

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 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;)	
)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	

REPLY COMMENTS OF VERIZON

Michael E. Glover
Of Counsel

Karen Zacharia
Joshua E. Swift
VERIZON
1515 N. Court House Road
Suite 500
Arlington, VA 22201-2909

Dated: June 2, 2006

Scott Delacourt
Wiley, Rein & Fielding LLP
1776 K Street, N.W.
Washington, D.C. 20006

Counsel for Verizon

EXECUTIVE SUMMARY

Commenters from many segments of the industry support Verizon's call for a flexible and balanced approach as the Commission reviews its CPNI rules in response to the EPIC Petition. This approach should focus on preventing data brokers from achieving unauthorized access to confidential customer data.

Consistent with this approach, the Commission should maintain the existing opt-out regime. The rules in place today adequately protect CPNI and imposing what is referred to as an "opt-in" requirement would do nothing to address the data broker issue raised here. Under the rules in place today, a carrier can use CPNI in marketing its own services or those of its affiliates, unless the customer elects otherwise. In contrast, under an "opt-in" regime a carrier is restricted from using CPNI for its own or its affiliates' marketing unless the customer first gives permission. Such a regime would run counter to customer expectations, would increase marketing costs (which ultimately would be borne by customers) and would do nothing to address the data brokering issue. The current rules already prohibit knowing disclosure to third parties and opt-in would do nothing to address practices used to dupe employees into disclosing CPNI. Finally, an opt-in requirement would directly infringe the ability of carriers to engage in protected commercial speech and would violate the First Amendment.

The Commission should, however, encourage a number of practices that enhance protection of subscriber data by making them the basis for safe harbor protection from enforcement action. Verizon supports a safe harbor incorporating the practices identified in its opening comments as well as the following measures identified by commenters: (1) posting current CPNI notices on carrier websites; and (2) indicating in annual CPNI certifications whether carriers have adopted safe harbor measures or conducted CPNI training in the past year.

In addition, on a voluntary basis, carriers could agree to support any FCC consumer education initiatives relating to privacy protection.

The Commission should reject other measures identified by commenters as unduly burdensome and adding no meaningful data security benefit. In particular, the Commission should reject proposals to require: (1) new opt-out notice format and content requirements; (2) customer notification before or after the release of CPNI; (3) imposition of data protection practices from the financial sector; (4) emergency data protection measures, including requiring domestic storage of all CPNI data; and (5) an inflexible schedule for review and revision of CPNI protections.

In addition, the Commission should preempt state regulation of CPNI in favor of a unified federal approach. Preemption would relieve carriers of the burden of complying with a patchwork of potentially conflicting measures. Such relief also is necessary to eliminate the burden on carriers' protected commercial speech imposed by state CPNI regulations more restrictive of commercial speech than the federal rules.

TABLE OF CONTENTS

	Page
I. COMMENTERS SUPPORTING OPT-IN AUTHORIZATION FAIL TO DEMONSTRATE A CONNECTION TO THE DATA BROKER PROBLEM.....	2
II. THE RECORD SUPPORTS AFFORDING CARRIERS THAT ADOPT ADDITIONAL PRIVACY PROTECTION PRACTICES A SAFE HARBOR FROM ENFORCEMENT.....	8
A. Commenters Support Incorporating The Privacy Protection Measures Identified By Verizon In A Safe Harbor.....	9
B. Verizon Supports Classification Of Certain Additional Measures Identified By Commenters As Safe Harbor or Voluntary Practices	13
(1) Carriers Should Indicate In Their Annual CPNI Certification Whether They Have Adopted Safe Harbor Measures Or Conducted CPNI Training In the Past Year	13
(2) Carriers Could Volunteer To Support FCC Consumer Education On Privacy Protection Practices.....	14
III. OTHER MEASURES IDENTIFIED BY COMMENTERS SHOULD BE REJECTED BECAUSE THEY ARE UNDULY BURDENSOME OR DO NOT IMPROVE CONSUMER PRIVACY PROTECTION	15
A. Notification of Customers Before or After The Release Of CPNI Is Burdensome and Impractical	15
B. The Commission Should Not Arbitrarily Import Data Protection Practices From The Financial Sector Into the Telecommunications Field	17
C. There Is No Basis For Imposing Interim, Emergency Data Protection Measures Or An Arbitrary Schedule For Reviewing CPNI Protections.....	18
IV. THE COMMISSION SHOULD PREEMPT STATE CPNI PROTECTION MEASURES TO AVOID A PATCHWORK OF CONFLICTING REQUIREMENTS.....	19
V. CONCLUSION.....	22

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 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;)	
)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	

REPLY COMMENTS OF VERIZON

Commenters from across the telecommunications industry support Verizon's call for a flexible and balanced approach as the Commission reviews its CPNI rules in response to the EPIC Petition.¹ This approach should focus on preventing data brokers from achieving unauthorized access to confidential customer data. Consistent with this approach, the Commission should reject calls to change the existing rules regarding opt-out authorization. No commenter has linked opt-in/opt-out authorization to data broker activity or identified changed circumstances that warrant revisiting settled precedent that opt-in requirements violate the First Amendment. Commenters agree, however, that flexibility is critical to addressing the threat posed by data brokers who constantly alter their tactics. For this reason, the Commission should afford carriers the flexibility they need by incorporating specific data security practices into an enforcement "safe harbor." At the same time, the Commission should not impose burdensome

¹ All comments referenced in this pleading were filed in CC Docket No. 96-115 on April 28, 2006 unless otherwise noted.

measures that do not improve data security. For example, no commenter disagreed with Verizon's position that, because business and enterprise customers have the incentive, expertise, and relational power to negotiate data protections that meet their particularized needs, there is no need to adopt new protections for these customers. In addition, Verizon supports commenters' requests for preemption of state CPNI regulations to relieve carriers of the burden of complying with a patchwork of potentially conflicting measures. Such preemption also is necessary to ensure that carriers' First Amendment rights are not compromised by state CPNI regulations more restrictive of protected commercial speech than the FCC's rules.

I. COMMENTERS SUPPORTING OPT-IN AUTHORIZATION FAIL TO DEMONSTRATE A CONNECTION TO THE DATA BROKER PROBLEM.

The rules in place today adequately protect CPNI and imposing what is referred to as an "opt-in" requirement would do nothing to address the data broker issue raised here. Under the current rules, a carrier can use CPNI in marketing its own services or those of its affiliates, unless the customer elects otherwise. As explained more below, these rules are consistent with customer expectations. Restricting a carrier from using CPNI for its own or its affiliates' marketing unless the customer first gives permission, referred to as "opt-in," would run counter to customer expectations, would increase marketing costs (which ultimately would be borne by customers) and would do nothing to address the data brokering issue. The current rules already prohibit knowing disclosure to third parties² and opt-in would do nothing to address practices used to dupe employees into disclosing CPNI. Finally, an opt-in requirement would directly

² Section 222 and the Commission's rules establish a carrier duty to safeguard customer data. 47 U.S.C. § 222(a); 47 C.F.R. § 64.2005.

infringe the ability of carriers to engage in protected commercial speech and would violate the First Amendment.³

The Commission's existing opt-out approach protects CPNI. Under current rules, a carrier may, among other possible uses, use CPNI either directly or through its agents, affiliates, independent contractors, and joint venture partners for the purpose of marketing "out-of-bucket" communications-related services, provided that a carrier notifies a customer and that customer does not elect to prevent such use (i.e., "opt-out").⁴ If the customer does nothing for 30 days, the customer is presumed to have authorized the use.⁵ However, customers understand the opt-out procedures and utilize them when they desire to protect their privacy.⁶

This opt-out approach is consistent with consumer expectations that, having entered into a customer-carrier relationship, their data will be used by their carrier to offer them discounts and market new service offerings. Customers want to be advised about other services their carrier may offer.⁷ Use of CPNI to target carrier marketing efforts provides substantial consumer benefits. Information about usage patterns enables carriers to tailor marketing to a consumer's

³ See *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999); *Implementation of the Telecommunications Act of 1996: 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*, Third Report and Order and Third Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002) ("*Third Report and Order*").

⁴ 47 C.F.R. § 64.2007(b).

⁵ 47 C.F.R. § 64.2008(d)(1).

⁶ See *Public Attitudes Toward Local Telephone Company Use of CPNI: Report of a National Opinion Survey Conducted November 14-17, 1996* by Opinion Research Corporation, Questions 5, 6, 10-11, Analysis at 9-10, Princeton, N.J. and Prof. Alan F. Westin, Columbia University, Sponsored by Pacific Telesis Group (now SBC).

⁷ *Third CPNI Order* ¶ 35 (citing Cincinnati Bell Telephone Comments (filed June 11, 1996), App. A at 2 ("*Cincinnati Bell Study*") (indicating that 81.5% of respondents wanted to be advised of the services that Cincinnati Bell Telephone offers).

needs, improving efficiency.⁸ At the same time, the practice reduce inefficient and unwanted advertising, enhancing consumer privacy.⁹ Indeed, it is not surprising that customers want to receive targeted notices regarding carrier service offerings as they expect to benefit from them.¹⁰

By contrast, an opt-in requirement frustrates consumer expectations and increases costs to carriers and consumers without improving existing safeguards against data brokers. As the Commission previously has found, opt-in – requiring affirmative customer approval prior to use of data for marketing – deprives consumers of commercial information they desire to receive.¹¹ For example, an opt-in requirement might prevent a carrier from marketing to a consumer a bundle of services – including services to which the consumer does not currently subscribe – that would reduce the costs of existing services while adding desired new services. Such a requirement also would increase the cost of targeted marketing campaigns – costs ultimately borne by consumers in higher rates – and result in more unwelcome marketing to consumers.

Moreover, opt-in burdens consumers and increases costs while adding nothing to existing safeguards on customer data. EPIC and NAAG claim that the more information can be used by agents or affiliates, the greater the risk of unauthorized disclosure and, further, that requiring opt-in will increase data security.¹² To support their claim, however, these commenters would have

⁸ *Id.* (citing Letter from Michael D. Alarcon, SBC, to William Caton, Acting Secretary, Federal Communications Commission, CC Docket Nos. 96-115 and 96-149 (filed April 12, 2002) (stating that interim opt-out approval has resulted in “[c]ustomized offerings of SBC’s products and services based on customers’ CPNI”).

⁹ *Id.* (citing AT&T Comments at 5, n.3 (“Indeed, limiting the use of CPNI may have the effect of increasing the number of solicitations by telecommunications carriers.”))

¹⁰ *Id.* at ¶ 36 (citing Letter from Gina Harrison, Pacific Telesis Group, to William F. Caton, Acting Secretary, Federal Communications Commission, CC Docket No. 96-115 (filed Dec. 12, 1996), Attach. A at 8 (“Westin Survey”)).

¹¹ *Id.* at ¶¶ 35-36.

¹² *See* EPIC Comments at 6-7; NAAG Comments at 8.

to demonstrate that data brokers are targeting agents or affiliates, know the identity of these entities, and are more successful in achieving unauthorized access from them. But EPIC and NAAG do not make such an argument and could not support it if they did. This is because use of an opt-in regime would not inhibit pretexters' ability to use deception and impersonation to get access to CPNI. Opt-in/opt-out regimes relate to the authorization required before companies may use CPNI, not the level of protection such information is afforded. Customers who do not exercise their opt-out rights are as secure from data broker activity as those who do.

In addition, opt-in burdens protected commercial speech in contravention of the First Amendment. As Verizon explained in its opening comments, the Tenth Circuit concluded that the FCC failed to carry its burden of demonstrating opt-in authorization both materially advanced a governmental interest in protecting consumer privacy and was narrowly tailored to restrict no more speech than necessary to achieve that purpose.¹³ On remand, the Commission adopted the opt-out rule that is in effect today after concluding that, despite extensive fact gathering and record development, it could not articulate a constitutional basis for requiring opt-in.¹⁴ The Federal District Court for the Western District of Washington followed the same approach as the Tenth Circuit and the FCC in striking down a Washington State opt-in rule on First Amendment grounds.¹⁵

Commenters fail to demonstrate a change that warrants revisiting this line of precedent. EPIC incorrectly argues that, since the Tenth Circuit decision, "every major challenge to privacy

¹³ See Verizon Comments at 23 (citing *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999)).

¹⁴ See *Third Report and Order*, Statement of Chairman Michael K. Powell ¶ 1.

¹⁵ *Verizon Northwest, Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1187 (W.D. Wash. 2003).

law based on commercial speech has failed.”¹⁶ The Western District of Washington decision post-dates the Tenth Circuit case, and that court found that opt-in infringes on protected commercial speech.¹⁷ In addition, unlike the Western District of Washington case, none of the cases that EPIC cites involves CPNI or Section 222 of the Act. Instead, these cases involve the Fair Credit Reporting Act, the Telephone Consumer Protection Act, and the Gramm-Leach-Bliley Act.¹⁸ NAAG states in a footnote that the Tenth Circuit did not hold that opt-in was unconstitutional *per se*, only that the record failed to demonstrate that opt-in advances the government’s interest in protecting consumer privacy and is narrowly tailored.¹⁹ NAAG fails to mention the FCC concluded on reconsideration that it could not develop a record to support the constitutionality of opt-in, even when it initiated a broad public notice and comment cycle for the purpose of doing so.²⁰ And NAAG makes no attempt to develop such a record in its comments. In light of commenters’ failure to demonstrate new circumstances suggesting that opt-in can withstand constitutional scrutiny, the FCC has no choice but to maintain the existing opt-out approach.

Not only should the Commission maintain its current opt-out authorization regime, it should not impose new opt-out notice format and content requirements. The Commission has already addressed the type of information such notices should contain and how they should

¹⁶ EPIC Comments at 11.

¹⁷ *Verizon Northwest, Inc.*, 282 F. Supp. 2d at 1187.

¹⁸ EPIC Comments at 11 n.21.

¹⁹ NAAG Comments at 7 n.20.

²⁰ *See Third Report and Order*, Statement of Chairman Michael K. Powell ¶ 1.

appear.²¹ An opt-out notice “must be comprehensible and must not be misleading” and, if written, “must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.”²² As a result, the Commission should reject NAAG’s recommendation that the FCC adopt “a short form notice which will include . . . concise, plain language explanations of the types of information shared [and] what specific steps a consumer must take to exercise his or her opt out or opt in right.”²³ Similarly, the Commission should reject NAAG’s proposal that the Commission adopt “standards for text font, size and background applicable to the means by which the [opt-out] notice is communicated.”²⁴ In light of existing Commission rules on opt-out notice format and content, the NAAG proposals are unnecessary and would impose burdens on carriers without attendant consumer benefit.

Further, implementing NAAG’s notice proposals could interfere with carriers’ ability to inform customers about the benefits of *not* opting out – namely, receiving information about how a carrier can provide customers with services specifically suited to their needs. Indeed, the Commission itself has recognized that “a carrier should not be prohibited from stating in the [opt-out] notice that the customer’s approval to use CPNI may enhance the carrier’s ability to offer products and services tailored to the customer’s needs.”²⁵ And, in any event, limiting

²¹ *Third CPNI Order* ¶¶ 89-106; *Implementation of the Telecommunications Act of 1996: 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*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, ¶¶ 130-142 (1998) (“*Second CPNI Order*”).

²² 47 C.F.R. § 64.2008(c)(4)-(5).

²³ *Id.* at 10.

²⁴ NAAG Comments at 11.

²⁵ *Second CPNI Order* ¶ 140.

carriers' ability to engage in such non-misleading commercial speech would be a blatant First Amendment violation.

Finally, NAAG suggests that the Commission consider adopting a requirement that all carriers that maintain web sites post their current CPNI notices.²⁶ As discussed in our initial comments, most carriers already publish privacy policies on their websites.²⁷ Because most carriers already include CPNI information as part of these privacy policies,²⁸ incorporating this practice into a safe harbor should be manageable for most carriers.

II. THE RECORD SUPPORTS AFFORDING CARRIERS THAT ADOPT ADDITIONAL PRIVACY PROTECTION PRACTICES A SAFE HARBOR FROM ENFORCEMENT.

Verizon takes very seriously its obligations to protect CPNI and as such has developed effective methods of safeguarding customer information. These methods have been tested to balance the need for protection with the ability of Verizon and its customers to conduct legitimate business transactions. Many of these methods, along with others that have been proposed and supported by multiple representatives of the communications industry, should comprise a legal "safe harbor." This safe harbor will provide both customers and carriers with certainty that CPNI is being adequately protected.

²⁶ *Id.* at 11.

²⁷ Verizon Comments at 9-10 and n.18.

²⁸ *See, e.g.,* Verizon, *Privacy and Customer Security Policies* (Jan. 2005), <http://www22.verizon.com/about/privacy/customer/> (last visited May 25, 2006); SBC, *Online Privacy Policy* (Sept. 19, 2005), available at <http://www.sbc.com/gen/privacy-policy?pid=2506>; Sprint Nextel, *Sprint Privacy Policy* (Sept. 1, 2005), http://www.sprint.com/legal/sprint_privacy.html#principles.

A. Commenters Support Incorporating The Privacy Protection Measures Identified By Verizon In A Safe Harbor.

In its Comments, Verizon proposed establishing a “safe harbor” against enforcement action for carriers that have implemented specific and appropriate data protection practices.²⁹ In particular, Verizon proposed affording carriers protection from enforcement action if they (1) cooperate with FCC, FTC, and DOJ efforts to identify and prosecute data brokers; (2) participate in a carrier working group dedicated to enhancing data security and combating theft of confidential information; (3) permit customers to voluntarily elect password protection for residential accounts; (4) file a more detailed annual CPNI certification with the FCC; (5) post their privacy policies online; and (6) prohibit certain categories of information – such as social security, driver’s license, and taxpayer identification numbers – from being disclosed to residential customers.³⁰ The record in this proceeding supports establishment of this safe harbor.

As indicated by multiple commenters in this proceeding,³¹ adoption of a safe harbor from enforcement action – rather than detailed and rigid rules – has the benefit of “provid[ing] flexibility for those subject to the regulations.”³² Indeed, carrier flexibility is essential given the ever-changing tactics of data brokers. In its Comments, Verizon Wireless stated that data brokers are constantly modifying their tactics to unlawfully obtain CPNI so as to circumvent

²⁹ Verizon Comments at 2.

³⁰ *Id.* at ii-iii.

³¹ *See, e.g.*, Cingular Comments at 31-33; Independent Carrier Group Comments at 10-11; Charter Communications Comments at 37.

³² Qwest Comments at 36.

carrier-imposed protections.³³ Carriers, in turn, must have the flexibility to eliminate data protections that are no longer effective and implement new, innovative safeguards. A safe harbor with the base level of protections proposed by Verizon will provide carriers this necessary flexibility. It will also provide an incentive for carriers to exceed current federal requirements for the protection of CPNI.

In addition, as noted by many commenters, a safe harbor will protect entities that take reasonable measures to protect their customers' CPNI from disclosure. As noted by Qwest, "[i]t is not necessarily the case that a carrier is at fault if it is duped out of information by a fraudulent impersonator maliciously preying on the good intentions of the carrier's employees and their desire to be helpful to a customer."³⁴ By establishing a safe harbor, the Commission will encourage carriers to continue to work with industry and government to develop a variety of safeguards that would protect consumers' CPNI while focusing enforcement on the entities that are actually causing such disclosures – the data brokers themselves.

Moreover, the specific elements of Verizon's safe harbor proposal are broadly supported by a wide variety of commenters. First, no one argues in the record that data brokers should not be prosecuted. Instead, almost all commenters acknowledge the significant problem that has developed as a result of data brokers' fraudulent activities.³⁵ By working with carriers and other entities possessing CPNI, the FCC, FTC, and DOJ will be able to more effectively identify and prosecute data brokers. Although carriers may not always be aware that a breach has occurred, carriers may be able to provide information to government agencies regarding which entities are

³³ Verizon Wireless Comments at 2. *See, e.g.*, Alltel Comments at 2 (stating that "methods through which unauthorized third parties obtain the data are varied, and the subject of constantly evolving technical and social engineering threats").

³⁴ Qwest Comments at 5.

³⁵ *See, e.g.*, AT&T Comments at 3; T-Mobile Comments at 7; NAAG Comments at 2.

orchestrating such fraud and what mechanisms they use to do so.³⁶ Accordingly, the FCC clearly should encourage carriers to cooperate with the government to prosecute data brokers and stop the prevalence of unauthorized CPNI disclosures.

Second, the record supports establishment of an industry working group that can quickly and continually monitor and assess the data broker problem. An industry working group is the ideal way to examine and address the problem of inadvertent CPNI disclosures.³⁷ Such a group also could function as a rapid response team to identify new breaches and implement immediate solutions. As NCTA notes, such an effort could help industry explore the mechanisms by which data brokers are exploiting existing safeguards and the efficacy of potential future safeguards. At the same time, carriers would maintain the flexibility to respond to data broker activities with new measures on an ongoing basis. Moreover, an industry working group provides a forum for a data protection discussion that avoids concerns about providing data brokers a roadmap of system vulnerabilities.

Third, multiple commenters note the benefits of making passwords available to residential customers. These same commenters, however, also note that password protection is not appropriate for all customers. For example, AT&T notes that passwords may be problematic for many customers because they are so often forgotten.³⁸ Similarly, the Missouri Public Service Commission notes the “monumental” task associated with establishing passwords for all

³⁶ While Section 222 limits the use or disclosure of CPNI for commercial purposes, it nevertheless allows information to be shared with law enforcement authorities and also permits disclosure of CPNI “to protect the rights or property of the carrier, or to protect users . . . and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services” 47 U.S.C. § 222(d)(2).

³⁷ *See, e.g.*, NCTA Comments at 6 (noting that an industry working group is the best way to examine and address the problem inadvertent disclosure of information to data brokers).

³⁸ AT&T Comments at 2.

telecommunications-related accounts.³⁹ As such, the record demonstrates that, although providing residential customers with the option to establish a password, the public interest favors the voluntary use of passwords through a safe harbor mechanism rather than a mandate.⁴⁰

Fourth, there is broad support in the record that (1) carriers filing an annual compliance certification with the FCC could aid the FCC in ensuring compliance with its CPNI rules⁴¹ and (2) carriers posting their privacy policies online could provide customers with much needed information.⁴² As noted by AT&T, such annual certifications could assist the FCC in assessing the extent of the data broker problem and determining the adequacy of a wide variety of CPNI security measures.⁴³ Similarly, the posting of privacy policies online will provide customers with information about how individual carriers collect and use CPNI, how customers can control how the information is used, and when and to whom it will be disclosed.⁴⁴

Finally, commenters agree that prohibiting the disclosure of certain categories of information – such as driver’s license, social security, and taxpayer identification numbers – would add an additional measure of security to existing CPNI protections.⁴⁵ As CTIA notes, it is a common pretexting tactic to call carriers and pretend to be a relative or other “authorized

³⁹ Missouri PSC Comments at 2.

⁴⁰ Imposing onerous authentication requirements, such as mandatory passwords, is especially inappropriate as to certain CPNI, such as bill balance information, when a customer, for example, seeks only to pay an overdue balance in order to maintain dial tone. The record here suggests that pretexters target Call Detail Records, *see, e.g.* EPIC Pet. at 6, not information such as bill balance amount. Carriers are in the best position to balance their customers’ competing interests in privacy and their need for efficient account access.

⁴¹ *See, e.g.*, Cingular Comments at 17; T-Mobile Comments at 16.

⁴² *See, e.g.*, CTIA Comments at 11 (filed May 1, 2006).

⁴³ AT&T Comments at 14.

⁴⁴ NAAG Comments at 19.

⁴⁵ *See, e.g.*, CTIA Comments at 21 (filed May 1, 2006).

person” that needs emergency access to such information.⁴⁶ Once a data broker has this type of information, however, it may use it to achieve unauthorized access to other types of CPNI or other entities.

Accordingly, the FCC should adopt the safe harbor Verizon proposed in its Comments to provide incentives for carriers to exceed current federal requirements for the protection of CPNI and give customers the ability to select a provider that offers the level of protection they desire.

B. Verizon Supports Classification Of Certain Additional Measures Identified By Commenters As Safe Harbor or Voluntary Practices.

Verizon supports the incorporation of certain additional measures that can effectively and efficiently protect CPNI into an enforcement safe harbor or on a voluntary basis. In particular, carriers could identify in their annual certifications the safe harbor measures they have implemented and training they have performed in the past year. Further, on a voluntary basis, carriers could support the Commission’s consumer education efforts on privacy protection. These measures properly balance the need for protection of customer information with flexibility that allows carriers and consumers to conduct legitimate business transactions without unnecessary cost and frustration.

(1) Carriers Should Indicate In Their Annual CPNI Certification Whether They Have Adopted Safe Harbor Measures Or Conducted CPNI Training In the Past Year.

CTIA proposes that the annual carrier certification, in addition to being filed with the Commission, should “include representations that the carrier has implemented security procedures to prevent unauthorized CPNI disclosures and conducted privacy and security training during the prior year for those personnel who have access to CPNI.”⁴⁷ Verizon agrees

⁴⁶ *Id.* at 3.

⁴⁷ CTIA Comments at 9 (filed May 1, 2006).

that including such a representation would promote greater transparency in carrier CPNI certifications, provided that the proposal does not require each employee to be re-trained on the same material every year.⁴⁸ Verizon trains new employees that handle or manage CPNI on Verizon's and federal requirements to protect such information, and such employees also receive additional periodic training as various internal procedures or external requirements change, or as a "refresher." But requiring each employee with access to CPNI to sit through the same CPNI training every year would impose costs on carriers without any attendant benefit.

Certifying each year that employees with access to CPNI have been trained would provide additional assurance to customers and further assist the Commission in its goal of promoting uniformity in carrier certifications.⁴⁹ These representations should be included among the criteria to qualify for safe harbor protection.⁵⁰

(2) Carriers Could Volunteer To Support FCC Consumer Education On Privacy Protection Practices.

The Pennsylvania Public Utility Commission ("Pennsylvania PUC") recommends that the Commission consider a campaign to educate consumers about their right to review prior releases of their CPNI.⁵¹ As discussed below, Verizon opposes the creation of such an advance notice right, but Verizon agrees that the Commission should continue its efforts to educate customers about this and other aspects of the CPNI rules.⁵² However, the Commission should

⁴⁸ *See id.*

⁴⁹ *Notice* at ¶ 29.

⁵⁰ Verizon Comments at 8-9.

⁵¹ Pennsylvania PUC Comments at 5-6.

⁵² The Commission's Consumer & Governmental Affairs Bureau already provides extensive information on consumer privacy issues through its web site. *See, e.g.* FCC Consumer

continue to take the lead as a trusted, neutral, and one-stop source for consumer information, rather than delegating the responsibility in the first instance to individual carriers as suggested by the Pennsylvania PUC.⁵³ Voluntary carrier efforts should be used to support and complement the Commission's consumer education activities, rather than to duplicate them.

III. OTHER MEASURES IDENTIFIED BY COMMENTERS SHOULD BE REJECTED BECAUSE THEY ARE UNDULY BURDENSOME OR DO NOT IMPROVE CONSUMER PRIVACY PROTECTION.

While supporting protection measures that are effective and efficient in the protection of CPNI, Verizon urges the Commission not to impose measures that are burdensome and ineffective. Requirements that result in great costs to carriers or frustration and irritation to customers, as opposed to improved security of CPNI, should be rejected. The measures discussed in the previous section provide effective means of protecting CPNI, without causing undue burden to carriers and customers.

A. Notification of Customers Before or After The Release Of CPNI Is Burdensome and Impractical.

Some commenters suggest that one means of improving any CPNI protection regime centers around notification to customers, both before CPNI is released and when there is any possibility that CPNI may have been improperly accessed by an unauthorized user.⁵⁴ For example, NAAG even suggests that customers should be notified *every time* their customer information is released. The Commission should not adopt such a notification requirement

Advisory, "Protecting the Privacy of Your Telephone Calling Records," available at <http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html> (last visited May 26, 2006).

⁵³ Pennsylvania PUC Comments at 5-6.

⁵⁴ See EPIC Comments at 14-15; NAAG Comments at 15.

because it is not a viable solution to data broker incursions and, in any event, would produce unnecessary customer concern and confusion that will outweigh any potential security benefit.⁵⁵

As Verizon has previously observed, notification in the case of unconfirmed breaches is particularly problematic.⁵⁶ Requiring notification before a carrier has confirmed a breach will cause customers needless concern and annoyance. Customers will quickly become irritated with a company that contacts the customer every time CPNI is utilized. Furthermore, such a system will potentially lead to a flurry of notices, which could desensitize customers to cases where an actual privacy breach has occurred.

Similarly, indicating on a customer's bill every instance in which the customer's CPNI has been accessed would be costly for the companies who prepare these bills and would provide little added protection for customers. Many customers confronted with such a statement would become concerned and contact customer service to inquire about the disclosure. The increased volume and duration of calls caused by this notification will lead to customer irritation. Verizon opposes any measure that will only serve to concern and annoy customers but will not lead to the greater protection of CPNI.⁵⁷

⁵⁵ In their joint comments, the DOJ and DHS state that “any rule requiring [customer notification of release of CPNI] 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.” DOJ and DHS Comments at 14. Because carriers are often barred from disclosing or asked not to disclose information about ongoing law enforcement investigations, the Commission should not adopt a requirement that customers be notified each time their CPNI is released.

⁵⁶ See Verizon Comments at 18.

⁵⁷ The NAAG proposal would also require customer notification of each release of CPNI even where data sharing has already been authorized by a customer pursuant to opt-out approval. If NAAG intends these additional notices to afford the customer further opportunities to opt-out or to prompt the customer to revoke opt-out authorization, such a requirement would burden protected commercial speech in contravention of the First Amendment. See Section I, *supra*.

Finally, some commenters have suggested that a customer be contacted prior to any release of that customer's CPNI. EPIC and NAAG suggest that a carrier send an "SMS" text message to a wireless phone, initiate a call to the customer, or leave an automated voicemail with the customer prior to any disclosure of customer information. As Verizon has previously noted, this requirement would be burdensome and costly to carriers and would frustrate customers who are trying to accomplish legitimate transactions. In order to comply with such a requirement, carriers would be required to contact a customer at an address or phone number of record, typically a home address or phone number, before disclosing CPNI. However, customer inquiries typically occur during regular business hours when many customers are at work, which would make contacting a customer at home largely impossible. Requiring such a precautionary customer notification would cause customer frustration and deter or slow legitimate transactions.

B. The Commission Should Not Arbitrarily Import Data Protection Practices From The Financial Sector Into the Telecommunications Field.

As opposed to assessing the specific safeguards that have been crafted to meet the needs of both carriers and customers in the protection of CPNI, some commenters suggest importing the security measures employed by financial institutions pursuant to the Gramm-Leach-Bliley Act.⁵⁸ But the Commission should not import security measures specifically adopted for financial institutions. Information security systems need to be developed based on the specific industry and type of information involved. The CPNI rules have developed based on a balancing of privacy protection and customer needs. The Gramm-Leach-Bliley Act was not developed to protect CPNI or to be implemented in communications companies. Furthermore, commenters have produced no evidence to demonstrate the effectiveness of security measures adopted

⁵⁸ 15 U.S.C. § 6801 *et seq.* See NAAG Comments at 14; EPIC Comments at 16.

pursuant to the Gramm-Leach-Bliley Act or that these methods will improve protection against data broker incursions.

C. There Is No Basis For Imposing Interim, Emergency Data Protection Measures Or An Arbitrary Schedule For Reviewing CPNI Protections.

In addition to notification requirements and the implementation of financial institution security measures, commenters have recommended other proposals that are ineffective in the protection of CPNI. For example, the Privacy Rights Clearinghouse proposes the implementation of immediate temporary emergency measures pending the development of new CPNI protection laws.⁵⁹ The Privacy Rights Clearinghouse provides no guidance suggesting what these emergency measures would involve, or how restricting the interactions of carriers and the customers they are attempting to serve would be beneficial to either party. The Commission should not adopt any such measures. Quickly adopted measures could not be properly tested for effectiveness and would almost certainly create great frustration for customers and impose significant burdens on carriers. Furthermore, neither the Privacy Rights Clearinghouse nor any other commenter has produced evidence to demonstrate a need for such radical measures. Although Verizon is committed to protecting customer information and minimizing pretexting, such protection should not be based on untested and potentially ineffective emergency measures.

Similarly, the Commission should not require that all CPNI be stored domestically.⁶⁰ Such a requirement will provide little or no added protection against data brokers but will increase costs for carriers. There is no need to require domestic storage of CPNI because there is no indication that data brokers target off-shore data. Imposing such a requirement would be costly and disruptive to carriers. Although master records of Verizon's CPNI information are

⁵⁹ See Privacy Rights Clearinghouse Comments at 2-3 (filed Apr. 24, 2006).

⁶⁰ See DOJ and DHS Comments at 10.

exclusively stored domestically, the location of data should not affect the measures a carrier takes in protecting this information. The Commission should not implement regulations that disrupt legitimate business process and provide no additional protection.

Additionally, EPIC has proposed a requirement that carriers review their security measures on a planned schedule and suggests that a review be conducted every five to seven years.⁶¹ This proposal seemingly ignores the problems faced by carriers in protecting CPNI. EPIC disregards the evidence that those who scheme to fraudulently obtain CPNI are constantly changing and evolving the tactics they use. Verizon and other carriers review and respond to new techniques used by pretexters as they are discovered. A required review on an arbitrary schedule will not be effective in improving protection techniques or information security programs.

IV. THE COMMISSION SHOULD PREEMPT STATE CPNI PROTECTION MEASURES TO AVOID A PATCHWORK OF CONFLICTING REQUIREMENTS.

The FCC should preempt state regulation of CPNI in favor of a unified federal approach. In support of a request for preemption in its comments, Centennial correctly explains that “[i]mplementing, potentially, over fifty different state-level CPNI compliance programs, as well as a federal ‘overlay’ scheme, is unworkable, overly burdensome and unnecessary.”⁶² As a practical matter, as Verizon has explained in other CPNI proceedings,⁶³ it is difficult to distinguish between the use of interstate and intrastate CPNI and to implement separate

⁶¹ See EPIC Comments at 16.

⁶² Centennial Communications Corp. Comments at 5-6.

⁶³ See Verizon’s Petition for Reconsideration of Third Report and Order in CC Docket No. 96-115, CC Docket No. 96-115 (filed Oct. 21, 2002) (“Verizon Recon. Petition”); Verizon’s Reply Comments to Petitions for Reconsideration of Third Report and Order in CC Docket No. 96-115 (filed Jan. 6, 2003).

regulatory compliance measures for each. And as this docket demonstrates, restrictions can be devised and combined in an almost limitless number of ways in the name of “protecting” CPNI. Moreover, since the FCC last considered a request for preemption, states have continued to flout settled law and FCC policy by adopting unconstitutional opt-in requirements. Preemption also is necessary to eliminate the burden opt-in requirements impose on carriers’ protected commercial speech.

The Commission should exercise its preemption authority here because the interstate and intrastate portions of CPNI are intertwined, and allowing states to regulate CPNI would thwart federal CPNI policy. Verizon’s systems cannot readily distinguish between the portions of CPNI that are related to interstate versus intrastate services.⁶⁴ The Commission has recognized the difficulty of doing so, explaining that “varying state [CPNI] regulations” could affect “carriers’ ability to operate on a multi-state or nationwide basis.”⁶⁵ As a result, state regulations on marketing of intrastate services necessarily restrict Verizon’s ability to market interstate services as well. Given the impossibility of complying with separate and inconsistent state and federal regulations, carriers will be forced to comply with the most restrictive state CPNI regulations, in disregard of the delicate balance the Commission has struck between competitive and consumer privacy interests.⁶⁶

Such a regulatory “race to the bottom” is particularly problematic where compliance with the most restrictive state CPNI regime, even while such a regime is being challenged, may result

⁶⁴ Verizon Recon. Petition at 9-10 (citing Declaration of Maura Breen, Senior Vice President and Chief Marketing Officer of Retail Markets for Verizon Services Corporation, ¶ 6 (“Breen Declaration”)).

⁶⁵ *Third CPNI Order* at 14891, ¶ 71.

⁶⁶ Verizon Recon. Petition at 11 (citing Breen Declaration, ¶ 14).

in a chilling of protected commercial speech.⁶⁷ Emboldened by the Commission’s rejection of prior requests for broad preemption in favor of a “case-by-case” approach,⁶⁸ several states have proposed CPNI rules that are more restrictive than, and inconsistent with, the Commission’s regulations. For example, as discussed above, Washington State adopted an opt-in regime that the Federal District Court for the Western District of Washington struck down on First Amendment grounds.⁶⁹ In Arizona, the Attorney General recently approved CPNI rules containing an opt-in provision that will take effect on June 19, 2006, in the absence of judicial intervention.

By granting states the discretion to enact CPNI regulations more restrictive of commercial speech than the Commission, even if those regulations are only in effect until the Commission has completed its case-by-case preemption review, the Commission infringes on carriers’ First Amendment rights. After inviting comments and conducting an extensive study of the record, the Commission determined that it could not adopt an opt-in policy without running afoul of the First Amendment.⁷⁰ Nonetheless, if states implement more stringent rules than the Commission with respect to the authorization required to share customer data – such as an opt-in requirement – carriers will be forced to comply. In other words, by affording states discretion to adopt CPNI regulations that are more restrictive of commercial speech than the Commission’s

⁶⁷ The Supreme Court has stated that even creating the fear of unjustified liability is enough to produce a chilling effect antithetical to First Amendment protected speech. *See Phila. Newspapers, Inc. v. Hepps*, 475 U.S. 767, 777 (1986). *See also Rosenberger v. Rector and Visitors of Univ. of Va.*, 515 U.S. 819, 835 (1995) (recognizing the “danger to liberty” that results from the government’s “chilling of individual thought and expression”).

⁶⁸ *See Third Report and Order*, ¶¶ 69-71 (2002) (Commission elected to exercise its preemption authority on a case-by-case basis, reasoning that states might be able to enact more restrictive CPNI regulations based on “different records”).

⁶⁹ *Verizon Northwest, Inc.*, 282 F. Supp. 2d 1187.

⁷⁰ *Third CPNI Order* at 14874, ¶ 31.

rules, the Commission is essentially delegating federal policy decisions to the states. Under a long line of Supreme Court precedent, this delegation to allow others to make decisions that may violate the First Amendment is itself a First Amendment violation.⁷¹ By leaving the door open to such discretion, the Commission is itself infringing on First Amendment rights.⁷² Accordingly, in order to avoid imminent constitutional violations, the Commission should preempt state CPNI regulations more restrictive of commercial speech than the Commission's own rules across the board.

V. CONCLUSION

For the foregoing reasons, the Commission should adopt an order granting the relief specified herein and in Verizon's Comments filed April 28, 2006.

⁷¹ See, e.g., *Forsyth County, Ga. v. The Nationalist Movement*, 505 U.S. 123, 130 (1992) (striking down county ordinance permitting government administrator to set various fees for parade permits because the ordinances did not contain 'narrow, objective, and definite standards to guide the licensing authority' (internal quotation marks and citation omitted)); *City of Lakewood v. Plain Dealer Publ'g Co.*, 486 U.S. 750, 757 (1988) ("[A] licensing statute placing unbridled discretion in the hands of a government official or agency constitutes a prior restraint and may result in censorship"); *Shuttlesworth v. City of Birmingham*, 394 U.S. 147, 151 (1969) ("It is settled by a long line of recent decisions of this court that an ordinance which, like this one, makes the peaceful enjoyment of the freedoms which the Constitution guarantees contingent upon the uncontrolled will of an official – as by requiring a permit or license which may be granted or withheld in the discretion of such official – is an unconstitutional censorship or prior restraint upon the enjoyment of those freedoms." (Internal quotation marks and citation omitted)).

⁷² See, e.g., *Hendler v. United States*, 952 F.2d 1364 (Fed. Cir. 1991), *aff'd* 75 F.3d 1394 (Fed. Cir. 1999) (holding that where California state officials entered plaintiff's land under authority granted by the EPA, the activities of the state within the scope of the order were attributable to the federal government for the purposes of the takings claim); *Presault v. United States*, 100 F.3d 1525 (Fed. Cir. 1996) (holding that the State of Vermont's conversion of private land into a recreational trail under authority of the Rails-to-Trails Act and by order of the Interstate Commerce Commission was an taking for which the federal government was liable).

Respectfully submitted,

Of Counsel
Michael E. Glover

By: /s/ Joshua Swift

Karen Zacharia
Joshua E. Swift
VERIZON
1515 N. Court House Road
Suite 500
Arlington, VA 22201-2909
703.351.3039

Scott Delacourt
Wiley, Rein & Fielding LLP
1776 K Street, N.W.
Washington, D.C. 20006

Dated: June 2, 2006

Counsel for Verizon