

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

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

COMMENTS OF CROSS TELEPHONE COMPANY, CIMARRON TELEPHONE COMPANY, POTTAWATOMIE TELEPHONE COMPANY, CHICKASAW TELEPHONE COMPANY, AND SALINA-SPAVINAW TELEPHONE COMPANY

Cross Telephone Company, Cimarron Telephone Company, Pottawatomie Telephone Company, Chickasaw Telephone Company, and Salina-Spavinaw Telephone Company (the "Oklahoma Carriers"), by their attorneys, respectfully submit the following comments in response to the FCC's Notice of Proposed Rulemaking regarding potential changes to the regulation of telecommunications carriers as it relates to customer proprietary network information ("CPNI") and other customer information.¹ The Oklahoma Carriers provide, directly or through affiliates, local exchange, exchange access, Internet access, long-distance, wireless, and other telecommunications and information services in rural areas of Oklahoma.

¹ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, Notice of Proposed Rulemaking, FCC 06-10 (rel. Feb. 14, 2006) ("NPRM").

I. Summary

The Commission is seeking comments on new proposals to address CPNI security. The petition by the Electronic Privacy Information Center (“EPIC”) asserts that additional CPNI rules could help prevent fraudulent activities by data brokers who wrongfully obtain access to CPNI by impersonating the customer, a practice known as “pretexting.” While the Oklahoma Carriers agree that pretexting is a violation of consumer privacy, the Oklahoma Carriers believe that current laws are adequate to address pretexting, and additional FCC regulation of telecommunications carriers is not warranted at this time.

Pretexting already is subject to significant federal and state sanctions. Consumers are adequately protected by these laws, as well as by the safeguards that telecommunications carriers already have put in place, at significant expense, implementing Section 222 of the Communications Act and the Commission’s existing CPNI rules. Pursuant to these rules, every carrier must protect the privacy of CPNI and respect customers’ wishes as to its use and disclosure, both within the carrier’s organization and with respect to third parties. Any possible added protection that might be gained from even stricter CPNI access rules must be weighed against the price to be paid by customers, both directly through carrier fees, and indirectly, through loss of access to services and the inconvenience associated with complex security measures. CPNI is appropriately addressed by customer choice and carrier compliance with the current CPNI rules.

II. Federal and State Law Provide Significant Deterrence To Pretexting

Pretexting violates existing federal and state law and is being actively prosecuted by law enforcement authorities. The Federal Trade Commission (“FTC”) is actively investigating data brokers and recently stated that it “plan[s] to pursue these investigations

vigorously.”² The FTC has further stated that “[m]aintaining the privacy and security of consumers’ personal information is one of the Commission’s highest priorities.”³ The FTC has asserted its authority to prosecute CPNI data brokers under section 5 of the Federal Trade Commission Act,⁴ which prohibits “unfair or deceptive acts or practices in or affecting commerce.”⁵ FTC staff have identified targets for investigation and have completed undercover purchases of phone records.⁶ The FTC currently is considering its enforcement alternatives.⁷

State attorneys general also are actively pursuing pretexters for violations of state law. A number of states have brought actions against data brokers, including California,⁸ Florida,⁹ Illinois,¹⁰ Missouri,¹¹ and Texas.¹² These efforts are meeting with success. For

² Prepared Statement of the Federal Trade Commission, Before the Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Affairs, Product Safety, and Insurance, U.S. Senate, On Protecting Consumers’ Phone Records, at 1 (Feb. 8, 2006), available at <http://www.ftc.gov/os/2006/02/commissiontestimonypretexting060208.pdf> (“FTC Statement”) (stating that the FTC is “currently investigating companies that offer consumer telephone records for sale”).

³ *Id.*

⁴ *Id.* at 7.

⁵ 15 U.S.C. § 45(a).

⁶ FTC Statement at 8.

⁷ *Id.*

⁸ Press Release, Office of Attorney General, State of California, Attorney General Lockyer Files Lawsuit Against Data Trace USA for Illegally Obtaining and Selling Cell Phone Records (Mar. 14, 2006), available at <http://ag.ca.gov/newsalerts/release.php?id=1269> (suit alleges violations of state law prohibiting unfair business practices and false or deceptive advertising, and seeks restitution as well as over \$10 million in civil fines).

⁹ Press Release, Office of the Attorney General of Florida, Crist Sues Data Brokers Over Sale of Telephone Records (Jan. 24, 2006), available at <http://myfloridalegal.com/newsrel.nsf/newsreleases/D510D79C5EDFB4B98525710000539060>; Press Release, Office of the Attorney General of Florida, Crist Charges Second Data Broker Over Sale of Phone Records (Feb. 24, 2006), available at <http://myfloridalegal.com/newsrel.nsf/newsreleases/40265981391EDECE8525711000659BA9>.

example, the Attorney General of Florida recently filed suit against 1st Source Information Specialists, Inc., and the defendant's operation was shut down in approximately two weeks.¹³

Likewise, the Attorney General of Missouri already has successfully sued multiple data brokers, generally achieving favorable results in a matter of weeks.¹⁴ Likewise, wireless carriers have

¹⁰ Press Release, Illinois Attorney General Lisa Madigan, Madigan Sues Company That Buys Cell Phone Records (Jan. 20, 2006), *available at* http://illinoisattorneygeneral.gov/pressroom/2006_01/20060120.html (suits alleges violations of Illinois' Consumer Fraud and Deceptive Business Practices Act, and seeks up to \$50,000 per violation).

¹¹ Press Release, Missouri Attorney General's Office, Nixon sues Internet business that sells records of cell phone calls (Jan. 20, 2006), *available at* <http://www.ago.mo.gov/newsreleases/2006/012006b.htm> (suit alleges violation of Missouri consumer protection laws, and seeks monetary penalties and an injunction); Press Release, Missouri Attorney General's Office, Nixon keeps up pressure on Internet businesses that illegally obtain and sell cell phone information (Feb. 21, 2006), *available at* <http://www.ago.mo.gov/newsreleases/2006/022106b.htm>; Press Release, Missouri Attorney General's Office, Another Internet business that illegally obtains and sells cell phone records is targeted by Nixon (Mar. 6, 2006), *available at* <http://www.ago.mo.gov/newsreleases/2006/030606.htm>.

¹² Press Release, Attorney General of Texas Greg Abbott, Attorney General Abbott Files First Suit Against Sellers Of Private Phone Records (Feb. 9, 2006), *available at* <http://www.oag.state.tx.us/oagnews/release.php?id=1449> (suit alleges violations of the Texas Deceptive Trade Practices Act, which provides for penalties of up to \$20,000 per violation).

¹³ Press Release, Office of the Attorney General of Florida, Crist Sues Data Brokers Over Sale of Telephone Records (Jan. 24, 2006), *available at* <http://myfloridalegal.com/newsrel.nsf/newsreleases/D510D79C5EDFB4B98525710000539060>; Press Release, Office of the Attorney General of Florida, Crist: Websites Hawking Phone Records Shut Down (Feb. 9, 2006), *available at* <http://myfloridalegal.com/newsrel.nsf/newsreleases/40265981391EDECE8525711000659BA9>.

¹⁴ Press Release, Missouri Attorney General's Office, Missouri first state to force Web business to stop selling cell phone records; Nixon obtains restraining order (Jan. 30, 2006), *available at* <http://www.ago.mo.gov/newsreleases/2006/013006b.htm>; Press Release, Missouri Attorney General's Office, Locatecell.com must stop selling cell phone records of Missourians, under court order obtained by Nixon (Feb. 15, 2006), *available at* <http://www.ago.mo.gov/newsreleases/2006/021506.htm>; Press Release, Missouri Attorney General's Office, Court orders Web business to stop obtaining, selling cell phone records of Missourians (Feb. 23, 2006), *available at* <http://www.ago.mo.gov/newsreleases/2006/022306c.htm>.

filed several lawsuits against data brokers. Cingular recently obtained a restraining order against two data brokers,¹⁵ and Sprint Nextel, T-Mobile, and Verizon Wireless reportedly have filed similar lawsuits against data brokers.¹⁶

Even as prosecution of parties engaged in pretexting continues under current federal and state law, at least *seven* bills addressing pretexting have been introduced in Congress since January.¹⁷ While the specific provisions vary, generally the bills would make it a federal crime to obtain by fraud or other unauthorized means confidential phone records, to knowingly sell such records without customer authorization, and to solicit another person to do so. The bills would impose penalties of fines and significant terms of imprisonment ranging from 5 to 25 years. Of the seven bills identified, only one would amend the Communications Act.¹⁸ Under

¹⁵ Press Release, Cingular Wireless, Cingular Wireless Fights Back Against Cell Phone Record Websites, Obtains Temporary Restraining Order Against Companies Involved in Theft and Sale of Cell Phone Records (Jan. 13, 2006), *available at* http://cingular.mediaroom.com/index.php?s=press_releases&item=1427.

¹⁶ Press Release, Sprint Nextel, Sprint Nextel Sues to Shut Down Online Services That Illegally Obtain and Sell Confidential Telephone Records (Jan. 27, 2006), *available at* http://www2.sprint.com/mr/news_dtl.do?id=9920; Press Release, Sprint Nextel, Sprint Nextel Files New Lawsuit to Halt Fraudulent Pursuit of Confidential Customer Information (Jan. 30, 2006), *available at* http://www2.sprint.com/mr/news_dtl.do?id=9960. Press Release, T-Mobile USA, Inc., T-Mobile Sues Cell Phone Record Brokers for Criminal Profiteering (Jan. 23, 2006), *available at* <http://www.t-mobile.com/Company/PressReleases.aspx>; Press Release, Verizon Wireless, Verizon Wireless Wins Another Injunction Against Data Thieves (Jan. 31, 2006), *available at* <http://news.vzw.com/news/2006/01/pr2006-01-31f.html>

¹⁷ Phone Records Protection Act of 2006, S. 2177, 109th Cong. (2006); Consumer Telephone Records Protection Act of 2006, S. 2178, 109th Cong. (2006); Secure Telephone Operations Act of 2006, H.R. 4657, 109th Cong. (2006); Consumer Telephone Records Protection Act of 2006, H.R. 4662, 109th Cong. (2006); Stop Attempted Fraud Against Everyone's Cell and Land Line (SAFE CALL) Act, H.R. 4678, 109th Cong. (2006); Law Enforcement and Phone Privacy Protection Act of 2006, H.R. 4709, 109th Cong. (2006); Phone Records Protection Act of 2006, H.R. 4714, 109th Cong. (2006). Additionally, the House Commerce Committee reportedly issued subpoenas last week to data brokers operating 26 websites selling CPNI. COMM. DAILY at 14 (Apr. 7, 2006).

¹⁸ See Consumer Telephone Records Protection Act of 2006, H.R. 4662, 109th Cong. (2006).

that bill, the only amendment would require a carrier that becomes aware of a CPNI violation to notify the customer.¹⁹

The appropriate response to pretexting and similar misappropriation of CPNI by third parties is prosecution under applicable federal and state law.²⁰ These efforts already have garnered significant results. Additional Commission regulation of carriers—who already have the duty to safeguard CPNI—is unnecessary.

III. The Current CPNI Rules Adequately Protect Consumers, and the Costs of Additional FCC Regulation Cannot Be Justified

By federal statute and FCC regulation, carriers already are subject to detailed rules requiring the protection of CPNI. Additional regulation would impose significant costs on both carriers and consumers without adding any significant protection for consumers. Therefore, the benefit of additional regulation does not justify the costs.

Congress struck a measured balance between permitting access to CPNI when appropriate for the provision of telecommunications services, and protecting customers from the unauthorized use or disclosure of CPNI.²¹ Carriers have the clear, express duty to protect the confidentiality of CPNI.²² At the same time, carriers must comply with the express desire of a customer who has authorized the disclosure of his or her CPNI.²³ Access to CPNI enables consumers to receive assistance with the telecommunications services to which they currently

¹⁹ *Id.* § 4.

²⁰ EPIC suggests that some employees of telecommunications carriers may be complicit in the fraud perpetrated by data brokers. *See NPRM* at ¶ 10. Carriers already are required to train their personnel as to when they are and are not authorized to use CPNI, and must have an express disciplinary process in place. *See* 47 C.F.R. § 64.2009(b). Moreover, any criminal activity is subject to the full range of legal sanctions described above.

²¹ *See NPRM* at ¶ 4.

²² 47 U.S.C. § 222(a).

²³ 47 U.S.C. § 222(c)(2).

subscribe, and to get new services or even a new service provider if they so desire. The Commission's rules therefore contain a number of specific safeguards that reflect this measured balance between protection and appropriate use of CPNI.

For example, carriers already are required to design customer service records so that the status of a customer's CPNI approval can be clearly established.²⁴ Likewise, carriers already are required to maintain a record of all instances where CPNI was used for marketing purposes or disclosed to third parties, and to keep such records for at least one year.²⁵ Moreover, carriers already are required to train their personnel as to when they are and are not authorized to use, disclose or access CPNI, and to have an express disciplinary process to address employee violations of CPNI policy.²⁶ Further still, carriers already are required to certify annually their compliance with CPNI requirements.²⁷ These requirements have been implemented by the industry at a material cost, and the penalties for non-compliance can be substantial. The Commission issued notices of apparent liability for forfeiture by both AT&T and Alltel in the amount of \$100,000 each for failure to comply with the annual certification requirements.²⁸

Additional regulation proposed by the Commission would not provide any significant benefit beyond that achieved under current rules. Notices to customers every time any party seeks access to their CPNI would likely be ignored. Moreover, such a requirement is inappropriate for carriers such as Salina-Spavinaw Telephone Company, whose practice is not to provide CPNI to third parties, even for marketing purposes, and who already notify customers in

²⁴ 47 C.F.R. § 64.2009(a).

²⁵ 47 C.F.R. § 64.2009(c).

²⁶ 47 C.F.R. § 64.2009(b).

²⁷ 47 C.F.R. § 64.2009(e).

²⁸ AT&T, Inc., Apparent Liability for Forfeiture, DA 06-221 (rel. Jan. 30, 2006); Alltel Corporation, Apparent Liability for Forfeiture, DA 06-220 (rel. Jan. 30, 2006).

rare cases of suspected attempts at unauthorized disclosure. Requiring an audit trail or encryption and use of a password for each use of CPNI by a carrier (for example, each time a customer calls with a billing question or service inquiry) would create an excessive record-keeping burden with no apparent benefit, since there is little likelihood that pretexting or similar theft of CPNI would occur in any but the rarest of cases of CPNI use.²⁹ In any event, some carriers, such as Salina-Spavinaw, already require the social security numbers of customer service callers and accommodate customer requests for an additional password. Establishing new records deletion requirements is unlikely to achieve any material benefit, since customer records must be retained for a reasonable period in order to facilitate the provision of telecommunications services, and most companies have records retention policies that dictate destruction of records following expiration of mandatory retention periods. For example, Salina-Spavinaw shreds customer records and destroys electronic media and media storage devices on which customer records have been stored, following the retention period.

Especially given the minimal benefits, additional regulation would be too costly—to both carriers and consumers. The audit trail and encryption proposals would be especially burdensome. Costs would include the purchase, installation, maintenance, and upgrade of encryption software, the human resources costs of the additional personnel required to implement these requirements and the retraining of existing personnel, and storage capacity for the record-keeping that would be required. Burdensome costs have played a significant role in past Commission decisions with respect to CPNI. For example, the Commission modified the

²⁹ From news reports, it appears that “pretexting” has occurred in the very limited circumstance where a person purporting to be a customer called the carrier and requested his or her CPNI. In the vast majority of instances when a carrier accesses, uses or discloses CPNI it does so as part of providing a telecommunications service to a customer, so this type of unauthorized disclosure would not occur.

flagging and audit trail requirements originally adopted in the *CPNI Order* due to concerns over excessive costs.³⁰ These significant costs would be especially burdensome on small carriers such as the Oklahoma Carriers. Many of the Commission's proposals, such as the encryption proposal, involve significant fixed costs that must be incurred regardless of the number of customers a carrier serves.³¹ These costs would have to be passed on to consumers, which would likely impact customers in rural markets most severely. The Oklahoma Carriers believe that the penalty for fraudulent access to CPNI should be borne by those engaged in fraudulently obtaining such information, not consumers.

In addition to the direct costs imposed by any new regulations, the proposed rules would impose indirect costs on consumers as well. For example, consumers may not want to have to keep track of yet another password,³² and passwords may hamper the transaction of legitimate business.³³ Frequent notices are an acknowledged nuisance to customers.³⁴ Such burdens would undermine the balance struck in the current CPNI rules between protecting

³⁰ *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, Order on Reconsideration and Petitions for Forbearance*, 14 FCC Rcd 14409 at ¶¶ 124-127 (1999).

³¹ The Commission noted this concern when it modified the flagging and audit trail requirements adopted in the *CPNI Order*. See *id.* ¶ 125 (“TDS argues that many of the costs of compliance with the flagging and audit trail requirements will place a heavier burden on small and rural carriers because they cannot be spread across a large customer base.”).

³² See *NPRM* at ¶ 15.

³³ See *id.*

³⁴ See *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; 2000 Biennial Regulatory Review—Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860 at ¶ 111 (2002).

privacy, on the one hand, and facilitating the offering of telecommunications services, on the other. The proposed regulations would impose even greater burdens on customers—burdens not justified by the benefits.

IV. Conclusion

The practice of pretexting to obtain CPNI has drawn intense scrutiny and quick action by both federal and state law enforcement officials. These actions appropriately penalize the data brokers who profit from such fraud. Increased regulation of telecommunications carriers is misplaced because it will impose significant burdens on consumers with no significant benefits. Therefore, the Oklahoma Carriers believe that none of the Commission's proposals should be adopted.

Respectfully submitted,

CROSS TELEPHONE COMPANY, CIMARRON
TELEPHONE COMPANY, POTTAWATOMIE TELEPHONE
COMPANY, CHICKASAW TELEPHONE COMPANY, AND
SALINA-SPAVINAW TELEPHONE COMPANY

/s/ Karen Brinkmann

Karen Brinkmann
Patrick Wheeler*
LATHAM & WATKINS LLP
Suite 1000
555 Eleventh Street, N.W.
Washington, DC 20004-1304
(202) 637-2200

*Counsel to Cross Telephone Company, Cimarron
Telephone Company, Pottawatomie Telephone
Company, Chickasaw Telephone Company, and
Salina-Spavinaw Telephone Company*

April 28, 2006

*Application Pending in New York; Not Yet Admitted in the District of Columbia