

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

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996;	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information;	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277
	)	

To: The Commission

**REPLY COMMENTS OF  
DOBSON COMMUNICATIONS CORPORATION**

Dobson Communications Corporation (“Dobson”) hereby submits its reply comments in the above-captioned proceeding.<sup>1</sup> Most commenters agree that imposition of additional prescriptive measures for carriers in the handling of Customer Proprietary Network Information (“CPNI”) is both unnecessary and unwarranted. Those favoring additional regulation point to no direct evidence of a continuing problem that needs fixing and provide no consensus on what measures are needed. Dobson thus urges the Commission to refrain from taking any actions that will merely burden the customer-carrier relationship without any significant benefit to consumers. To the extent that additional regulatory obligations are imposed, Dobson again urges the Commission to include regional Tier II carriers within any relief provided to smaller carriers.

---

<sup>1</sup> *Implementation of the Telecommunications Act of 1996*, CC Docket No. 96-115, *Notice of Proposed Rulemaking*, FCC 06-10 (rel. Feb. 14, 2006) (“*NPRM*”).

## DISCUSSION

The root problem is criminals fraudulently pretending to be customers who, until recently, could practice their fraud relatively risk free.<sup>2</sup> Dobson agrees with Verizon Wireless that “[t]he best way to stop pretexters is to put them out of business.”<sup>3</sup> No level of security will completely stop the theft of phone records,<sup>4</sup> but the EPIC petition and ensuing media attention have highlighted the issue for the country, resulting in (i) proposed state and federal legislation that would clearly outlaw and impose serious penalties for pretexters; (ii) stepped up enforcement activity by the Federal Trade Commission and state attorney generals; and (iii) increased civil litigation by carriers to stop the trafficking of phone records.<sup>5</sup> And the record shows that these actions have already had a chilling effect, resulting in the closing of data broker websites.<sup>6</sup> The Commission should not impose additional regulatory obligations until the full effects of these efforts are felt.

---

<sup>2</sup> Some commenters allege that employee “insiders” are engaging in fraud and point to studies performed in the financial industry, but there is no hard evidence to support such claims of abuse in the telecommunications industry. *See* Electronic Privacy Information Center *et al.* (“EPIC”) Comments at 14. Moreover, these allegations contradict Dobson’s own experiences that show “pretexting,” not insider fraud, as the primary method used to obtain CPNI without the subscriber’s authorization.

<sup>3</sup> Verizon Wireless Comments at ii.

<sup>4</sup> The record shows that carriers have every incentive to implement, and have implemented, meaningful security measures to protect CPNI. *See* Alltel Corp. Comments at 4-5; California Public Utility Commission Comments at 2-3; Centennial Communications Corp. (“Centennial”) Comments at 3-4; Cingular Wireless LLC (“Cingular”) Comments at 3, 18; Dobson Comments at 3-5; MetroPCS Comms. Inc. (“MetroPCS”) Comments at 6, 10; Sprint Nextel Comments at 10 n.25; T-Mobile Comments at 8-11; Verizon Wireless Comments at 8-9, 16. Dobson notes that it had replaced the web access blocking option with a web access double password option prior to the filing of its comments. *See* Dobson Comments at 5.

<sup>5</sup> *See* Cingular Comments at 11-12; Dobson Comments at 3 n.5; National Association of Attorney Generals (“NAAG”) Comments at 3 n.7; Missouri Public Service Commission (“MO PSC”) Comments at 6-7; Sprint Nextel Comments at 7-8; Verizon Wireless Comments at 5-6.

<sup>6</sup> *See* Cingular Comments at 3 n.4; Cross Tel. Co. *et al.* Comments at 3-6; Sprint Nextel Comments at 8; Verizon Wireless Comments at 2; *see also* Jennifer C. Kerr, “Websites hawking phone records shut down,” USA Today (rel. Feb. 8, 2006).

Moreover, the record clearly demonstrates that the prescriptive measures under consideration in this proceeding will not cure the problem of pretexting. Indeed, even proponents of new regulation questioned whether the additional regulatory obligations proposed by EPIC will provide the desired level of security, recognizing that:

- passwords are not a panacea and establishing passwords for all existing accounts would be a “monumental task;”<sup>7</sup>
- “audit trails do little to prevent the unauthorized release of consumer information” but simply aid in identifying disclosure after the fact;<sup>8</sup> and
- encryption will not prevent pretexting and rogue insiders from obtaining CPNI.<sup>9</sup>

Most commenters also agree that prescriptive regulations will unduly burden carriers and consumers. Those supporting audit trails and advance or post-notifications to consumers when CPNI is accessed, used and disclosed fail to appreciate the burden of such requirements on carriers and consumers.<sup>10</sup> As Verizon Wireless, Dobson and others pointed out, just about every customer service inquiry involves the access and use of CPNI, because CPNI does not only include sensitive call record data (the disclosure of which is of the greatest concern to the public

---

<sup>7</sup> MO PSC Comments at 2. The Missouri PSC states that if individuals possessing biographical data obtained from the Internet “are able to obtain unauthorized access to customer accounts, then presumably these same entities will be able to obtain access to the password associated with an account.” MO PSC Comments at 3. The National Assoc. of State Utility Consumer Advocates (“NASUCA”) states that neither consumer-set passwords nor “shared secret” security systems alone “appears to be adequate to guard against unauthorized use of CPNI.” NASUCA Comments at 14. Many consumers use a single passcode for multiple accounts undercutting the effectiveness of consumer-set passwords. NASUCA Comments at 15; MO PSC Comments at 3. NASUCA correctly points out that people forget passwords and call customer service representatives when they are misplaced or forgotten, resulting in the need for a subscriber verification process that is susceptible to data brokers armed with biographical identifiers. NASUCA Comments at 16.

<sup>8</sup> MO PSC Comments at 3.

<sup>9</sup> While encryption is already utilized by carriers to a certain extent to secure information from “hacking,” there is no evidence of a problem with “hacking” that would warrant the imposition of an encryption requirement. *See* Sprint Nextel Comments at 5 (“unaware of any instance in which an unauthorized person obtained CPNI by electronically ‘hacking’ into any Sprint Nextel information system”); Verizon Wireless Comments at 4 (“not aware of any cases in which data brokers were able to obtain such information through ‘hacking’”).

<sup>10</sup> For example, the State of New Jersey Rate Payer Advocate concludes that “carriers already must record CPNI disclosure for marketing purposes or to third parties (47 C.F.R. § 64.2009(c)), and, therefore, the marginal cost to also record disclosure to purported account holders should be small.” *See* State of New Jersey Comments at 4.

and lawmakers) but also general billing and service plan information.<sup>11</sup> Wireless carriers receive millions of customer service inquiries each month and expanding audit trails and notification requirements to each time CPNI is accessed, used, or disclosed would lead to costly upgrades even if a carrier already has procedures or information technology systems in place that provide such functionality to a limited degree.<sup>12</sup> In addition, imposition of these measures will increase delays for consumers when accessing their account information, increase the number of unwanted carrier intrusions into their daily lives, and simply create confusion.<sup>13</sup> The Commission should not impose regulation when, as here, the cost clearly outweighs any conceivable benefit to consumers.

Dobson is troubled by the suggestions of EPIC, NAAG and NASUCA that carriers should be required to obtain customer consent before sharing CPNI with joint venture partners, affiliates, and independent contractors even when the disclosure is in connection with providing services to which the customer already subscribes.<sup>14</sup> First, there is absolutely no evidence of a problem of such entities making unauthorized disclosures of CPNI; statements that CPNI in the hands of third parties contributes to the problem are sheer speculation. Second, carriers, especially smaller businesses, rely extensively on independent contractors to assist in the

---

<sup>11</sup> See 47 U.S.C. § 222(h)(1); Verizon Wireless Comments at 14.

<sup>12</sup> See Cingular Comments at 22 (stating that it receives approximately 380,000 customer service calls a day); CTIA Comments at 16 (reiterating that there are over 100 million customer service inquiries received each year); Verizon Wireless Comments at 14, 17 (recording each customer service call would cost approximately \$8 million per year); see also Princeton University Students Comments at 5 (“requiring carriers to notify customers of routine CPNI transfers is too burdensome and adds little value to the consumer who wants to protect his CPNI”).

<sup>13</sup> If consumers are inundated with notifications, they will also become immune to them and simply ignore them in time, further undercutting any purported benefit. See e.g., NASUCA Comments at 7-8 (stating that notwithstanding the technical limitations of providing customer notices in a bill or bill insert, consumers may become immune to another line item description).

<sup>14</sup> See EPIC Comments at 6; NAAG Comments at 5; NASUCA Comments at 3-4.

provision of competitive low-cost service with innovative features.<sup>15</sup> Finally, comments favoring obtaining customer approval before sharing CPNI in the context of the “total services” approach are outside the scope of the *NPRM*, completely unworkable, and contrary to Section 222 of the Act.<sup>16</sup>

To the extent the Commission determines that new regulation is appropriate, Dobson supports, conceptually, the Cingular and Verizon Wireless proposals advocating adoption of a “safe harbor” that is based on general voluntary standards for protecting CPNI that would shield a carrier from liability while giving carriers the flexibility to determine which security safeguards are needed to address ever-changing security threats.<sup>17</sup> If the Commission nevertheless imposes prescriptive safeguards, then Dobson urges the Commission to include Tier II carriers within any

---

<sup>15</sup> Carriers utilize independent contractors for a wide variety of functions, including printing and mailing of bills, fraud detection, off site data backup and CALEA compliance. *See Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, *Second Report and Order and Memorandum Opinion and Order*, FCC 06-56 at ¶ 26 (rel. May 3, 2006) (giving providers the option of using trusted third parties that have access to a carriers’ network for the provision of a variety of services for CALEA compliance, including processing requests for intercepts, conducting electronic surveillance, and delivering relevant information to law enforcement agencies); *see also* Alltel Corp. Comments at 4 (noting that smaller carriers rely on outsourcing to obtain operational efficiencies).

<sup>16</sup> Section 222 expressly authorizes carriers to use and disclose CPNI without the subscriber’s consent in the provision of service from which the CPNI was derived. 47 U.S.C. § 222(c)(1). Further, in the *NPRM*, the Commission only sought comment on whether the “opt-out” regime for sharing CPNI with joint venture partners and independent contractors that provide communications-related services to which the customer does not already subscribe should be changed to “opt-in” consent and whether to provide “opt-in” notification before releasing CPNI to a subscriber. *See NPRM* at ¶¶ 12 n.35, 22-23.

<sup>17</sup> Cingular suggested that insofar as the Commission is inclined to adopt regulations, it should adopt “safe harbor” guidelines based on the Federal Trade Commission’s Safeguards Rule that provides for: (i) designating an employee or employees to coordinate the information security program; (ii) having a risk assessment process to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information; (iii) designing and implementing information safeguards to control the risks identified in the risk assessment process; (iv) overseeing service providers; and (v) evaluating and adjusting the information security program in light of the results of testing and monitoring of procedures. *See Cingular Comments* at 32-33. Verizon Wireless supported the following voluntary standards: (i) carriers must develop detailed written CPNI security procedures and conduct regular training of employees in the security of customer information; (ii) carriers must verify that the account holder or an authorized party on the account is on the phone, in the store, or online (verification procedures can and should vary, but each carrier should have such procedures in writing); (iii) the customer’s social security number, tax identification number, and billing address should not be made available to individuals calling to request it, including the account holder; and (iv) carriers should give customers the option to password protect their account information. *See Verizon Wireless Comments* at 21.

regulatory relief provided for smaller businesses.<sup>18</sup> The Commission should not label and treat regional providers, like Dobson, as large carriers when Tier I carriers have 10-30 times more subscribers. Dobson, like other smaller carriers, serves primarily less-populated suburban and rural areas and does not have the customer base of national carriers over which to spread the fixed costs associated with additional CPNI requirements. The subscribers of small and regional carriers will therefore bear a higher proportion of the costs of additional CPNI measures than will the subscribers of the Tier I carriers.<sup>19</sup>

Finally, Dobson opposes the Pennsylvania PUC's suggestion that the FCC employ cooperative federalism in imposing and enforcing CPNI requirements on carriers. The Pennsylvania PUC's suggested approach would lead to different, and perhaps conflicting, CPNI requirements in fifty states that are simply unworkable for commercial wireless service providers that operate their businesses without regard to state lines.<sup>20</sup>

---

<sup>18</sup> See also Rural Cellular Association Comments at 5-6 (urging the Commission not to burden regional and small wireless carriers from new CPNI obligations).

<sup>19</sup> See, e.g., Princeton University Students Comments at 11 ("The costs of upgrading technology are likely to fall disproportionately on small carriers.").

<sup>20</sup> For example, Dobson like most carriers offers regional and nationwide service plans and has national call centers taking customer inquiries from every state served by Dobson.

## **CONCLUSION**

For the reasons stated above, Dobson urges the Commission not to adopt the prescriptive measures for the handling of CPNI that are under review in this proceeding.

Respectfully submitted,

**DOBSON COMMUNICATIONS CORPORATION**

By: /s/ Ronald L. Ripley  
Ronald L. Ripley, Esq.  
Senior Vice President & General Counsel  
Dobson Communications Corporation  
14201 Wireless Way  
Oklahoma City, OK 73134  
(405) 529-8500

June 2, 2006