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	)	
	)	RM-11277
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	

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 comments on the Commission's *Notice of Proposed Rulemaking* ("*Notice*") in the above-captioned docket.[3] The

---

[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 and Immigration and Customs Enforcement.

[3] *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*

Departments submit these comments to assist the Commission in its development of further rules protecting the privacy of customer proprietary network information ("CPNI") without sacrificing lawful access to important information that helps solve crimes, prevent terrorist attacks, and safeguard our national security.

This proceeding was initiated primarily in response to a Petition for Rulemaking filed by the Electronic Privacy Information Center ("EPIC") that raised concerns about the sufficiency of carrier practices related to CPNI.[4] Among other things, EPIC recommended that the Commission adopt rules requiring that call detail records be destroyed when they are no longer needed for billing or dispute purposes or, in the alternative, requiring carriers to "de-identify" identification data from the transactional records.[5] In the *Notice*, the Commission requested comment on "whether CPNI records should eventually be deleted, and if so, for how long such records should be kept."[6] In exploring the potential negative consequences of a record destruction mandate, the Commission has asked whether "deleting CPNI or

---

Proprietary Network Information, Notice of Proposed Rulemaking, CC Docket No. 96-115, RM-11277, FCC 06-10 (rel. Feb. 14, 2006).

[4] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance the Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) ("EPIC Petition").

[5] *See* EPIC Petition at 11-12.

[6] *Notice* ¶ 20.

removing personal identification conflict with other priorities, such as . . . law enforcement."[7]

The answer to the above question is an unequivocal "yes," and we urge the Commission to explore ways to resolve the issues EPIC has raised in ways that preserve lawful access to communications records and other CPNI. For law enforcement, such CPNI is an invaluable investigative resource, the mandatory destruction of which would severely impact the Departments' ability to protect national security and public safety. As reflected in prior Commission filings on CPNI issues, the Departments fully support the Commission's goal of protecting the privacy and security of CPNI through rules prescribing the proper use and handling of that very sensitive information.[8] But while measures are needed to prevent *improper* access to this sensitive information, such measures should not work to limit properly authorized officials from lawfully accessing CPNI in order to solve and prevent crimes and to protect national security and public safety. In crafting

---

[7] *Id.*

[8] *See, e.g.*, Reply Comments of the United States Department of Justice and the Federal Bureau of Investigation, *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Third Further Notice of Proposed Rulemaking, CC Docket No. 96-115 at 4, n. 8 (filed Nov. 19, 2002); Comments of the Federal Bureau of Investigation, *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 Jul. 9, 1997); Comments of the Federal Bureau of Investigation, *In the Matter of 1998 Biennial Regulatory Review of International Common Carrier Regulations*, Notice of Proposed Rulemaking, IB Docket No. 98-118 (filed Aug. 13, 1998).

any solution to the problems raised by the EPIC Petition, the Departments urge the Commission to reject imposing a mandate to destroy invaluable information used by the Departments in many of their most important investigations.[9]

II. The Commission's Rules Should Focus On Proper Security For All CPNI, Not On A Mandatory Destruction Requirement That Fails To Protect Some Records And Frustrates Lawful Access To Others.

A mandatory destruction requirement is the wrong approach for two reasons. First, because not all records would be immediately destroyed, efforts are better focused on proper security for the records while they are maintained. Second, and more importantly, the inability to produce records in response to lawful authority would have a significant negative impact on national security and public safety. Accordingly, the Departments urge the Commission to focus on security measures to protect all CPNI against *unauthorized* access rather than a rule that would also preclude lawfully authorized access.

---

[9] EPIC's alternative recommendation – record de-identification – is also an unworkable option with respect to law enforcement's lawful access to such records. De-identification would separate the data that identify a particular caller or recipient (e.g., name, address, numbers called, etc.) from the general transaction records. Because the data that identifies a particular caller or recipient is often the critical portion of the call record for investigatory purposes, an irreversible de-identification approach would undermine the usefulness of the information provided pursuant to legal access. Accordingly, mandating the de-identification of such records would be the equivalent of mandating their destruction for law enforcement investigatory purposes. A de-identification approach should therefore be rejected for the same reasons.

As the Commission recognized when it explicitly asked about the impact of EPIC's records destruction proposal on other concerns, CPNI has other valid uses, such as fraud prevention and the protection of a carrier's own network.[10] Another legally authorized use is to investigate crime and protect national security and public safety. The Departments seek lawful access to CPNI in connection with investigations of all kinds – from child pornography to illegal drug trafficking, counter-intelligence, espionage, and more. In fact, as the FBI has previously advised the Commission, lawfully-obtained CPNI is used in virtually every federal, state, and local investigation of consequence.[11] Such CPNI is critically important not only in solving crimes but also in preventing crimes and even saving lives.[12] As discussed below, the same is true in the national security and espionage contexts, where lawfully-obtained CPNI has enabled law enforcement and national security agencies to prevent terrorist acts and acts of espionage.[13] The courts have likewise long recognized the importance of telephone records to the administration of justice – both to law enforcement in the investigation

---

10 The Departments submit that, beyond any retention period required by law, carriers should be free to retain voluntarily CPNI for other legal and appropriate purposes, such as protecting their networks and mitigating fraud.

11 *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.

12 *Id.*

13 *Id.* at 6-7.

and prosecution of serious offenses, such as illegal drug trafficking and organized crime, and to defendants in establishing an alibi defense.[14] Thus, a mandatory destruction requirement – particularly one tied to a point in time completely unrelated to these purposes, i.e., when 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.[15]

Moreover, a mandatory records destruction regime would be particularly inappropriate, because it could hinder efforts to counter international terrorism. Lawful access to communications records is a critical tool in the fight against global terrorism. Such records, when combined with other investigative information, can be used to establish the movements and identities of known and suspected terrorists. Mobile phone records, for example, were instrumental in tracking down the perpetrators of the Madrid bombings that killed 191 and injured approximately 1,800 people

---

[14] *See, e.g. U.S. v. Hanardt*, 173 F. Supp. 2d 801 (N.D. Ill. 2001) (phone records helped establish defendant's "long-time connection to Chicago organized crime"); *U.S. v. Scala*, 388 F. Supp. 2d 396 (S.D.N.Y. 2005) (cellular phone records showed numerous calls between defendant and known organized crime figures); *Reporters Committee for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1036-37 (D.C. Cir. 1978) (noting that "toll-billing records have become an invaluable law enforcement aid" and that information from toll-billing records has been used by state and federal law enforcement officials in criminal investigations and prosecutions for over 50 years). *See also Butler v. State*, 716 S.W.2d 48 (Tex. Crim. App. 1986) (telephone toll record was the key factor in establishing alibi defense).

[15] We note that any mandatory data destruction requirement would also largely negate the utility of the existing data preservation scheme under 18 U.S.C. § 2703(f); if the data relating to a specific investigation has been destroyed, there will be nothing for providers to preserve in response to a request from law enforcement.

on March 11, 2004.[16] The National Commission on Terrorist Attacks Upon the United States also relied on telephone records in numerous instances to establish the movements and contacts of the 9/11 hijackers before their terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001.[17]

It is precisely these kinds of concerns that motivated the Commission to abandon its former rules requiring data destruction and adopt its current rules that require the maintenance of certain categories of CPNI. Prior to 1986, the Commission's Part 42 carrier record-keeping rules required, among other things, that carriers (1) macerate or destroy the legibility of records the contents of which are forbidden by law to be divulged to unauthorized persons,[18] and (2) retain telephone toll records for six months.[19] As part of a comprehensive review by the Commission of its Part 42 rules and in response to a related request by DOJ to extend the telephone toll record retention

---

16 *See* "Madrid Bombing 'Manager' in Court," BBC News (June 3, 2005), viewable at http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/england/berkshire/4607175.stm (telephone records used to show bombing "manager" had been in contact with people involved in the Madrid bombings).

17 *See The 9/11 Commission Report* (released Jul. 22, 2004) at 217, 515 n.26, 522 n.68.

18 *See In the Matter of Revision of Part 42, Preservation of Records of Communication Common Carriers*, Notice of Proposed Rulemaking, 1985 FCC LEXIS 2945 ¶¶ 13, 23 (1985) ("*Part 42 NPRM*") (discussing the record destruction requirement contained in the then-current version of Section 42.6 of the Commissions rules, 47 C.F.R. § 42.6 (Destruction of Records) (1985)).

19 *See Part 42 NPRM* ¶ 18 (discussing the toll record retention requirement contained in the then-current version of Section 42.9 of the Commissions rules, 47 C.F.R. § 42.9 (List of Records) (1985)).

period specified therein, the Commission (among other things) eliminated the records destruction requirement and extended the toll record retention period to 18 months.[20] In granting DOJ's request, the Commission specifically recognized that an extension of the retention period was warranted in order to "support successful investigations and prosecutions . . . ."[21] In extending the retention period, the Commission – with DOJ's input – refined and narrowed the specific information that law enforcement stated it would need to support its investigative efforts at that time.[22]

In addition to the Commission's own prior acknowledgment of the difficulties a destruction requirement presents, recent experience in other countries further highlights the problems created by such requirements. The establishment of a data destruction regime in the European Union ("EU") a number of years ago has been found to be incompatible with protection of public safety and national security. In response, the EU recently adopted a

---

[20] *See In the Matter of Revision of Part 42, Preservation of Records of Communication Common Carriers*, Report and Order, 1986 WL 290829, 60 Rad. Reg. 2d (P&F) 1529 ¶¶ 4, 23-27, 38, 41-42 (1986) ("*Part 42 Order*"). DOJ's request was supported by the Advisory Committee for United States Attorneys, the FBI, the Bureau of Alcohol, Tobacco and Firearms, the U.S. Postal Service, and the Immigration and Naturalization Service. *See Part 42 NPRM* ¶ 18.

[21] *See Part 42 Order* ¶ 41.

[22] *See Part 42 Order* ¶ 43. The specific information that DOJ indicated law enforcement would need at that time includes the name, address, and telephone number of the caller; telephone number called; the date, time, and length of the call; and automatic message accounting tapes. *Id.* The list of law enforcement-required information was incorporated into Section 42.6 of the Commission's rules and remains listed therein today. *See* 47 C.F.R. § 42.6 (2006).

Directive – binding on all of its member countries – that will have the effect of mandating all "providers of publicly available communications services" to store and retain communications data for up to two years.[23] In acknowledging the need for data retention requirements, the EU Parliament and Council recognized that:

> retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive.[24]

EPIC's recommended data destruction mandate would cause the Commission to regress to a course it has long since rejected. If anything, reliance on telephone call records as an investigative resource to protect public safety and national security has only increased and become more critical in the almost twenty years since the Commission revised Section 42.6 of its rules to extend the telephone records retention period.[25]

---

[23] *See* Council Directive, 2006/24/EC, 2006 O.J. (L 105) 54, Article 6 ("Directive"), viewable at http://europa.eu.int/eur-lex/lex/JOHtml.do?uri=OJ:L:2006:105:som:en:html. *See also* Miriam H. Wugmeister and Karin Retzer, *Data Retention – Implications for Business*, 7 NO. 2 Privacy & Info. L. Rep. 7 (2006).

[24] *See* Directive at 4 ¶ 9.

[25] Moreover, as the Commission notes in the *Notice*, carriers themselves have already expressed concern about potential conflicts with Commission rules that require that call records and other CPNI be kept for at least a

Notwithstanding this increased reliance on such records, however, the efficacy of the Commission's current Section 42.6 requirement to meet law enforcement needs has been significantly eroded.

While the risks are clear and many, the benefit from a mandatory destruction requirement is largely unclear and certainly limited. The mandatory destruction of some CPNI does nothing to address a significant portion of CPNI, specifically information needed for billing disputes, which will still need to be secured.[26] In fact, the material retained will most likely be the most recent records and hence possibly the most useful for data brokers. Rather than expending effort on promulgating rules with significant omissions, the Commission should instead focus its efforts, and those of carriers, on appropriate security measures that ensure that any access to such records is done only with valid legal authority. As the Department of Justice has urged the Commission for years, one large step in that direction would be to require that CPNI of U.S. customers of domestic services be stored exclusively within the United States.[27]

---

minimum period of time. *See Notice* ¶ 20 (noting carriers' comments that destroying records might conflict with the Commission's Part 42 record-keeping rules, 47 C.F.R. §42.01-11).

[26] The statute of limitations in Section 415 of the Communications Act for billing disputes is two years. 47 U.S.C. § 415. The nature of Section 415 necessarily compels carriers to maintain all potentially relevant documents needed in connection with resolving actions concerning recovery of lawful charges or damages.

[27] *See* Reply Comments of the United States Department of Justice and the Federal Bureau of Investigation, *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of*

In opposing and pointing out the inadequacies of a data destruction regime, the Departments do not thereby imply that the current CPNI rules are adequate effectively to meet law enforcement's needs or protect public safety and national security. As noted above, the Departments have previously asked the Commission to strengthen the security of these records in a number of ways.[28] Further, developments in the world and in the communications marketplace since the Commission's last examination of these rules have highlighted the limited scope of the Commission's rules. Today, many modern communications service providers maintain sensitive records about their customers' private communications, yet these new carriers have not been made subject to the rules that have traditionally governed CPNI.[29] In addition, as carriers covered by the Commission's existing rules have increasingly moved away from classic billing models, in which charges are itemized and billed by type of service, to non-measured, bundled, and flat-rate service plans, some carriers have claimed that call records under such new plans are not covered by Section 42.6 because they

---

Customer Proprietary Network Information and Other Customer Information, Third Further Notice of Proposed Rulemaking, CC Docket No. 96-115 at 4, n.8 (filed Nov. 19, 2002).

[28] *See id. See also* Comments of the United States Department of Justice, *In the Matter of IP-Enabled Services*, Notice of Proposed Rulemaking, WC Docket No. 04-36 (filed May 28, 2004).

[29] *Id.* To the extent that the *Notice* requests comment on whether any requirements that the Commission might adopt in the present rulemaking should extend to VoIP or other IP-enabled service providers, the Departments refer to their May 28, 2004 comments on this subject.

are not "toll records." Therefore, these carriers have argued that no records need be retained. This has significantly diminished the availability of call records that were historically made available to law enforcement, pursuant to lawful process, as traditional "billing records" under the Commission's rules. While it is recognized that changes in the communications industry over the past decade have resulted in changes in the record retention practices of such providers, it must also be acknowledged that the nature and immediacy of the threat confronting public safety and national security has significantly changed and evolved such that the need lawfully to access these critical records has increased, not diminished.

As a consequence of these changes, the Departments believe it is necessary to re-examine the Commission's existing rules which no longer fulfill critical public safety or national security needs in three key respects: 1) the scope of carriers and providers covered; 2) the scope of information and records covered, and; 3) the duration of retention of information and records.[30]

The critical role that communications records play in the Departments' most important investigations and the serious consequences for public safety and national security which result from the unavailability of such records

---

[30] It should be noted that whereas the Commission has limited the retention period for toll records to 18 months, the statute of limitations for many federal felony crimes is five years, during which time law enforcement needs for relevant evidence continue. The Commission should explore, with further input from law enforcement, the degree to which the existing 18-month rule should be extended.

cannot be understated. The Attorney General recently underscored this point when he noted that the investigation and prosecution of child predators depends critically on the availability of evidence that is often in the hands of Internet service providers. He observed that this evidence will be available to law enforcement only if the providers retain the records for a reasonable amount of time. Consequently, the Attorney General asked experts at the Department of Justice to examine how the failure of some Internet service providers to keep such records has hampered the Department's efforts to investigate and prosecute child predators.[31] In recognition of the importance of this issue, the Departments each will be evaluating how the availability of different categories of data held by different types of modern communications carriers impacts the Departments' respective missions. In addition, the Attorney General has pledged to reach out personally to leading service providers and other industry leaders to solicit their input and assistance. As these efforts develop, the Departments expect to have further views on how long data should be held, what data should be retained, and which carriers should have such obligations.

III. Any Notice Requirement Adopted by the Commission Should Include A Provision Requiring Advance Notice to Law Enforcement and, Where Appropriate, Delayed Notice To The Consumer.

---

[31] *See* Prepared Remarks of Attorney General Alberto R. Gonzales at the National Center for Missing and Exploited Children (NCMEC) in Alexandria, Virginia, on April 20, 2006, available at http://www.usdoj.gov/ag/speeches/2006/ag_speech_060420.html.

The EPIC Petition also suggested that carriers should be required to notify affected customers when there has been an improper disclosure of CPNI.[32] In the *Notice*, the Commission went further and asked for comments regarding "the costs and benefits of routinely notifying customers after any release of their CPNI."[33] While the Departments strongly support prompt victim notification in the case of security breaches, we believe any rule requiring such notification should also require that carriers first notify law enforcement authorities and, where appropriate, allow law enforcement to request a reasonable delay in notification to the consumer where such notification might harm related law enforcement investigative efforts. In addition, any requirement that customers routinely be notified of disclosures of their CPNI should make clear that it does not alter the rules already established by Congress regarding the circumstances under which a customer must be notified of law enforcement access to customer records.

Requiring advance notice to law enforcement of security breaches, together with the option of delaying consumer notification, can serve several important goals. First, anecdotal evidence suggests that many CPNI breaches go unreported to law enforcement. Only by prompt investigation of such breaches can the offenders be identified and punished. Thus, required reporting to law enforcement will deter further breaches of CPNI security. Second, where deemed necessary by law enforcement, a reasonable delay can

---

[32] *See* EPIC Petition at 11.

help preserve evidence critical to the investigation of misappropriation of CPNI. If a carrier suffering an intrusion or theft must immediately announce the security breach to affected customers and to the public, the persons responsible may be tipped off that law enforcement is investigating their crime. Criminals would then have the opportunity to destroy evidence, change their behavior, and otherwise jeopardize the investigation and avert justice. Indeed, the approach outlined above is the one taken by a variety of proposed legislation currently under consideration by Congress.[34]

The Commission's questions regarding routine notification of any access to CPNI, even when no security breach is suspected, raise additional issues.[35] There may be good reasons that a carrier may want to disclose CPNI without notifying its customer, e.g., during the course of a fraud investigation. But if the Commission does decide to go beyond notification of actual security breaches, it should at a minimum make clear that any new requirements do not alter the balance struck by Congress for when law enforcement access to customer records must be disclosed. *See* 18 U.S.C. 2701 *et seq*. Because Congress has already established a structure for customer notification of law enforcement access to customer records, the

---

33 *Notice* ¶ 23.

34 *See, e.g.*, Data Accountability and Trust Act, H.R. 4127, 109th Cong. (2005); Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005).

35 *Notice* ¶ 23.

Commission should exclude disclosure of CPNI to law enforcement from any routine notification requirement.

IV. Conclusion

For the reasons stated herein, the Departments urge the Commission not to adopt rules mandating the destruction of call records and similar CPNI, a vitally important investigative resource for protecting public safety and national security. Such a rule would undoubtedly hinder the Departments' ability to carry out their respective public safety and national security responsibilities. Additionally, the Departments suggest that any new rules requiring customer notification in the case of improper CPNI disclosure include a requirement that carriers provide prompt notice to law enforcement and an opportunity for law enforcement to request delayed notification to the consumer. We appreciate the Commission's recognition and support of the Departments' important mission in these areas.

Dated: April 28, 2006

Respectfully submitted,

THE UNITED STATES DEPARTMENT OF JUSTICE

/s/ Laura H. Parsky

Laura H. Parsky
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Room 2113
Washington, D.C. 20530
(202) 616-3928

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/ Michael L. Ciminelli

Michael L. Ciminelli
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