

**Before the  
Federal Communications Commission  
Washington, DC 20554**

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

CG Docket No. 96-115

RM-11277

**REPLY COMMENTS OF CHARTER COMMUNICATIONS, INC.**

Christin McMeley  
Vice President & Senior Counsel  
Privacy & Regulatory  
Charter Communications, Inc.  
12405 Powerscourt Drive  
St. Louis, MO 63131

Michael C. Sloan  
Timothy P. Tobin  
Brian J. Hurh  
Cole, Raywid & Braverman, L.L.P.  
1919 Pennsylvania Avenue, NW  
Suite 200  
Washington, DC 20006  
(202) 659-9750

*Attorneys for Charter Communications, Inc.*

June 2, 2006

## SUMMARY

Charter Communications, Inc., (“Charter”) agrees with the virtually unanimous conclusion by industry commenters that new CPNI rules are unnecessary. The current rules already impose substantial requirements upon carriers and adequately protect CPNI from improper use and disclosure. There are other protections as well. Criminal and civil prosecution by state and federal law enforcement will punish and deter pretexters. Market forces, including the negative publicity concerning the sale of CPNI, also provide powerful incentives for carriers to further safeguard their customers’ information and records. New rules will only impose costs on carriers (and in turn consumers) without any corresponding consumer benefit.

Charter strongly disagrees with many of EPIC’s proposed changes to the current CPNI protection regime. In particular, Charter opposes any requirement that carriers be required to receive their customers’ affirmative “opt-in” assent before sharing CPNI with joint venture partners (“JVs”) and independent contractors (“ICs”) who, unlike unrelated “third parties,” market or provide “communications related services” on behalf of or with the carrier. The Commission’s current “opt-out” approach for sharing CPNI with JVs and ICs provides more direct consumer control over how customer information is used than many other well-known U.S. privacy laws. In recognition of the ever-increasing convergence of communications services – voice, video and data – by single companies and their affiliates, information sharing requirements should instead be relaxed to allow and encourage more effective marketing of bundled services to existing customers.

Finally, Charter sees little merit in the increased procedural “protections” EPIC proposes. These measures, including use of passwords, encryption, prescribed record retention requirements and the like, will be costly and potentially counterproductive as technology evolves.

**TABLE OF CONTENTS**

	<u>Page</u>
I. INTRODUCTION .....	1
II. OPT-OUT UNDER THE CURRENT RULES IS UNRELATED TO THE PRETEXTING PROBLEM AND PROVIDES A REASONABLE BALANCE BETWEEN CONSUMER PRIVACY AND INDUSTRY INTERESTS.....	3
A. Limiting CPNI Sharing with JVs and ICs Through Opt-in Does Not Substantially Reduce the Risk of CPNI Disclosure to Pretexters.....	4
B. Other Arguments in Support of Prohibiting Opt-out for ICs and JVs Offering Communications-Related Services Are Unpersuasive.....	5
1. The Current CPNI Rules Provide Adequate Notice .....	6
2. EPIC’s Use of Surveys and Polls is Misleading .....	7
3. U.S. West v. FCC Remains Good Law.....	9
4. Most U.S. Privacy Laws Use an Opt-out Regime .....	11
C. Because of Ever-Increasing Bundled Service Offerings, The Commission Should At a Minimum, Expand Its Definition of Communications-Related Service to Include Cable Video Service; It Should Also Add Video and Internet Access to Its Total Service Approach .....	14
III. EPIC’S PROPOSED SAFEGUARDS AND NOTICE RULES ARE UNNECESSARY AND COSTLY .....	16
IV. IF THE COMMISSION DOES WANT TO PURSUE NEW APPROACHES, IT SHOULD BE VERY CAREFUL NOT TO BURDEN PROVIDERS AND THEREFORE HARM CONSUMERS .....	19
A. A More Reasonable Alternative to Regulatory Mandates Would Be an Industry-Wide Working Group.....	19
B. If the Commission Enacts New Rules, a Carrier Safe Harbor Provision for CPNI is Desirable. ....	20
C. Whether or Not the Commission Enacts New Rules It Should Preempt More Restrictive State Laws .....	20
V. CONCLUSION.....	22

**Before the  
Federal Communications Commission  
Washington, DC 20554**

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

CG Docket No. 96-115

RM-11277

**REPLY COMMENTS OF CHARTER COMMUNICATIONS, INC.**

**I. INTRODUCTION**

Charter Communications, Inc., ("Charter") agrees with the virtually unanimous conclusion by industry commenters that no new CPNI rules are needed to address pretexting.<sup>1</sup> The current rules adequately protect CPNI from improper uses and disclosures, and market forces, including the negative publicity concerning the sale of CPNI, provide sufficient incentives for carriers to further safeguard their customers' information and records. Law enforcement will pursue pretexters while carriers that make improper disclosures will suffer the consequences of consumer backlash and be subject to Commission action. Accordingly, the

---

<sup>1</sup> See initial comments filed pursuant to *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*,

current rules, market incentives, and vigorous pursuit by law enforcement provide all the protection that is required.

Proponents of new, more stringent CPNI rules offer little justification for their proposals, the costs of which plainly exceed the limited – if any – benefits consumers will receive. In these Reply Comments, Charter addresses some of the particularly misguided arguments made by those in favor of new CPNI rules. Charter disagrees vigorously with those who favor a consumer opt-in requirement for sharing CPNI with joint venture partners (“JVs”) and independent contractors (“ICs”) who participate with the carrier to market or provide “communications related services.” Instead, Charter favors retention of the current opt-out requirement for such disclosures. The Commission has previously recognized that such sharing (subject to strict safeguards) is akin to internal sharing among affiliates and is *not* analogous to third party sharing. In this era of bundled offerings made possible by the convergence of previously distinct consumer offerings, narrowing opt-out is exactly the wrong approach. Indeed, Charter favors expanding opt-out by adding “cable video service” to the definition of “communications-related” service, 47 C.F.R. § 64.2003(b), so that cable providers can more effectively market their expanded communications offerings to current customers. These Reply Comments also explain why the additional “safeguards” EPIC proposes are unnecessary and potentially counterproductive.

## **II. OPT-OUT UNDER THE CURRENT RULES IS UNRELATED TO THE PRETEXTING PROBLEM AND PROVIDES A REASONABLE BALANCE BETWEEN CONSUMER PRIVACY AND INDUSTRY INTERESTS**

The Electronic Privacy Information Center, filing jointly with several other consumer groups (collectively, “EPIC”),<sup>2</sup> relies on several unsubstantiated grounds as the basis for the conclusion that consumers should be required to “opt-in” or otherwise affirmatively authorize carriers to share CPNI with JVs and ICs. EPIC claims that opt-in is the “only” adequate means for protecting CPNI,<sup>3</sup> but fails to present any credible evidence that the current opt-out regime is responsible for, or even related to, the recent CPNI disclosures. Nor does EPIC explain how its proposals would prevent or reduce pretexting. In fact, the proposals would accomplish little, but would significantly increase carriers’ costs, which would ultimately be passed on to consumers and make legitimate marketing efforts less effective.

Indeed, it is plain that some commenters attack opt-out generally – *i.e.*, as applied to other industries in other contexts – without considering the application of opt-out under the current CPNI rules, which limit CPNI disclosures to only a few types of entities and in very limited circumstances (addressed more fully below). The need for carriers to share information with JVs and ICs is even more important today than when the rules were first promulgated because recent market and technological developments permit carriers to offer bundled services that cut across current regulatory classifications. These developments would suggest *expanding* opt-out so that carriers can work more closely with their affiliates and JV partners, whose participation is necessary to offer new services.

---

<sup>2</sup> EPIC filed comments jointly with Consumer Action, Privacy Rights Now Coalition, Center for Digital Democracy, Consumer Federation of America, Privacy Journal, Center for Financial Privacy and Human Rights, and National Consumers League (“EPIC Comments”).

<sup>3</sup> EPIC Comments, at 7 -12.

**A. Limiting CPNI Sharing with JVs and ICs Through Opt-in Does Not Substantially Reduce the Risk of CPNI Disclosure to Pretexters**

EPIC argues that “[t]he more information is shared, the greater the risk that is [sic] may be acquired by dishonest employees or others who have access to data in the course of its transfer.”<sup>4</sup> For support, EPIC cites a Michigan State University research project that reviewed 1,000 identity theft cases and found that approximately 50-70 percent were “inside jobs” where employees with authorized access were the ones responsible for the unauthorized disclosure of customer data.<sup>5</sup> That study, however, does not demonstrate that altering the current opt-out approach will enhance protection of CPNI, as the risk of improper disclosure due to employee wrongdoing is unrelated to whether opt-in or opt-out approval is required. If the effect of an “opt-in only” regime would be to limit those who have access to CPNI, then it will only concentrate CPNI with the carrier and its direct affiliates, and criminals will accordingly focus their attention on unlawfully obtaining access to CPNI from those entities.<sup>6</sup> In the end, whatever the vehicle for authorizing disclosure, it cannot prevent an unscrupulous employee who already has access to customer data from improperly releasing that information. Finally, as one commenter remarks, neither EPIC nor any other commenter has provided actual evidence that

---

<sup>4</sup> EPIC Comments, at 6.

<sup>5</sup> *Id.* (citing to Bob Sullivan, *Study: ID theft usually an inside job; Up to 70 percent of cases start with employee heist*, MSNBC, May 21, 2004, available at <http://www.msnbc.msn.com/id/5015565/>).

<sup>6</sup> EPIC Comments, at 7 (explaining how organized crime groups encourage members to apply for positions with access to personal information). Moreover, if the point of EPIC’s proposal is that CPNI will be better safeguarded by limiting the number of entities that have access, the institution of an opt-in requirement would not be a sufficiently narrowly tailored means of achieving that objective, as the United States Court of Appeals has already determined. *See U.S. West v. F.C.C.*, 182 F.3d 1224 (10th Cir. 1999).

CPNI was taken from JVs or ICs.<sup>7</sup> Thus, there is no justification for imposing an opt-in consent requirement for sharing CPNI with JV's or IC's for communications-related purposes.

**B. Other Arguments in Support of Prohibiting Opt-out for ICs and JVs Offering Communications-Related Services Are Unpersuasive**

Charter's initial Comments explained that the Commission's rationale for its current rules, which authorize opt-out for sharing CPNI with ICs and JVs involved in providing communications-related services, was based on the same factors that led the Commission to allow an opt-out approach for affiliates.<sup>8</sup> Those factors include customers' expectations and the benefits that accrue from these specific limited entities' ability to offer more "personalized service offerings (and possible cost savings)" and "more efficient and better-tailored marketing [that] has the potential to reduce junk mail and unwanted advertising."<sup>9</sup> The Commission concluded that disclosing CPNI to ICs and JVs is more akin to sharing with affiliates than with third parties.<sup>10</sup> Under the current rules, customers are offered an opportunity to prevent carriers from sharing their CPNI with JVs and ICs for the purpose of targeted marketing of communications-related services. Charter believes that this approach better facilitates the "free

---

<sup>7</sup> See Joint Comments of Eschelon Telecom, Inc., Snip Link Inc., and XO Communications, Inc., at 12 ("The Joint Commenters do not have any reason to believe that either their joint venture partners or independent contractors are misusing, disclosing, or sharing access to CPNI outside of the scope of the arrangement with the carrier. Nor has EPIC presented any evidence that either joint venture partners or independent contractors are responsible for unauthorized use of, access to, or disclosure of CPNI.").

<sup>8</sup> Charter Comments, at 16-20 (citing *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 F.C.C.R. 14,860, 14,875-880, ¶¶ 32, 35-36, 45 (July 25, 2002) (hereinafter *Third Report and Order*)). Also, as reflected in the NPRM, EPIC has not proposed altering the ability to offer consumers an opt-out choice to prevent carriers' sharing of CPNI with *affiliates* offering communications-related services. See generally *CPNI NPRM*.

<sup>9</sup> *Third Report and Order*, at 14,876 ¶ 35.

<sup>10</sup> *Id.* at 14,880-888 ¶¶ 45 -52, 63.

flow of information” that consumers expect.<sup>11</sup> EPIC’s arguments for replacing this regime with an opt-in requirement overlook the merits of the current opt-out approach and its specific arguments lack merit. We review them in more detail below:

1. *The Current CPNI Rules Provide Adequate Notice*

EPIC argues that an “opt-out approach is inadequate because it is not calculated to reasonably inform consumers about their privacy options.”<sup>12</sup> But EPIC’s criticisms overlook the fact that the current rules detail the timing and content of customer notices.<sup>13</sup> The current rules also contain specific requirements for informing customers about their opt-out rights.<sup>14</sup> These rules, coupled with market incentives to provide customers with privacy options to distinguish carriers from their competitors, ensure that customers will receive adequate information about their right to prevent their providers from sharing CPNI with JVs and ICs.

The anecdotal evidence EPIC cites does not prove otherwise. For example, EPIC asserts that “opt-out is the standard choice for companies that are trying to stop consumers from taking an action” and contends that opt-out strategies are employed as obstacles to prevent consumers from canceling contracts and subscriptions, among other things.<sup>15</sup> But EPIC’s examples are far

---

<sup>11</sup> *Id.*; see also Michael E. Staten & Fred H. Cate, *The Impact of Opt-in Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 DUKE L.J. 745, 766 (2003) (“[O]pt-out presumes that consumers do want the benefits (greater convenience, wider range of services, and lower prices) facilitated by a free flow of information, and then allows people who are particularly concerned about privacy risks to remove their information from the pipeline” \*\*\* “By setting the default rule to ‘no information flow,’ an opt-in system restricts the information lifeblood on which today’s economic activity depends.”).

<sup>12</sup> EPIC Comments, at 7.

<sup>13</sup> 47 C.F.R. § 64.2008(c)(7) (requiring, *inter alia*, that notices “be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer”).

<sup>14</sup> *Id.* § 64.2008(d).

<sup>15</sup> EPIC Comments, at 8. In addition, *Ting v. AT&T*, 182 F. Supp. 2d 902 (N.D. Cal. 2002), has no bearing on whether the current CPNI opt-out regime is sufficient, as *Ting* did not involve consumer privacy. Instead it involved what was ultimately deemed an unconscionable contract

afield from the issue before the Commission. Carriers subject to the Commission’s CPNI rules have on-going relationships with their customers involving the provision of an ever-increasing array of complex services.<sup>16</sup> In its previous rulemaking, the Commission carefully considered the different choice options for carrier CPNI sharing, and concluded that opt-out is appropriate for sharing with JVs or ICs that offer communications-related services on the carrier’s behalf, while opt-in should be required for sharing with third parties.<sup>17</sup> None of EPIC’s “evidence” casts doubt on this reasoning.

## 2. *EPIC’s Use of Surveys and Polls is Misleading*

EPIC’s citation to polling data that purports to show that consumers prefer opt-in regimes is also unconvincing.<sup>18</sup> There is no indication that the pollsters asked consumers whether they would prefer an opt-in requirement if information was shared only with affiliates or comparable entities. Nor is there any evidence that the benefits of such sharing (information regarding new, expanded, or lower priced services) was a consideration presented to the poll respondents.

---

because the court found it to be a contract of adhesion. The court explained that the hallmark of a contract of adhesion is no choice whatsoever. *See Ting v. AT&T*, 319 F.3d 1126, 1149 (9th Cir. 2003). Under the CPNI rules, the limited opt-out is clearly a choice within the control of the customer.

<sup>16</sup> Moreover, cable operators such as Charter are already prohibited from using “negative option” billing practices and must have the specific affirmative request of the customer in order to bill for any service or equipment. 47 U.S.C. § 543(f).

<sup>17</sup> *See Third Report and Order*, at 14,880-888, ¶¶ 45-52, 63.

<sup>18</sup> For example, EPIC emphasizes the high percentage of consumers who support requiring customer consent before sharing driver’s license information. However, the question was posed in the context of whether customers approve of state governments selling driver’s license and car registration information to businesses as a means to raise government funds, not whether a company with whom a consumer has an ongoing relationship would like to share information to market additional new and enhanced *related* services to the consumer. *See Anders Gyllenhaal & Ken Paulson, Freedom of Information in the Digital Age*, Apr. 2001, at <http://www.freedomforum.org/>.

Charter believes that consumers want to receive service-related information from their carrier.<sup>19</sup> The current opt-in/opt-out regime is a carefully constructed, narrowly tailored means to balance both the consumer's privacy *and* commercial interests.<sup>20</sup> This balancing is especially important in light of the increasing number of companies utilizing and depending on third party JVs and ICs to either provide cost-effective communications-related services or to market services on the carrier's behalf. Requiring opt-in now will therefore immediately and negatively "impact the way carriers conduct business."<sup>21</sup>

EPIC itself cites a poll stating that "*if given a choice*, 90% of Internet users would either always or sometimes *opt out* of information collection."<sup>22</sup> But the CPNI rules afford consumers this very choice. Consumers who prefer that their CPNI not be shared can instruct their carriers accordingly because the current rules allow customers to opt-out.<sup>23</sup> Just as carriers should respect their customers' privacy preferences, the Commission should respect consumers' ability to determine their preferred level of privacy in light of their desire to receive cost-effective services.

---

<sup>19</sup> See Cingular Wireless Comments, at 4 ("The goal of protecting CPNI must be continuously tested, however, against the needs of Cingular's fifty-million plus customers who require convenient access to their own information.").

<sup>20</sup> See Charter Comments, at 13-20; *see also* T-Mobile Comments, at 14 ("Commission's 'total service approach' and the existing opt-in and opt-out requirements are reasonable and the product of extended deliberations by the Commission and the courts.").

<sup>21</sup> Charter Comments, at 17 (citing *Third Report and Order*, at 14,881 ¶ 45).

<sup>22</sup> EPIC Comments, at 10 (citing to *Business Week/Harris Poll: A Growing Threat*, BUSINESSWEEK, Mar. 20, 2000, at [http://www.businessweek.com/2000/00\\_12/b3673010.htm](http://www.businessweek.com/2000/00_12/b3673010.htm), which asked, "If privacy notices allowed you to 'opt-out,' letting you choose not to have your personal information collected by a particular Web site, how often would you 'opt-out'?" (emphasis added)).

<sup>23</sup> Charter Comments, at 18.

### 3. *U.S. West v. FCC Remains Good Law*

EPIC's attempt to characterize *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999) as an anomaly or as anything other than good law is disingenuous.<sup>24</sup> In *U.S. West*, the Tenth Circuit vacated the Commission's first attempt at promulgating CPNI rules, which contained an opt-in requirement. The court found that even if the government's interest in enacting the CPNI rules was substantial and the Commission's regulations directly and materially advanced those interests, the Commission did not sufficiently narrowly tailor its rules as the First Amendment requires.<sup>25</sup> The opt-out approach adopted in the current rules corrected this error. EPIC's citation to various cases upholding privacy laws against commercial speech challenges do not weaken *U.S. West* or call its reasoning into question.

While most of EPIC's cases are distinguishable simply because they do not involve information sharing, they are distinguishable on other grounds, as well. For example, *White Buffalo Ventures LLC v. Univ. of Texas*, 420 F.3d 366 (5th Cir. 2005) did not even discuss the opt-in or opt-out option because it did not involve customer choice. The issue was whether a university could block intrusive spam email messages to its students, and the case was easily decided on other grounds. In *Missouri ex rel. Nixon v. Am. Blast Fax, Inc.*, 323 F.3d 649, 660 (8th Cir. 2003), the court found the blanket restriction on unsolicited fax advertising (which could be overridden by a company securing opt-in of potential recipients) was narrowly tailored because of circumstances unique to that medium – namely the “cost shifting” associated with

---

<sup>24</sup> EPIC Comments, at 11 (stating that “[s]ince [U.S. West] was decided, every major challenge to privacy law based on commercial speech has failed.”).

<sup>25</sup> In light of recent events, the Missouri Public Service Commission contests the Tenth Circuit's finding that “no evidence showing the harm to either privacy or competition is real.” Missouri PSC Comments, at 6. The Court's holding was not dependent on its determination of no substantial harm. Even if the Missouri PSC is correct, the lack of narrow tailoring was and

unsolicited faxes, specifically “recipients ... are forced to contribute ink, paper, [sustain] wear on their fax machines, ... personnel time ... and use of their machines by preempting the fax line.” 323 F.3d at 652, 659.<sup>26</sup>

And although EPIC cites *Mainstream Mktg. Servs. v. FTC*, 358 F.3d 1228 (10th Cir. 2004), that case actually affirmed an approach that is very similar to the Commission’s current CPNI opt-out option. The case involved the FTC’s Do-Not-Call program, which requires the public to affirmatively *opt-out* of telephone marketing by signing up to the national Do Not Call registry or by signing up on a company-specific Do Not Call list.<sup>27</sup>

Other cases cited by EPIC are similarly unpersuasive. *Trans Union v. FTC*, 245 F.3d 809 (D.C. Cir. 2001) involved a statutory ban on sale of consumer reports to *third parties* for targeted marketing purposes. The case is inapplicable because the Commission has already concluded that disclosure of CPNI to affiliates, JVs, and ICs offering communications-related services is

---

remains sufficient to strike down any new CPNI rules that remove the limited opt-out choice that companies can provide customers.

<sup>26</sup> In 2005, Congress enacted and the President signed into law the Junk Fax Prevention Act of 2005, PL 109-21, July 9, 2005, 119 Stat. 359, which allows companies to send commercial faxes to entities with whom they have an established business relationship as long as opt-out notice is provided. *See* 47 U.S.C. §§ 227(b)(1)(C) and (2)(D); *see also In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order and Third Order on Reconsideration, CG Docket Nos. 02-278; 05-338; FCC 06-42 (rel. Apr. 6, 2002). The law was passed because “[t]he cost and effort of compliance [with the Commission’s then-existing junk fax rules] could place significant burdens on some businesses” in their efforts to market their services to their customers. S. Rep. 109-76, 109th Cong., 1st Session, at 6 (2005).

<sup>27</sup> 358 F.3d at 1242. The court in *Mainstream Mktg. Servs.* loosely refers to the Do Not Call Registry as an “opt-in feature” but was not examining the details of opt-in versus opt-out choice. Instead it was using the language to distinguish any consumer choice regime from “laws that prohibit speech directly.” *Id.* Also, the different nature of the Do-Not-Call rules and the CPNI rules explains why the court did not cite to *U.S. West*. EPIC Comments, at 12. Nowhere did the court in *Mainstream Marketing Services* say it was overruling or disapproving its prior holding in *U.S. West*, as EPIC suggests.

not like a disclosure to “third parties.”<sup>28</sup> In an identically styled case, *Trans Union v. FTC*, 295 F.3d 42 (D.C. Cir. 2002), the court rejected consumer reporting agencies’ attempts to re-use personal information obtained from financial institutions when the financial institution had already offered the customer notice and *opt-out* choice. The Court rejected the First Amendment challenge because “[t]here is no reason to believe a consumer would be more eager to relinquish his privacy right to a CRA that subsequently obtains his NPI [non-public personal information] than he was to the financial institution with which he initially dealt.” *Id.* And in *Anderson v. Treadwell*, 294 F.3d 453 (2d Cir. 2002), also curiously cited by EPIC, the Court approved an *opt-out* regime similar to the Commission’s current CPNI rules and is, thus, of no help to EPIC’s position in this proceeding.

The current rules are a reasonable accommodation of both privacy protection and commercial convenience and are narrowly tailored to meet the Commission’s objectives. Whether the Commission’s previous rules requiring customers to affirmatively authorize CPNI sharing with JVs and ICs might survive a legal challenge today is irrelevant. The Commission’s current opt-in/opt-out regime remains sound policy and should be maintained.

#### 4. *Most U.S. Privacy Laws Use an Opt-out Regime*

EPIC’s statement that “[a]n opt-in framework would better protect individuals’ rights, and is consistent with most United States privacy laws” is false.<sup>29</sup> Most U.S. Privacy laws use an opt-out framework, especially in the context of an ongoing business relationship between a service provider and a customer where the information is not being provided to unrelated third parties, as is the case with the Commission’s CPNI rules. For example, one of the most

---

<sup>28</sup> *Third Report and Order*, at 14,880-888 ¶¶ 45-52, 63 and n. 151 (distinguishing yet another identically styled case, *Trans Union Corp. v. Federal Trade Comm’n*, 267 F.3d 1138, 1143 (D.C. Cir. 2000) because it involved third-party disclosure).

prominent U.S. privacy laws, the Gramm Leach Bliley Act (“GLBA”), takes an approach to the sharing of “non-public personal information” that is much more liberal than the Commission’s CPNI rules.<sup>30</sup> Yet, the legislative history reveals that Congress believed it would “provide some of the strongest privacy protections to ever be enacted into federal law,<sup>31</sup> and would “represent the most comprehensive federal privacy protections ever enacted by Congress.”<sup>32</sup>

But despite Congress’ view that GLBA contained effective privacy protections – and it certainly does – those protections are not as far-reaching as the Commission’s current CPNI rules. GLBA does not, for example, require consumer approval at all for sharing of non-public personal information with affiliates, third parties who perform marketing and other functions on behalf of a financial institution, and certain joint venture partners.<sup>33</sup> And GLBA only authorizes consumers to direct, through an *opt-out* mechanism, that their non-public personal information not be shared with *nonaffiliated* third parties.<sup>34</sup> Thus, the Commission’s CPNI rules are plainly more protective than the GLBA.

Other U.S. privacy laws are also less restrictive on information sharing than the Commission’s CPNI regime. For example, the Fair Credit Reporting Act (“FCRA”), as amended by the Fair and Accurate Credit Transactions Act (“FACT Act”), specifically allows certain

---

<sup>29</sup> EPIC Comments, at 9.

<sup>30</sup> 15 U.S.C. § 6801 *et. seq.*

<sup>31</sup> 145 Cong. Rec. H11, at 539-40 (daily ed. Nov. 4, 1999) (statement of Rep. Vento)

<sup>32</sup> 145 Cong. Rec. H11, at 544 (daily ed. Nov. 4, 1999) (statement of Rep. Sandlin).

<sup>33</sup> 15 U.S.C. § 6802(b)(2).

<sup>34</sup> *Id.* at § 6802(b)(1). California’s attempt to impose an opt-out requirement on financial institutions’ sharing of non-public personal information among affiliates through passage of SB 1 in 2003 was subsequently found to be preempted by the Fair Credit Reporting Act, as amended by Fair and Accurate Credit Transactions Act. *See American Banker’s Assn’ v. Gould*, 412 F.3d 1081 (9th Cir. 2005) and *American Banker’s Assn’n v. Lockyer*, No. Civ. S04-0778MCE KJM, 2005 WL 2452798 (E.D. Cal. Oct. 5, 2005) (on remand).

information covered by the statute to be shared with affiliates for marketing purposes under an opt-out regime.<sup>35</sup> Moreover, where the entity is marketing to customers with whom they have a pre-existing business relationship, providing these customers with an opt-out choice is not required.<sup>36</sup> The Electronic Communications Privacy Act, cited by EPIC, actually allows providers of remote computing service or electronic communications service to disclose customer records (but not the contents of communications) to non-governmental entities without customer consent of any type.<sup>37</sup> And the Cable Communications Policy Act, also cited by EPIC, allows disclosure to third parties without customer consent in certain instances, including as necessary to “conduct a legitimate business activity related to a cable service or other service provided by the cable operator to the subscriber.”<sup>38</sup>

Other U.S. privacy laws that do not directly involve disclosure of personal information, including the CAN-SPAM Act, also require consumers to opt-out to avoid receiving future solicitations.<sup>39</sup> Congress adopted an “opt-out” approach for curbing unwanted spam e-mail despite the fact that such intrusions are among the most annoying and potentially dangerous facing consumers in cyberspace today. Charter believes that consumers find marketing from a communications service provider with whom the customer has a longstanding relationship, especially when the marketing informs customers about new and useful services and cost-saving bundled offerings, much less intrusive than spam e-mail. Also, as noted, the FTC’s Do-Not-Call

---

<sup>35</sup> *Id.* § 1681s-3 (referring to information that would be a consumer report, but for the provisions in 15 U.S.C. § 1681a(d)(2)(A), which encompasses what is referred to in the banking industry as “experience information” and “non-experience information.”).

<sup>36</sup> *Id.* at § 1681s(a)(4)(A).

<sup>37</sup> 18 U.S.C. § 2702(c)(6).

<sup>38</sup> 47 U.S.C. § 551(c)(2)(A).

<sup>39</sup> 15 U.S.C. § 7704(a)(3)(A)(i).

rules under the Telephone Consumer Protection Act, 47 U.S.C. § 227, and the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, respectively, also employ an opt-out regime and expressly exempt certain on-going business-consumer relationships from Do-Not-Call's prohibitions.<sup>40</sup> Given the greater connectivity between a carrier and the customer for communications-related services, requiring opt-in to share CPNI with affiliates, JV partners and ICs to provide or market "communications related services" is not reasonable.

**C. Because of Ever-Increasing Bundled Service Offerings, The Commission Should At a Minimum, Expand Its Definition of Communications-Related Service to Include Cable Video Service; It Should Also Add Video and Internet Access to Its Total Service Approach**

The American Cable Association ("ACA") noted that the current CPNI rules are outmoded in an era of bundled services.<sup>41</sup> For that reason, the ACA explained that cable operators should not have to obtain "opt-in" approval to use CPNI to market video services to customers.<sup>42</sup> Charter agrees. The current regime should be revised to reflect the reality that service providers are increasingly offering multiple services – voice, video, and data – and authorize the marketing of such cross-platform services. The Commission should, therefore, at a

---

<sup>40</sup> See 47 C.F.R. §§ 64.1200(c)(2), (d)(3) and (f)(9)(ii); 16 C.F.R. §§ 310.4(b)(1)(iii)(B)(ii) and 310.4(b)(1)(iii)(A); see also *supra*, note 26 (addressing the Junk Fax Prevention Act of 2005 and how it recognized an existing business relationship exception for fax solicitors).

<sup>41</sup> ACA Comments, at 6-7. It should go without saying that technological "convergence," and the ability to bundle previously disparate services made possible by convergence, is no longer something anticipated, it has arrived. Telephone companies and cable companies both now offer bundled packages of voice, data, and video. While regulatory distinctions between these service offerings still exist, they have gradually been eroding. Most significantly, the services themselves are overlapping with increasing integration of services. See *Cable Operators Expand into Other VoIP Services*, COMMUNICATIONS DAILY, Apr. 14, 2006, at 7-8. For example, cable operators will soon be introducing such services as "caller-ID on TV", which enables customers to control and monitor calls over the television screen and remote while watching TV. In addition, consumers will be able to control certain phone features through cable operators' broadband web portals. *Id.*

<sup>42</sup> ACA Comments, at 6-7.

minimum, modify its definition of “communications-related service” to include cable video service. Alternatively, for the same reasons, the Commission should modify its “total service approach” to include Internet access service and video services when consumers are subscribers to multiple services.

A cable video affiliate, like a joint-venture partner or independent contractor, should be able to access CPNI for marketing purposes when its affiliated carrier obtains CPNI from a VoIP offering over the cable video affiliate’s cable system, subject to opt-out approval when a customer does not already receive video service. A customer receiving multiple “telecommunications” services from the same company would not expect that company to maintain internal divisions, but would expect it to use the customer’s CPNI to provide cost-efficient service. As the Commission explained in its *Third Report and Order*, “telecommunications consumers expect to receive targeted notices from their carriers about innovative telecommunications offerings *that may bundle desired telecommunications services and/or products, save the consumer money, and provide other consumer benefits.*”<sup>43</sup>

To require more than an opt-out option for sharing CPNI with cable video affiliates, in light of bundled services, is counterproductive. Even in its 1998 *Second Report and Order*, the Commission recognized that the total service approach “facilitates any convergence of technologies and service in the marketplace.”<sup>44</sup> The Commission agreed it would be “desirable for carriers to provide integrated one-stop shopping, as past ‘product market’ distinctions ...

---

<sup>43</sup> *Third Report and Order*, at 14,877 ¶ 36.

<sup>44</sup> *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 F.C.C.R. 8061, 8106 ¶ 58 (Feb. 26, 1998).

blur.”<sup>45</sup> Although the Commission was focused on telecommunications service categories and did not appear to envision the type of convergence seen today, it did cite open video systems (“OVS”) as an example of a new service technology that the total service approach would be “sufficiently flexible to accommodate.”<sup>46</sup> OVS has not since been used widely for telephone carriers’ entry into video service, but cable video by telecommunications carriers is now occurring on a widespread basis.<sup>47</sup> Likewise, in 1998, the Commission did not envision the widespread entry by cable into telephone service using VoIP, an information service. The Commission should therefore adapt its CPNI rules to the current world of bundled consumer services.

### **III. EPIC’S PROPOSED SAFEGUARDS AND NOTICE RULES ARE UNNECESSARY AND COSTLY**

Charter agrees with the overwhelming majority of industry commenters that EPIC’s proposals are unnecessary. These proposals, which purportedly seek to better protect CPNI data and improve customer choice, do not actually address the pretexting problem, and will be prohibitively expensive to implement and maintain. EPIC’s recommendation that the Commission mandate passwords, for example, will not prevent fraud,<sup>48</sup> is generally inconvenient, and clearly limits consumer choice.<sup>49</sup> The Commission should not mandate

---

<sup>45</sup> *Id.* at 8111 ¶ 64.

<sup>46</sup> *Id.* at 8106 n.219.

<sup>47</sup> *In the Matter of Implementation of Section 621(a)(1) of the Cable Communications Policy Act of 1984 as Amended by the Cable Television Consumer Protection and Competition Act of 1992*, Notice of Proposed Rulemaking, MB Docket No. 05-311, FCC 05-189 (rel. Nov. 18, 2005) (hereinafter Section 621 NPRM).

<sup>48</sup> *See* Sprint Nextel Comments, at 11.

<sup>49</sup> *See* T-Mobile Comments, at 11 (finding that mandating passwords may conflict with consumer’s desire not to use passwords).

passwords, but should allow businesses to decide whether to offer passwords on their own.<sup>50</sup> Encryption is even less necessary, given that this type of protection is only relevant to hacking and other direct attacks on a company's system. As the Princeton University IT students recognize, it is unlikely that cyberattacks and theft of records were responsible for the recent disclosures of CPNI.<sup>51</sup> Moreover, encrypting all stored CPNI records would be prohibitively expensive.<sup>52</sup> Similarly, EPIC's audit trail proposal does not address pretexting, since it fails to proactively prevent pretexting while imposing additional storage and maintenance costs on carriers.<sup>53</sup>

EPIC's notice proposals likewise impose far too great a burden on companies without any appreciable benefit to consumers. Dobson Communications estimates that notice of any disclosure would be unworkable because it could generate 30,000-40,000 notices per day for Dobson alone.<sup>54</sup> Dobson also suggests that pre-disclosure notification to obtain authorization would be exceedingly frustrating and inconvenient for its customers.<sup>55</sup>

Charter agrees with the National Cable & Telecommunications Association ("NCTA") that post-breach notification would be an ineffective and unnecessary rule. If the carrier did not know the caller was a pretexter, it would not know that a breach occurred, and would not send a notice to the customer; likewise, if the carrier discovered that the caller was a pretexter, then the

---

<sup>50</sup> *See also* Charter Comments, at 25-28 (discussing passwords).

<sup>51</sup> Princeton University Students Comments, at 2.

<sup>52</sup> Charter Comments, at 29.

<sup>53</sup> *See* NCTA Comments, at 4.

<sup>54</sup> Dobson Comments at 7.

<sup>55</sup> Dobson Comments at 8. (envisioning the frustration and annoyance of a customer who, after going through automated voice prompts and then waiting to speak with a representative, is told that the representative must now call the customer's registered number to verify the customer's identity).

carrier would not disclose the information, and no breach would occur.<sup>56</sup> That is one of the reasons Charter argued in its initial comments that if the Commission does require breach notification to consumers, the obligation should only be triggered when a carrier has *knowledge* of a breach with a “significant risk” or “clear risk of danger or harm to the consumer.”<sup>57</sup>

EPIC’s proposal for limited data retention and de-identification would not affect the accessibility or the content of more recently compiled CPNI, which pretexters appear to value most,<sup>58</sup> and would likely conflict with federal and state laws. As the Departments of Justice and Homeland Security note, record destruction would result in the “inability to produce records in response to lawful authority” and “would have a significant negative impact on national security and public safety.”<sup>59</sup> Other commenters remind the Commission that state tax laws may be implicated if the Commission required the premature destruction of records.<sup>60</sup>

In response to the Commission’s request for commenters to “think broadly and creatively” about how to protect CPNI, EPIC admits that there are “myriad approaches to securing data, and new technologies may bring innovative approaches to the problem.”<sup>61</sup> That concession highlights why new mandates do not make sense. Technology will continue to evolve rapidly allowing service providers to adopt technologies that fit their particular business. EPIC instead suggests that the Commission should routinely revisit security issues on a planned

---

<sup>56</sup> NCTA Comments, at 6.

<sup>57</sup> Charter Comments, at 35.

<sup>58</sup> See Princeton University Students Comments, at 2 (recognizing that pretexters advertise ability to obtain up-to-date CPNI).

<sup>59</sup> DOJ/DHS Comments, at 4.

<sup>60</sup> See BellSouth Comments, at 23 (stating that current record retention is based on the statute of limitation for each state’s sales and use tax audits plus any extensions, which varies from state to state, making adoption of a uniform rule “exceedingly problematic”).

schedule, for example, every five to seven years. But a new Commission-mandated review every 5-7 years would not serve carriers' or customers' interests. Technology does not change on schedule. In five years, nothing substantial may occur. On the other hand, a revolution in security technology could occur in the next few months. More importantly, unless pretexters agree to follow this schedule and only develop new fraud tactics accordingly, it would be pointless to establish scheduled reviews. Pretexters and others who seek illegal access to CPNI will continue to search for new ways to defeat security systems (because no security system is perfect), and the industry and the Commission will review their systems accordingly. There is no need to have set review cycles with corresponding rule changes when review already occurs on a continuing basis.

**IV. IF THE COMMISSION DOES WANT TO PURSUE NEW APPROACHES, IT SHOULD BE VERY CAREFUL NOT TO BURDEN PROVIDERS AND THEREFORE HARM CONSUMERS**

**A. A More Reasonable Alternative to Regulatory Mandates Would Be an Industry-Wide Working Group**

To the extent the Commission requires action, Charter agrees with NCTA that “promulgating specific rules and standards [would be] excessively costly, ineffective and counterproductive.”<sup>62</sup> A better approach would be to “establish an industry-wide working group to address the problem systematically.”<sup>63</sup> Such a group could more effectively discuss, in private, how brokers and pretexters are exploiting current safeguards and what safeguards work best.<sup>64</sup> These discussions, “with fewer adverse costs and effects, through a working group approach than

---

<sup>61</sup> EPIC Comments, at 16. It should be noted that this statement serves to refute, rather than support, EPIC’s own proposals for rigid technological mandates like passwords and encryption.

<sup>62</sup> NCTA Comments, at 6.

<sup>63</sup> *Id.*

<sup>64</sup> *Id.*

through formal, public and inflexible rules,” could lead to new industry standards, thereby fulfilling the objectives of the Commission without the need for new rules and regulations<sup>65</sup> Charter, therefore, agrees that the Commission should encourage the industry to cooperate with consumer privacy groups and establish a working group to address the CPNI issue.

**B. If the Commission Enacts New Rules, a Carrier Safe Harbor Provision for CPNI is Desirable.**

CPNI disclosures are often the result of pretexters defrauding carriers, and not the fault of carriers themselves. Charter, therefore, agrees with Verizon Wireless’ suggestion that, whatever procedures the Commission adopts, it should include a safe harbor provision so that carriers will not be liable for unauthorized disclosure if they can show that they reasonably and routinely follow a set of established, acceptable CPNI protection practices.<sup>66</sup> As Verizon Wireless notes, “the prima facie violation is the product of a third party’s fraudulent conduct,” not carrier error, further illustrating why a safe harbor provision for CPNI makes even more sense.<sup>67</sup> Indeed, a safe harbor policy makes sense in the context of CPNI, because no matter how many rules and procedures are followed, CPNI will still be vulnerable to pretexters, who will undoubtedly continue their efforts to circumvent carriers’ security procedures.<sup>68</sup>

**C. Whether or Not the Commission Enacts New Rules It Should Preempt More Restrictive State Laws**

Centennial Communications recognizes that “[i]mplementing, potentially, over fifty different state-level CPNI compliance programs, as well as a federal ‘overlay’ scheme, is

---

<sup>65</sup> *Id.*

<sup>66</sup> Verizon Wireless Comments at 20.

<sup>67</sup> *Id.* at 20-21. If the disclosure was due to carrier error, then presumably the safe harbor provision would not apply. The safe harbor provision could be similar to the one found in the Commission’s Do-Not-Call rules, under 47 C.F.R. § 64.1200(c)(i)

<sup>68</sup> Verizon Wireless Comments at 21.

unworkable, overly burdensome and unnecessary.”<sup>69</sup> Although many state legislative proposals appropriately address pretexters, as opposed to carriers,<sup>70</sup> others do not. Georgia, for example, seeks to impose criminal liability on carriers, and other states may follow suit.<sup>71</sup> In addition, the Pennsylvania Public Utilities Commission (“Pa PUC”) argues against preemption, suggesting that federal regulations should remain a “regulatory floor as opposed to a regulatory ceiling.”<sup>72</sup>

Charter disagrees. Allowing states to individually and independently implement a wide variety of more restrictive security standards would create a compliance nightmare and would interfere with carriers’ abilities to efficiently provide uniform service to customers. Inconsistent state rules could make compliance difficult (if not impossible) and create unnecessary but costly disputes over which state’s law applied when the carrier and customer resided in different states. The Commission should therefore exercise its authority to preempt state regulations to the extent that they are more restrictive than the Commission’s rules.<sup>73</sup>

---

<sup>69</sup> Centennial Communications Comments at 5-6.

<sup>70</sup> See Charter Initial Comments at 11 n.34.

<sup>71</sup> See Centennial Communications Comments at 6; see also Charter Initial Comments at 11 n.34 (citing Connecticut H.B. 5783 as another bill that would impose new standards on carriers).

<sup>72</sup> Pa PUC Comments at 3.

<sup>73</sup> It is well established that “[t]he statutorily authorized regulations of an agency will preempt any state or local law that conflicts with the regulations or frustrates the purposes thereof.” *City of New York v. FCC*, 486 U.S. 57, 64 (1988). Moreover, it is of no significance that Congress did not expressly state that more restrictive interstate regulations would be preempted as “[a] pre-emptive regulation’s force does not depend on express congressional authorization to displace state law.” *Id.* (quoting *Fidelity Federal Savings & Loan Ass’n v. De la Cuesta*, 458 U.S. 141, 154 (1982)). Indeed, even where Congress has preserved some role for the states, the Supreme Court has found that “state law is nullified to the extent that it actually conflicts with federal law.” *De la Cuesta*, 458 U.S. at 153.

