

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996:)	CC Docket No. 96-115
)	WC Docket No. 04-36
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information)	RM-11277
)	
IP-Enabled Services)	
)	

**REPLY COMMENTS OF THE UNITED STATES
DEPARTMENTS OF JUSTICE AND HOMELAND SECURITY**

I. Introduction

The United States Department of Justice (“DOJ”)¹ and the United States Department of Homeland Security (“DHS”)² (collectively, “the Departments”) hereby submit these reply comments on the Commission’s *Further Notice of Proposed Rulemaking* (the “*Further Notice*”) in the above-captioned docket.³ The Departments submit these reply comments in order to urge that the Commission not adopt rules requiring the destruction or de-identification of customer proprietary network information (“CPNI”); such rules would prevent lawful access to this important information that helps

¹ DOJ includes its constituent components, including the Federal Bureau of Investigation (“FBI”) and the Drug Enforcement Administration (“DEA”).

² DHS includes its constituent law enforcement components, including the United States Secret Service (“USSS”) and Immigration and Customs Enforcement (“ICE”).

³ *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115, WC Docket No. 04-36, FCC 07-22 (rel. Apr. 2, 2007).

solve crimes, prevent terrorist attacks, and safeguard national security. These comments are intended to supplement the views expressed by the Departments in their earlier filings in this docket.⁴

In an initial *Notice of Proposed Rulemaking* (the “*Notice*”) released in 2006,⁵ the Commission requested comment on “whether CPNI records should eventually be deleted, and if so, how long such records should be kept.”⁶ In exploring the potential negative consequences of a record destruction mandate, the Commission asked whether “deleting CPNI or removing personal identification [would] conflict with other priorities, such as . . . law enforcement.”⁷

Following the *Notice*, the Commission adopted new rules intended to increase safeguards for CPNI.⁸ In addition to those new rules, in the *Further Notice*, the Commission again asked whether, “in light of the [new rules relating to CPNI security] and the recent enactment of criminal penalties against pretexters, [it] should adopt rules that require carriers to limit data retention.”⁹

⁴ See Comments of the United States Departments of Justice and Homeland Security, *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, CC Docket No. 96-115 (filed Apr. 28, 2006) (the “2006 Comments”).

⁵ *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, Notice of Proposed Rulemaking, CC Docket No. 96-115, RM-11277, FCC 06-10 (rel. Feb. 14, 2006).

⁶ *Notice* ¶ 20.

⁷ *Id.*

⁸ See generally *Order and Further Notice*.

⁹ *Id.* ¶ 71.

II. The Commission Should Not Adopt Any Additional Rules Requiring the Destruction or De-identification of CPNI.

The Departments have considered the impact of the new Commission rules and of Congress's enactment of the Telephone Records and Privacy Protection Act of 2006,¹⁰ and we reaffirm that that the Commission should not adopt rules that require carriers to limit data retention.¹¹ In fact, because the Commission has strengthened its rules governing carriers' handling of CPNI, there is even less reason to require carriers to destroy or de-identify CPNI after a period of time. On the other hand, the reasons for not adopting such a requirement are as strong as ever. CPNI remains an invaluable investigative resource for law enforcement, the mandatory destruction or de-identification of which would severely impact the Departments' ability to protect national security and public safety.

As stated by the Departments in their comments to the *Notice*, a mandatory destruction requirement is unnecessary and inappropriate. The benefit of such a requirement would be minimal, especially in light of the new rules adopted by the Commission (e.g., the general prohibition on releasing CPNI based on customer-initiated telephone contact, the requirement to password protect online access to CPNI, and new notification requirements for certain account changes), which will help to accomplish the goal of protecting CPNI in carriers' possession.

On the other hand, the harms resulting from such a requirement would be substantial. As the Departments have repeatedly stated, carriers' inability to produce records in response to lawful authority (e.g., based upon claims that records for "flat rate"

¹⁰ See 18 U.S.C. § 1039.

¹¹ See 2006 Comments.

services are not “toll records,” and thus not required to be maintained) has had a significant negative impact on national security and public safety. Any new rules that would mandate the destruction or de-identification of CPNI would also preclude lawfully authorized access.

As previously noted by the Departments,¹² CPNI has many other valid uses, such as fraud prevention, handling of billing disputes, marketing, customer service, and the protection of a carrier’s own network. Indeed, for a variety of the above-stated reasons, the overwhelming majority of comments in the instant proceeding have urged the Commission not to adopt any new rules requiring data destruction or de-identification.¹³ As the FBI has previously advised, lawfully-obtained CPNI is used in virtually every federal, state, and local investigation of consequence.¹⁴ Such CPNI is critically important not only in solving crimes but also in preventing crimes and even saving lives.¹⁵ The same is true in the national security and espionage contexts, where lawfully-obtained CPNI has greatly assisted law enforcement and national security agencies in preventing terrorist acts and acts of espionage.¹⁶ Thus, a mandatory destruction requirement – particularly one tied to a point in time completely unrelated to these purposes, e.g., when

¹² *Id.*

¹³ *See, e.g.*, Comments of AT&T, Comcast, Qwest, Time Warner, T-Mobile, Sprint-Nextel, United States Telecom Association, and Verizon.

¹⁴ *See* Comments of the Federal Bureau of Investigation, *in re Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115 (filed Jul. 9, 1997) at 5.

¹⁵ *Id.*

¹⁶ *Id.* at 6-7.

records cease to be “needed for billing or dispute purposes” – would inevitably result in the loss of critical information to many such investigations and cases.

Accordingly, the Departments urge the Commission not to adopt any new rules that would mandate the destruction or de-identification of CPNI.

III. Conclusion

For the above-stated reasons, and for those stated in the 2006 Comments, the Departments reiterate their recommendation that the Commission not adopt rules mandating the destruction or de-identification of CPNI, a vitally important investigative resource for protecting public safety and national security. Such a rule would hinder the Departments’ ability to carry out their respective public safety and national security responsibilities.

Dated: August 7, 2007

Respectfully submitted,

THE UNITED STATES DEPARTMENT OF JUSTICE

/s/ Sigal P. Mandelker

Sigal P. Mandelker
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Room 2113
Washington, D.C. 20530
(202) 305-8319

and

/s/ Elaine N. Lammert

Elaine N. Lammert
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
United States Department of Justice
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.
Room 7435
Washington, D.C. 20535
(202) 324-1530

and

/s/ Timothy D. Wing

Timothy D. Wing
Assistant Deputy Chief Counsel
Office of Chief Counsel
Drug Enforcement Administration
United States Department of Justice
Washington, D.C. 20537
(202) 307-8020

and

THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY

/s/ Stewart A. Baker

Stewart A. Baker
Assistant Secretary for Policy
United States Department of Homeland Security
3801 Nebraska Avenue, N.W.
Washington, D.C. 20528
(202) 282-8030