, and (3) require carriers to provide adequate notice to subscribers affected by a CPNI transfer and get adequate customer consent for the further use of subscribers' CPNI.

Respectfully submitted,

Mikal J. Condon
Staff Counsel
Electronic Privacy Information Center