
Before the
Federal Communications Commission
Washington, DC 20554

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

To: The Commission

COMMENTS OF CINGULAR WIRELESS LLC

J. R. Carbonell
Carol L. Tacker
Michael P. Goggin
5565 Glenridge Connector
Suite 1700
Atlanta, GA 30342

Its Attorneys

April 28, 2006

TABLE OF CONTENTS

SUMMARY	ii
INTRODUCTION	1
DISCUSSION.....	4
I. PRIVACY AND SECURITY OF CUSTOMER INFORMATION.....	4
A. Cingular’s Approach to CPNI Privacy and Security	4
B. The Customer’s Role in Preserving CPNI Privacy and Security.....	6
C. Carriers and Regulators Need to Consider Consumers’ Attitudes When Crafting Privacy and Security Policies for CPNI	7
II. WHAT IS THE EXTENT AND NATURE OF THE PROBLEM?	9
III. HOW DATA BROKERS OBTAIN ACCESS TO CPNI (¶ 11)	12
IV. ISSUES RELATING TO OPT-OUT REGIME AND REPORTING AND NOTICE REQUIREMENTS	13
A. Opt-Out Regime (¶ 12)	13
B. Reporting and Notification (¶¶ 27-30).....	14
V. CURRENT CARRIER PRACTICES (¶ 13)	17
VI. PROPOSED SECURITY MEASURES	19
A. Consumer-Set Passwords (¶¶ 15-16)	19
B. Audit Trails (¶¶ 17-18)	21
C. Encryption (¶ 19)	23
D. Reduced Data Retention (¶ 20).....	24
E. Notice of CPNI Disclosure or Security Breaches (¶¶ 21-24).	25
F. Other Approaches (¶ 25).....	29
G. Enforcement (¶ 26)	31
VII. SMALL CARRIERS VS. LARGE CARRIERS	33
CONCLUSION.....	34

SUMMARY

The Commission adopted the *NPRM* in response to a petition for rulemaking filed by EPIC, which brought to the Commission's attention the fact that data brokers have been advertising and selling personal telephone records, including call detail records of wireless phone customers. Cingular agrees that such activity should be stopped, and has successfully sued data brokers who invade its customers' privacy by doing so. Nevertheless, Cingular cannot support the adoption of the rules proposed. The proposed rules will not significantly improve the privacy of customer records, because they are misdirected toward carriers instead of data brokers, who are misappropriating CPNI through pretexting and other schemes.

Carriers generally give customers the ability to implement passwords and other measures to protect their CPNI, but surveys show that many customers prefer not to use them. Some of the proposed rules, however, would contravene consumers' preferences by mandating passwords, contrary to the public interest. Instead, Cingular urges the Commission to support Congressional action to impose criminal sanctions on data brokers who obtain CPNI through fraud and deceit.

No new prescriptive rules regarding carriers' protection of CPNI are needed. Section 222 and the rules require carriers to safeguard CPNI, and carriers such as Cingular take these obligations seriously. Carriers are already trying to curb data brokers' abuses through legal action, and the theft of CPNI appears to be on the wane.

Some of the rules proposed have nothing to do with the issues posed by data brokers. There is no need for any change to the existing rules regarding consumers' opting in or out of the use of their CPNI for purposes outside their carrier's total service approach. There is also no need for changes to the existing rules on consumer notifications concerning CPNI, or for the adoption of new reporting requirements. Cingular has no objection, however, to a rule requiring all carriers to file their annual CPNI certifications, provided that a reasonable period is provided for the filing, such as through April 15 of the following year.

The data broker incidents do not warrant the adoption of new rules concerning passwords, audit trails, encryption of data, reduced retention times for data, or notices to consumers about actual or potential security breaches. The proposed rules would do nothing to address the problem and would impede the delivery of service at an affordable cost. Voluntary efforts by carriers, guided by realistic policies, will work far better than prescriptive rules.

If the Commission nevertheless decides that new rules are needed, it should adopt only narrow rules targeted to address identified problems, rather than broad rules with unforeseen consequences. Properly limited, access to CPNI is essential; carriers use CPNI routinely in providing and billing for service, as well as in assisting customers. At most, the Commission should adopt rules that would subject CPNI to protections similar to those governing customer financial records under the Gramm-Leach-Bliley Act ("GLBA"). Moreover, optional "safe harbor" rules would give carriers needed flexibility, unlike detailed prescriptive rules.

Any rule deemed important enough to adopt for the sake of customers' privacy should be applicable to all telecommunications providers, not only large or urban carriers. The same rules should protect the privacy of customers of rural telephone companies or VoIP-based providers as apply to the customers of long-distance carriers, urban/suburban local exchange carriers, and wireless operators.

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

COMMENTS OF CINGULAR WIRELESS LLC

Cingular Wireless LLC (“Cingular”) hereby submits its Comments in response to the Commission’s *Notice of Proposed Rulemaking* concerning the need for new regulations to safeguard customer proprietary network information (“CPNI”).¹

INTRODUCTION

The Commission adopted the *NPRM* in response to a petition for rulemaking filed by the Electronic Privacy Information Center (“EPIC”), which brought to the Commission’s attention the fact that data brokers have been advertising and selling personal telephone records, including

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*, CC Docket 96-115, *Notice of Proposed Rulemaking*, FCC 06-10 (Feb. 14, 2006) (*NPRM*), summarized, 71 Fed. Reg. 13317 (Mar. 15, 2006).

call detail records of wireless phone customers.² Cingular agrees that such activity should be stopped. Indeed, Cingular has sued data brokers who have invaded its customers' privacy by wrongfully obtaining and selling their wireless phone records and has obtained injunctive relief against these activities.³

Nevertheless, Cingular cannot support the adoption of the rules proposed in the EPIC petition and the *NPRM*. The proposed rules will not significantly improve the privacy of customer records, because they are misdirected toward the carriers instead of the data brokers. Carriers are not intentionally supplying CPNI to data brokers. Instead, data brokers are misappropriating CPNI through pretexting and other schemes; corrective measures need to be directed at the data brokers.

Carriers generally give customers the ability to implement passwords and other measures to protect their CPNI, but surveys show that many customers feel inundated with passwords and

² Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115, RM-11277 (filed Aug. 30, 2005) ("EPIC Petition").

³ *Cingular Wireless LLC v. Data Find Solutions, Inc.; James Kester; 1st Source Information Specialists Inc.; Kenneth W. Gorman; Steven Schwartz; John Does 1-100; and XYZ Corps. 1-100*, Case No. 1:05-CV-3269-CC (N.D. Ga. filed Dec. 23, 2005). Defendants were temporarily enjoined by the court January 13, 2006 and have tentatively agreed to a consent permanent injunction. *Cingular Wireless LLC v. Efindoutthetruth.com, Inc.; Lisa Loftus; Tiffany Wey; North American Services, LLC d/b/a North American Information; Tom Doyle; John Does 1-100; and XYZ Corps. 1-100*, Case No. 1:05-CV-3268-ODE (N.D. Ga. Dec.23, 2005). Efindoutthetruth.com, Inc., Tiffany Wey and Lisa Loftus have agreed to a consent permanent injunction. North American Services, LLC and Tom Doyle have tentatively agreed to a consent permanent injunction. *Cingular Wireless LLC v. Global Information Group, Inc.; GIG Liquidation, Inc. f/k/a Global Information Group; Bureau of Heirs, Inc.; Edward Herzog; Laurie Misner; Robin Goodwin; John Does 1-100; and XYZ Corps. 1-100*, Case No. 1:06-CV-0413-TWT (N.D. Ga. filed Feb. 23, 2006). Defendants tentatively agreed to a consent permanent injunction. *Cingular Wireless LLC v. Get A Grip Consulting, Inc.; Paraben Corporation d/b/a Get A Grip Software Publishing; Robert Schroeder; John Does 1-100; and XYZ Corps. 1-100*, Case No. 1:06-CV-0498 (N.D. Ga. filed Mar. 2, 2006). Defendants tentatively agreed to a consent permanent injunction.

prefer not to use yet another one. Despite many consumers' preference for convenience over heightened security, some of the rules proposed will work against the interests of consumers by making passwords mandatory. This is inconsistent with the public interest. Instead, Cingular urges the Commission to support Congressional action to impose criminal sanctions on the wrongdoers — the data brokers who use fraud and deceit to obtain CPNI to which they are not entitled.

No new prescriptive rules regarding carriers' protection of CPNI are needed. Both Section 222 and the Commission's existing rules require carriers to safeguard CPNI, and carriers such as Cingular take these obligations seriously. EPIC raised legitimate concerns about data brokers' acquisition and sale of CPNI, which carriers had already been seeking to curb through legal action, and the practice appears to be diminishing after exposure in news articles, Congressional hearings, and FCC proceedings, as well as prosecutions by both State Attorneys General and the Federal Trade Commission. Above and beyond the data brokers who have been enjoined by carrier lawsuits, a number of the websites cited in the EPIC petition have since bowed to such pressures and "voluntarily" ceased offering call records, some even expressly stating so on their websites⁴.

If the Commission nevertheless decides that new rules are needed, it should ensure that any rules adopted are narrowly targeted to address the concrete problems that have been identified, and not adopt broad rules that may have many unforeseen consequences. Carriers (and their employees and agents) need routine access to CPNI to provide and bill for service and

⁴ See, e.g., <<http://cellulartrace.com/>> ("We are not currently obtaining any cellular call records. We have made this very clear on our Searches page even going as far as explaining the fact in flashing text. Despite this, some customers continue to place orders for other searches and expect call records as the result. The searches that are available are on our "Searches" page.").

to assist customers. At most, the Commission should adopt rules that would subject CPNI to protections similar to those governing customer financial records under the Gramm-Leach-Bliley Act (“GLBA”).⁵

DISCUSSION

I. PRIVACY AND SECURITY OF CUSTOMER INFORMATION

A. Cingular’s Approach to CPNI Privacy and Security

Cingular takes very seriously the privacy and security of customer information. Protection against unauthorized use of or access to customer data is the responsibility of all Cingular employees. 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. To ensure consumer confidence, Cingular must react to unscrupulous business practices by persons and entities intent on breaching safeguards.

In general terms, Cingular has taken an interdisciplinary approach to countering breaches. This approach encompasses the following broad categories: (1) oversight; (2) education and training; (3) policies and procedures; and (4) enforcement and response.

(1) Oversight. There are critical stakeholders within Cingular that have direct access to customer data, as well as the processing and management of that data. Cingular has established a number of teams that focus on specific aspects of privacy and security that oversee how this data is safeguarded.

⁵ An Act to Enhance Competition in the Financial Services Industry by Providing a Prudential Framework for the Affiliation of Banks, Securities Firms, Insurance Companies, and Other Financial Service Providers, and for Other Purposes, P.L. 106-102, Title V, 113 Stat. 1338, 1436-50 (1999), *codified*, 15 U.S.C. §§ 6801-27.

(2) Education and Training. All employees are required to annually review and certify to their familiarity with the Cingular Code of Business Conduct. This Code contains, *inter alia*, a section that outlines the CPNI obligations of all Cingular employees and that warns of disciplinary action (up to and including termination) in the event of a breach of these obligations. Employees also must take formal privacy training. Following its recent merger with AT&T Wireless, Cingular's senior management sent a communiqué to sales and marketing employees summarizing Cingular's supervisory review and marketing campaign approval process for the use of CPNI, as well as Cingular's policies related to telemarketing. Cingular also provides information to relevant employees about privacy issues in employee news bulletins and holds informal training meetings with specific groups of employees as needed to explain changes in procedures or processes designed to protect customer data.

(3) Policies and Procedures. Cingular takes a dynamic view of policies and procedures designed to protect customer data. As the methods and focus of attempted breaches of internal security evolve, the policies designed to protect that data must be constantly tested and improved to defeat those deceitful initiatives. The policies also must take into account evolving regulation and law, as well as trends identified from customer usage demands. Improvements in technology must be evaluated and implemented where feasible. Rules internal to particular departments must be evaluated and assessed and employees must be educated and trained on new procedures. Automated systems are scrutinized for potential breaches and employees who maintain and operate these systems must be trained.

(4) Enforcement and Response. Cingular maintains an internal hot line where employees can report Code of Business Conduct violations, including improper access to or use of customer accounts. Each such report results in an investigation into the claim and, if

warranted, appropriate disciplinary action for any wrongdoing. Additionally, Cingular proactively searches for internal system breaches through both its Internal Audit process and management oversight. When an issue is identified, corrective processes are implemented. Cingular aggressively pursues external entities or persons intent on breaching the privacy of customer data. Cingular employs all lawful means to stop these breaches, including formal legal action. The company also enforces its internal procedures and, where appropriate, disciplines employees found to have violated these policies.

B. The Customer's Role in Preserving CPNI Privacy and Security

Customers share responsibility with Cingular for protection of their CPNI. All the passwords, authentication systems, audit trails, and regulations in the world will not secure the privacy of data that customers do not treat securely. Cingular provides the following guidance to customers in its privacy policy posted on its website:

What Can I Do to Protect My Personal Information?

An important part of ensuring the security of personal information is your own effort to protect against unauthorized access to your wireless device and the personal information contained in it and on your SIM card. Most phones and wireless PDA-type devices store calling information both in the phone and on the SIM card. Therefore, before discarding your phone or PDA, trading it in or giving it away, be sure you remove and retain your SIM card and follow the manufacturer's instructions for deleting all personal information on the device itself. (This can be found in your owner's manual or on the manufacturers' Web site.)

In addition, use passwords to prevent unauthorized access to your wireless device, your wireless service account, and your voicemail. If you write down your passwords or user names, keep the information in a secure location. Do not give your password to someone else unless you intend them to have the same full access

and ability to make changes to your account as you have. Change your passwords periodically.⁶

C. Carriers and Regulators Need to Consider Consumers' Attitudes When Crafting Privacy and Security Policies for CPNI

Companies that must interact with consumers, as well as agencies that regulate such companies, must balance the benefits of high levels of data security against consumers' ability and willingness to maintain a high level of security. In essence, there is a tradeoff between consumer friendliness and security — a high degree of security and privacy may result in systems that are user-hostile. Both carriers and regulators need to take this tradeoff into account in developing policies regarding the privacy and security of CPNI.

In point of fact, the complexity of consumers' interactions with computer services leads them to disfavor high levels of security for accessing their information. Unfortunately, today's consumers are faced with the need to remember numerous passwords, and not infrequently they forget them, write them down, or share them with others.⁷ In fact, several surveys reveal that many consumers are willing to compromise their passwords in exchange for a trivial gift, such as a pen or candy bar.⁸ The way to improve the security of such information is not by adopting prescriptive regulations or laws, any more than the way to address housebreaking is to mandate that homeowners lock their doors. Many consumers tend to value convenience over security where access to personal data is concerned. Thus, for example, a recent survey by the Ponemon

⁶ <http://www.cingular.com/privacy/privacy_policy>

⁷ See, e.g., <http://www.protocom.com/whitepapers/password_survey.pdf>.

⁸ See <<http://news.bbc.co.uk/2/hi/technology/3639679.stm>>; <http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/>.

Institute, a privacy research think tank, found that most consumers — fully 87% of those surveyed — do not want mandatory passwords on their accounts.⁹

Because of consumers' attitudes, it is simply not practicable to "lock down" CPNI completely. Security can be improved, and, consistent with Section 222, carriers are constantly working on such improvements. It is unlikely, however, that any set of internal security measures or FCC regulations can provide complete security without alienating a large number of customers.

Moreover, there is no single set of security measures that is appropriate for all varieties of CPNI. For example, most carriers allow customers to access information such as the number of minutes of airtime used during the current billing period or their billing status, or even to pay their bills, by pressing a star- or pound-key combination on their phones, with no further verification needed. This customer-friendly method of accessing limited types of CPNI is in the public interest and should not be restricted by requiring additional verification beyond the fact that it is being done on the customer's own phone. A higher level of security is appropriate for access to call detail records, and Cingular and other carriers use a variety of methods that balance consumers' desire for easy access to this information against the need for security. Adoption of rules that would mandate multiple forms of verification for access to all CPNI would disserve consumers' interest in convenient access, as well as require a costly fundamental redesign of many different parts of carriers' infrastructures. Moreover, any mandated security measures would soon become obsolete by virtue of advances in information technology as well as in the

⁹ See Larry Ponemon, *Data Security: Study on Passwords Reveals Most Forget, Must Reset Passwords Multiple Times*, 5 Privacy & Security Law Report (BNA) No. 10, 335 (Mar. 6, 2006) ("Ponemon Study").

ever-evolving sophistication of “hacking” techniques. There is no such thing as perfect security, and “adequate” security is a constantly evolving standard.

II. WHAT IS THE EXTENT AND NATURE OF THE PROBLEM?

In reviewing the need for changes in its CPNI rules, the Commission needs to focus on the extent and nature of the problem that has been presented. It is important to note that while the Commission is considering the solutions proposed in the EPIC Petition, EPIC has identified phone records as only one of many types of consumer information that are susceptible to fraudulent interception and sale.

EPIC performed a valuable service in bringing this problem to the attention of the industry, the Commission, the FTC, State Attorneys General, and Congress. Before it filed its petition with the FCC, EPIC filed a complaint with the Federal Trade Commission concerning the sale by data brokers of a wide variety of personal data, including not only phone records but also the identities of mailbox subscribers and the identities associated with various online “screen names.”¹⁰ In other words, the data brokers are not unique to telecommunications; they are seek to obtain many types of private information through questionable means. The real problem is that data brokers, undeterred by existing laws, have adopted fraudulent techniques for improperly gathering private data; it is not that telecommunications carriers have lax security.

Moreover, the extent of the data broker problem is unknown. There is little information available about how many of these companies exist and how many times they have obtained private information through fraudulent means. Before EPIC filed its complaint with the FTC,

¹⁰ See <<http://www.epic.org/privacy/iei/ftccomplaint.html>>; see generally <<http://www.epic.org/privacy/iei/>>.

there appear to be few, if any, news reports regarding data brokers obtaining phone records.¹¹ It is noteworthy that the only news articles about the data broker problem cited in the EPIC Petition to the FCC were two articles published in response to EPIC's FTC complaint.¹²

How many such data brokers are there? EPIC identified forty web sites offering private information, including phone records and other data.¹³ It is unclear how many of these web sites are independent of the others and actually gather the data themselves. EPIC noted that several of the sites appear to be operated by the same entities; in addition, some of the sites purport to be run by private investigators, who may employ outside data brokers. There may be only a handful of companies actually obtaining phone records themselves. The *NPRM* does not provide any information about these companies beyond the information supplied by EPIC.¹⁴

The fact that some unscrupulous website operators have used fraudulent techniques to obtain private information from telecommunications carriers does not necessarily mean that there are any significant flaws in carrier safeguards that cannot be addressed by the carriers once the issue has been highlighted; there is not necessarily a need for regulatory attention. The fact that some unscrupulous companies advertise that, in effect, they can steal something to which they do

¹¹ The earliest article revealed in a NEXIS search of several leading newspapers for "data broker" and "phone record" was a Washington Post article published after EPIC filed its petition with the FTC. A Google search for the same terms revealed the same article and did not appear to indicate any earlier matches on the Web or in Google's News database. See Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, Washington Post, July 8, 2005, at D1, available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862_pf.html>

¹² EPIC cited the Washington Post article cited in the preceding footnote and another article published on the same date, July 8, 2005, Susan Kuchinskas, *EPIC Fighting Online Phone Record Sales*, InternetNews, July 8, 2005, available at <<http://www.internetnews.com/ent-news/article.php/3518851>>. See EPIC Petition at nn.12-13.

¹³ See Attachment A to EPIC's FTC complaint, available at <http://www.epic.org/privacy/iei/attachment_a.pdf>. This list is also included as Attachment C to the EPIC Petition and was referenced by the Commission; see *NPRM* at ¶ 10 n.26.

¹⁴ See *NPRM* at ¶ 10.

not have legitimate access does not mean that there is a widespread problem or that, as EPIC claimed, “these violations are occurring at an alarming rate.”¹⁵ In fact, there appears to be little or no evidence of how widespread the instances are in which CPNI has been fraudulently obtained and the extent to which this is a growing problem.¹⁶

This is not to downplay the impact on customers when data brokers are successful in pretexting to obtain customer information. Customers can suffer significant consequences, but the solution to this problem must be focused on the data brokers, not the telecommunications carriers who need access to the data to operate their businesses.

Telecommunications carriers have reacted to the theft of CPNI by data brokers by filing lawsuits to stop them from doing so. The *NPRM* noted that both Verizon Wireless and Cingular have lawsuits seeking injunctions.¹⁷ In fact, both Verizon and Cingular have obtained injunctions,¹⁸ and other wireless carriers, including Sprint Nextel and T-Mobile, also have filed suits and/or obtained judicial relief; some State Attorneys General also have engaged in litigation.¹⁹

¹⁵ See EPIC Petition.

¹⁶ The EPIC Petition did not supply any such numbers, nor did the *NPRM*. Moreover, neither the Commission nor the FTC apparently know how widespread a problem there is. At a recent hearing, Chairman Martin responded to a question about whether the FCC had “information about the number or the volume of instances in the aggregate, or the volume of calls that have been sold without the real phone holder’s permission” by stating, “No we don’t at the FCC.” Hearing before the House Committee on Energy and Commerce, *Phone Records For Sale: Why Aren’t Phone Records Safe From Pretexting?*, Serial No. 109-53, at 48 (Feb. 1, 2006). The FTC, likewise, had no data about the prevalence of such practices. See *id.*

¹⁷ See *NPRM* at ¶ 10 & n.30.

¹⁸ See footnote 3 above.

¹⁹ See *Sprint Nextel Files 3rd Phone-Record Suit*, CIO News Alerts, March 20, 2006, available at <http://www.cio.com/blog_view.html?CID=19298>; *T-Mobile Sues Cell Phone Record Brokers for Criminal Profiteering*, Business Wire, Jan. 23, 2006, available at <<http://biz.yahoo.com/bw/060123/20060123006047.html?.v=1>>; Press Release, Attorney General Abbott Files First Suit Against Sellers Of Private Phone Records, Feb. 9, 2006, available at

(continued on next page)

Given that the industry and state regulators have taken legal action to stop the theft of consumers' phone records, and that the lawsuits have resulted in injunctions, the question remains whether there is a need for additional regulations. Cingular submits that the answer is no. Wireless carriers have acted responsibly in safeguarding their customers' CPNI, but no safeguard is perfect. When unscrupulous operators have used fraudulent means to bypass these safeguards, carriers have acted responsibly by taking appropriate legal action.

History has demonstrated that increased security measures do not, ultimately, keep hackers and other bad actors out. If software companies have been unable to make their applications hacker-proof despite spending billions on development, it would be foolhardy to believe that the adoption of new CPNI rules will prevent all access by data brokers. They will find a way to obtain CPNI as long as there is a market for the information and there are no swift and certain penalties for obtaining it. The best way to deter such activity is to make it expressly illegal. Just as locks can be picked and safes blown, security measures can be overcome, but criminal sanctions certainly deter such activities.

III. HOW DATA BROKERS OBTAIN ACCESS TO CPNI (¶ 11)

In the *NPRM*, the Commission inquires about the techniques used by data brokers to obtain access to CPNI.²⁰ In Cingular's experience, a number of different techniques have been used. In virtually all cases, the particular CPNI being sought was call detail records — what numbers have been called, where the called number is located, and the dates, times, and duration of calls.

(footnote continued)

<<http://www.oag.state.tx.us/oagNews/release.php?id=1449>>; *Phone record brokers targeted*, Chicago Sun-Times, Jan. 6, 2006, available at <<http://www.suntimes.com/output/news/cst-nws-cell06.html>>; *Florida Sues Data Broker Over Sale of Phone Records*, <http://www.consumeraffairs.com/news04/2006/02/fl_global.html>.

²⁰ *NPRM* at ¶ 11.

The primary focus of data brokers has been tricking service representatives, who are trying to be helpful to customers, into providing customer information. Cingular has not, to date, found evidence that information systems have been “hacked” for the purpose of obtaining and selling customer’s call detail records.

The primary method by which the call detail records have been obtained appear to be “pretexting.” This occurs when a third party such as a data broker or investigator falsely represents to the carrier that he or she is the customer, a carrier employee or agent, or a TTY operator or other intermediary, typically claiming to be assisting a customer. Other ways in which CPNI has been improperly obtained are much less frequently used, and typically not by data brokers.²¹

IV. ISSUES RELATING TO OPT-OUT REGIME AND REPORTING AND NOTICE REQUIREMENTS

In the *NPRM*, the Commission seeks comment on the adequacy of its current opt-out regime and on whether there need to be new notice and reporting requirements concerning CPNI. For the most part, these are not directly related to the data broker issue, and will be dealt with separately from that issue in these comments.

A. Opt-Out Regime (§ 12)

The *NPRM* asks about whether the existing opt-out rules regarding marketing adequately protect CPNI from improper use in marketing or disclosure to joint venture partners and

²¹ For example, unauthorized CPNI access also occurs when a relative or someone close to a customer, such as a spouse or ex-spouse, uses personal information that the person knows about the customer. A relative may be able to venture answers to the “secret questions” used to verify identity, such as the place of birth, a pet’s name, or other personal details. By using such information, the relative may be able to access the customer’s account and thereby obtain CPNI such as call detail records.

independent contractors.²² Cingular currently does not use or share the CPNI of its customers for marketing services other than in accordance with the “Total Services Approach,” and, in appropriate cases, Section 64.2005(a)(1). As a result, Cingular does not see any need for changes to this regime. Cingular’s investigation into theft of data records has not identified any breach due to the current opt-out rule requirements and the safeguards related to the carrier’s use or disclosure of customer information for marketing purposes. Thus, the existing safeguard of requiring a confidentiality agreement with a joint venture partner or independent contractor is adequate. The carrier can take appropriate steps to correct or even terminate the relationship if a breach occurs or the policy is not being followed.

B. Reporting and Notification (¶¶ 27-30)

In the *NPRM*, the Commission seeks comment on possible changes to its notification requirements, including how notifications to consumers should be worded; it also asks whether there should be any additional reporting requirements, whether the current rule regarding the annual CPNI certification should be changed, and about the benefits and burdens associated with such requirements.²³

Changes to notification rules. Cingular does not believe there is any need for changes to the consumer notification rules. Many carriers only use CPNI to market services within the total service category where customer approval is not required. Thus, notification and opt-in and opt-out procedures are not required. The Commission adopted its current rules only after exhaustive consideration of the alternatives and undergoing judicial review (and vacatur) of its rules

²² *NPRM* at ¶ 12.

²³ *NPRM* at ¶¶ 27-30.

regarding consumer options, and further proceedings after remand.²⁴ There is no reason for changing the rules to require notifications or opt-in/out determinations that are currently unnecessary.

Changes to how notifications are worded. Cingular believes that no rule changes are needed with respect to ensuring that customers fully understand what personal records telecommunications carriers seek permission to use and/or disclose. As with the truth-in-billing rules, the best standard is to require only that customer communications are stated in a clear and non-misleading manner. The Commission should not attempt to prescribe particular grammatical usages and vocabulary. Given the complexity of the existing CPNI rules, there is no way to meet the existing notification requirements and make the notifications truly simple to understand.²⁵ Again, the GLBA experience provides evidence that when you have a complex issue it is almost impossible to make it easy for customers to understand, and frequent mailings of notifications virtually guarantee that such notifications will not be read and understood.

New reporting requirements. Cingular opposes the adoption of new reporting requirements as unnecessary. No reporting requirement is needed for cases of unauthorized access to or disclosure of CPNI. In the data brokerage cases, Cingular discovered the activities

²⁴ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Dockets 96-115 and 96-149, *Second Report and Order and Further Notice of Proposed Rulemaking*, 13 F.C.C.R. 8061, ¶¶ 86-142 (1998), *vacated sub nom. U S WEST, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999); *id.*, *Order on Reconsideration and Petitions for Forbearance*, 14 F.C.C.R. 14409 (1999); *id.*, *Clarification Order and Second Further Notice of Proposed Rulemaking*, 16 F.C.C.R. 16506 (2001); *id.*, *Third Report and Order*, 17 F.C.C.R. 14860 (2002).

²⁵ That, of course, would require that the FCC provide its own clear and simple definitions of every possible variety of CPNI, a task that would prove as challenging as comprehensively determining in advance, in simple language, the boundaries of every variety of information service and telecommunications service.

of data brokers and took legal action against them. Cingular changed its policies regarding the provision of call detail over the phone and provided extensive training to its employees on identifying social engineering attempts by data brokers. Reporting a data broker's breach to all customers who could *potentially* have been affected would not have provided useful information to customers, the vast majority of whom would have been unaffected. Instead, Cingular posted information on its website that gave details about the data broker issue and explained how customers could further protect their accounts.²⁶

In addition, Cingular opposes any new requirement that carriers file reports with the FCC on either a per-incident or periodic basis concerning CPNI security incidents. Moreover, there are good reasons for *not* requiring carriers to file detailed reports on security incidents or potential incidents. If such reports provided significant details concerning the incidents or carrier

²⁶ Cingular's home page, <<http://www.cingular.com>>, has a link to a page entitled, "Cell Phone Records Security," which provides the following information to customers:

As you may have read or seen in the media, a number of websites are advertising the availability for sale of wireless phone records. Please know that Cingular Wireless does not sell customer information to, or otherwise cooperate with, these companies, and we are working aggressively to combat their practices. Cingular has filed lawsuits against several of such companies, and has obtained restraining orders prohibiting them from obtaining Cingular customer information or providing it to anyone.

Cingular is supporting efforts to criminalize the unauthorized acquisition or sale of wireless phone records. We are also working with law enforcement to address the practice that we call Cell Phone Record Ripoffs.

In addition, Cingular has a variety of safeguards in place to protect against unauthorized access to customer information, and we continue to evaluate and enhance these safeguards.

If you wish to better protect your account from unauthorized access, contact us at 1-866-CINGULAR (1-866-246-4852) and ask that a passcode be placed on your account.

<http://www.cingular.com/privacy/records_privacy>.

countermeasures, they would provide a roadmap for further security breaches, and the presence of such reports in a central location such as the FCC would present a tempting target for those wishing to exploit the information.

Changes regarding annual carrier CPNI certifications. Cingular does not oppose providing the FCC with its annual certification of the processes it has implemented to comply with the rules and existing safeguards. The Commission must, however, provide carriers with sufficient time to prepare the certifications. Given the need for the certifying officer to make the certification based on personal knowledge, that officer must undertake an extensive review of the carrier's CPNI-related activities spanning an entire year, which cannot be done in a few days or weeks at the end of the year in question. Cingular believes that, at a minimum, the Commission should allow the certification for a given year to be filed 15 days after the first quarter of the following year (*i.e.*, April 15). No meaningful purpose would be served by shortening the period within which carriers are diligently performing their internal reviews; indeed, shortening the period unduly could likely lead to errors and oversights in the reports.

V. CURRENT CARRIER PRACTICES (¶ 13)

The *NPRM* asks about current carrier practices regarding CPNI disclosure and their adequacy.²⁷

At the outset, we note that Cingular has an extensive employee training program to ensure that employees understand and follow company policies concerning CPNI privacy. Cingular has trained its employees about its privacy policies and the “social engineering” techniques such as pretexting that may be used. This program is ongoing, and employees receive additional training as needed.

²⁷ *NPRM* at ¶ 13.

Cingular's practices regarding CPNI vary by platform — phone, retail stores/agents, and online. These practices can be summarized as follows:

By phone:

- The customer's identity is validated before discussing the account. Verification of customer identity involves asking for the passcode if one is present on the account. If no passcode is present, the customer is asked for several other specific items.
- Call detail information is not provided by phone, by fax, or by email.
- In short, Cingular's policies prohibit representatives from providing customers with any immediate access to call detail information by phone. Instead, the customer can have his or her call detail information mailed to the address on record, can access it online through Cingular's online account management system, or can take a photo ID to a retail store to get a bill reprint.

In retail stores/agents:

- Retail representatives and agents can provide a print of the bill for a customer who shows a photo ID to prove they are the account holder and, if the account is passcode-protected, the passcode must be supplied.
- If the customer does not have this identification, they can create an online account which allows them access to their call detail (see below).
- Otherwise, the representative can mail a copy of the bill to the billing address.

Online:

- Network and information security safeguards are in place to protect Cingular's website against "hacking."
- Online accounts (which are optional) are password-protected.
- Customers must validate their identities before establishing an online account.
- Various options are continuously being explored for strengthening Cingular's online account safeguards.

VI. PROPOSED SECURITY MEASURES

A. Consumer-Set Passwords (¶¶ 15-16)

In the *NPRM*, the Commission asks whether consumer-set passwords should be mandatory, and related questions.²⁸ Cingular supports the optional use of consumer-set passwords, but opposes mandatory passwords. A rule requiring carriers to give customers this option would be appropriate, provided such a password applies only to sensitive categories of CPNI, such as call detail records.

No Mandatory Passwords: Cingular agrees that optional consumer-set passwords can be effective in protecting customer information and encourages the use of passwords by customers to protect accounts.²⁹ However, account passwords or codes should not be mandated because many customers prefer not to use them.

The recent Ponemon Study surveyed customers about mandatory passwords for accessing services such telephone or airline accounts.³⁰ The study shows that an overwhelming majority of customers — 87% — do not want to have mandatory passwords on their accounts.³¹ Only 12% of the consumers supported a government-mandated password requirement.³² The Ponemon Study cites the following reasons for customers not wanting additional passwords: 63% said it is inconvenient to remember another password, 60% said that passwords are not necessary if the

²⁸ *NPRM* at ¶¶ 15-16.

²⁹ Cingular does inform its customers about the options available for protecting the privacy of their accounts. *See* note 26.

³⁰ *See* note 9 and accompanying text.

³¹ Ponemon Study at Bar Chart 2 and Tables 4, 6.

³² *Id.* at Table 6.

company has other ways of determining who they are, and 42% said that using a password would not increase security.³³

It goes without saying that privacy is important. At the same time, it is not *all*-important. As noted above, some consumers do not consider the privacy of their password-protected accounts sufficiently important to keep the passwords secret and will give away the passwords willingly.³⁴ Perhaps these consumers are not typical, or they may not believe that they have important information in their accounts. At the same time, most consumers are willing to trade some degree of privacy protection for convenience, and there are limits on the amount of information they are willing to supply to verify their identities. As discussed above, most consumers oppose mandatory passwords, and most object because they consider passwords to be unnecessary and inconvenient.³⁵

Cingular takes into account the appropriate balance between security/privacy and customer convenience when adopting policies for account access. Cingular believes that it is possible to meet the demands of both types of customers, those who value security over convenience and *vice versa*. For those customers who *want* more security, Cingular offers an account password. For those customers who don't want to remember yet another password, they can access their accounts without a password by supplying other validation information.

Applicability of passwords. While optional consumer-set passwords are an appropriate security tool, they should not necessarily be applicable to all forms of CPNI. For example, many wireless carriers allow consumers to obtain very limited forms of CPNI from their handsets merely by dialing a star- or pound-code. Such codes allow customers to check their balance,

³³ *Id.* at Table 5.

³⁴ *See* note 8 and accompanying text.

³⁵ *See* Ponemon Study at Tables 1, 5.

airtime minute allowances, last payment, and similar information, or to make payments, quickly and easily. While such information constitutes CPNI, it is not the kind of sensitive information that is sought through deceit by data brokers. Requiring carriers to provide password protection for these limited forms of CPNI, even optionally, would increase the complexity of this service feature and defeat its principal attraction: simplicity. Password protection regimes are more appropriately limited to sensitive information such as call detail records.

Password Changes: Customers who take advantage of the password option will occasionally need to change their passwords for a variety of reasons. Because of the risk of fraud, Cingular does not permit customers to change the password for their entire account over the phone, and a customer can only change the password used for online access over the phone after following procedures for verification of his or her identity. A photo ID is required when a consumer attempts to change a forgotten account password at a retail store.

Cingular believes customers should be sent a notice of a password change on their accounts, whether the change occurs in a retail store or online. There is no need for a government regulation to this effect, however. Cingular and many other responsible carriers already provide customers with such a notice. There is likewise no need for a prescriptive rule regarding how such notice must be given.

B. Audit Trails (¶¶ 17-18)

The *NPRM* asks about EPIC's suggestion that carriers be required to record all instances when a customer's records have been accessed, whether information was disclosed, and to whom.³⁶

³⁶ *NPRM* at ¶¶ 17-18.

Extending the recordation requirements of Section 64.2009(c), which governs disclosures of CPNI for marketing or to third parties, to all accesses or disclosures of CPNI would not be a simple matter. Cingular does not share CPNI with unaffiliated third parties for marketing, and does not use it in its own marketing in such a way that would require customer consent. As a result, Section 64.2009(c) does not impose a major burden at present. CPNI is accessed constantly, however, in the provision of, billing for, and marketing of permitted services. Every time a customer makes a call, the customer's CPNI is accessed by the switching system. Every time a customer inquires about his or her balance, CPNI is accessed and disclosed. Every time a customer seeks to verify or change features, CPNI is accessed and disclosed. Logging all such accesses and disclosures would be a tremendous burden, because virtually every aspect of a telecommunications company's business involves access to CPNI.

This huge expansion of CPNI data recordation is clearly not justified by the fact that a few unscrupulous companies have managed to obtain CPNI illicitly. Cingular's investigations of data brokers did not result in finding "insiders" selling or knowingly providing customer data to the data brokers. Thus, requiring carriers to record every access to and disclosure of CPNI would not fix the data broker problem that is the genesis of the instant rulemaking.

Cingular does record access to customer accounts electronically through many of its systems today. But EPIC is suggesting that carrier representatives make account notes *every time* CPNI is provided to the account holder. Cingular representatives receive approximately 380,000 customer service calls a day. Requiring representatives to record every time they access or provide information about customers' verification information, service plan, balance, minutes, or other CPNI information would increase call time and add significant costs with little or no benefit from a security perspective.

Moreover, EPIC's proposal, and that of the *NPRM*, is not limited to accesses by a customer service representative. It would potentially require logging of every electronic access to CPNI. This would clearly apply to customers accessing their CPNI by using an automated attendant or an abbreviated dialing code to determine their usage or balance. In addition, customer data that constitutes CPNI is accessed electronically every time a phone is used.

There is simply no basis for any requirement of an audit trail for accesses to CPNI. An audit trail requirement would be of little or no help in tracking down improper access by data brokers and would greatly increase the cost of operating a business that consists of service that can only be provided by accessing CPNI.

C. Encryption (¶ 19)

In the *NPRM*, the Commission asks whether stored CPNI should have to be encrypted.³⁷ Encryption would have had no impact on the data broker access to call records. As described above, there is no indication that data brokers hacked into any of the carriers' systems in order to get the customer data.

Encryption guards against unauthorized access to systems, so if someone hacks into a protected system and they shouldn't be there, the data will be unreadable. However, in the case of "social engineering" or "pretexting," the representatives who are contacted are authorized to be in the system with access to the CPNI, and thus if the data is encrypted they will have decrypted access to it. As a result, encryption for stored call records would do nothing more than add significant costs, cause delays in responding to customer inquiries, and jeopardize system availability and performance. Cingular service representatives obtain access to nearly 2 million customer accounts every day in the routine performance of their jobs. Likewise, the network

³⁷ *NPRM* at ¶ 19.

computers that manage the process of setting up and completing calls would have to endure greatly increased overhead if every access to CPNI had to involve encryption and decryption processes.

D. Reduced Data Retention (¶ 20)

In the *NPRM*, the Commission asks for comment on EPIC's proposal to reduce the retention period for call records and other CPNI.³⁸ Cingular does not oppose shorter retention periods for call detail records, but this would do little, if anything, to address the problem of data brokers illicitly acquiring CPNI. Cingular's experience is that most data brokers are focusing on the last 100 calls made or calls within the last 90 days. Moreover, there are currently no FCC regulations mandating a specific retention period, so there is no need for prescriptive regulations. In any event, because of the costs associated with storage and retrieval of large quantities of data, carriers have economic incentives not to maintain call records any longer than necessary.

EPIC suggests that call records should be deleted when they are no longer needed for billing or dispute purposes, and it recommends depersonalizing the call detail records in order to avoid the data brokers from getting this information. Neither of these approaches would solve the data broker social engineering situations, because data brokers are focusing on obtaining recent call records.

Carriers must have ready access to call detail records in order to bill the customer and address billing disputes, which requires accessing this information for about six months, given that not all issues are raised or resolved immediately. Accordingly, Cingular's customer care representatives have immediate access to only 180 days worth of call detail records. Thus, even without agency intervention, the call detail records are already being made readily accessible for

³⁸ *NPRM* at ¶ 20.

only a limited period of time. Moreover, there is no evidence of system breaches that have provided data brokers with access to call records or CPNI from archived records. Requiring a reduced retention time for such records or depersonalizing them would serve little purpose.

E. Notice of CPNI Disclosure or Security Breaches (¶¶ 21-24).

In the *NPRM*, the Commission asks for comment on EPIC proposals regarding the issuance of notices to customers when the security of CPNI may have been breached and also asks whether carriers should be required to notify customers either before or after the release of CPNI to others.³⁹

Notice of Potential Breach of Security. The Commission seeks comment on the benefit of notifying customers not only when the security of their CPNI *has* been breached, but when it *may* have been breached. Such notifications are unnecessary, counterproductive, and costly; the Commission should not require them.

It is instructive to look to the experience of the financial industry, where customer notifications have been required by federal agency guidance issued pursuant to the Gramm-Leach-Bliley Act. There is considerable evidence that widespread notifications of possible data security breaches do not benefit consumers, because not every breach, or potential breach, raises a significant risk of identity theft or financial fraud, and some experts have recommended limiting such notifications to situations where the consumer needs to take action to safeguard his or her information.⁴⁰ Requiring notifications to be made in less critical cases results in “unnecessarily alarming and immunizing consumers to notices that information about them may

³⁹ *NPRM* at ¶¶ 21-24.

⁴⁰ See Testimony of Oliver I. Ireland before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, on H.R. 3997, Nov. 9, 2005, *available at* <<http://www.sia.com/testimony/html/ireland11-9-05.html>>.

have been compromised.”⁴¹ Already, many consumers pay scant or no attention to notifications from financial institutions.⁴² Eventually, consumers will start treating lightly even the serious notices of actual breaches posing a risk, just as the villagers in the tale of the boy who cried “Wolf!” discounted a real distress call after becoming inured to the boy’s false alarms.

Requiring customer notification of all potential breaches of security regarding CPNI and more specifically, call detail records, would not compel customers to immediately act to protect their identity. Equally as compelling is the fact that Cingular’s experience demonstrates that customers normally contact their carrier to advise that someone has gotten access to their account information, so in that case, the carrier has been notified by the customer. Obviously, in such cases, there is no need for the carrier, in turn, to notify its customer of a potential breach.

Required Notice prior to releasing CPNI. Cingular does not support notifying customers before CPNI is released. Even banks and other financial institutions that are subject to GLBA requirements do not have to notify customers before releasing private information in a permissible manner. The Commission’s proposal is that carriers be required to call customers on their registered telephone number for the account to verify the customer’s identity before releasing the CPNI to that subscriber. Such an approach would disrupt provision of customer service. Examples of customer inquiries include requests for the bill balance or the minutes used, or requests for an evaluation of which plan best suits a customer’s needs. Requiring such calls to be interrupted for a callback on the account owner’s registered phone number would

⁴¹ *Id.*

⁴² A study submitted to the FTC by the Ponemon Institute showed that of the respondents who recalled receiving privacy notices from their banks, 36% did not read the notices at all and 35% gave them only a “quick read.” Ponemon Institute, Privacy Trust Survey for Retail Banking (redacted version), at question 8B, submitted as attachment to Summary of Statement by Larry Ponemon, *available at* < <http://www.ftc.gov/os/meetings/040129ponemon.pdf>>.

result in long waiting times and increase lost connections, not to mention frustrating customers seeking routine information. Moreover, many such calls are initiated from the mobile handset, whose number can be verified by the customer service representative or automated information system, making a callback totally unnecessary.

Requiring callbacks also should not be necessary regarding the most sensitive CPNI, and the CPNI most likely to be sought by fraudsters, namely call detail records. Current carrier practices in response to the call broker issue render such rules unnecessary. Cingular, for example, has adopted very “customer unfriendly” policies in this regard — prohibiting representatives from providing call detail information to *anyone* by phone, fax, or email. This practice is necessary, but unfortunate — because it prevents Cingular from helping legitimate customers who may have the need to discuss call detail records over the phone. Currently Cingular offers to send the customer a copy of his or her bill by mailing it to the address on file, or, in the alternative, informs the customer that he or she can set up or use an online account to check call detail or instead can go to a retail store and obtain a bill reprint with a photo ID. Carriers are implementing variety of means to protect customer records and need flexibility to continue to change procedures in response to developments. Prescriptive rules, on the other hand, would merely result in static procedures that would deny carriers needed flexibility and could, thereby, reduce rather than increase security.

The real “bad guy” is the data broker. If their activities are curtailed by Congress or the FTC, Cingular may be able to again adopt more customer-friendly policies regarding call detail records. Any prescriptive regulation that requires notification will have a significant negative effect on the customer experience. Imagine a customer calling regarding a potentially fraudulent call under such regulations:

Customer: My bill shows that I made a call to Argentina on February 14th, but I don't know anyone in Argentina; this must be a mistake. Can you help me with that?

Representative: Sure, before we get started I need to verify that you are authorized to have access to the account. Could you give me your Cellular Telephone Number, please? OK, next I need your billing ZIP code. Thank you, please provide me with [certain personal information]. Thank you, now before I can give you any information about your call detail records, I will need to call you on the telephone number registered on this account. Please hold the line while I call you on that line to verify that I can give you this information.

At that point, the situation could go downhill fast. For example, the customer may not be located where they can answer a call to the registered number or could be already calling from that number, or the phone with that number could be stolen, lost, or out of service because of a malfunction or a dead battery. As this illustration shows, a mandatory callback does not offer an acceptable customer service experience. Given the small number of social engineering calls compared to the total number of calls any carrier receives in a day, requiring a representative to go through a routine such as this on every call where call detail records are discussed would be burdensome, costly and time-consuming, and would produce very little, if any, benefit in terms of reducing data broker abuses.

This is true even if the customer is given the opportunity to opt into a notification regime. Offering customers the ability to opt into notification would add significant costs to the business (and thus increase the cost of wireless service to all customers), because accounts would need to be marked with this information and the systems to support this process would need to be designed and maintained. Moreover, if one were to ask a typical customer if he or she wants to opt to be notified by callback when the customer is already talking to the customer representative to ask for information (which would be the majority of cases), the merits of the proposal would

not be immediately apparent to the customer (who would undoubtedly consider the idea silly) and would therefore require a lengthy explanation. Add a one-minute dialog and explanation to each call handled by customer service representatives, and there would be a tremendous negative impact, both financially and in the amount of time the customer spends waiting and then dealing with the representative.

Cingular believes it has struck the right balance for providing notifications about customer accounts. Cingular's policy is to notify customers when their online passwords have been changed. While this is not CPNI, it is the key to accessing sensitive customer information, and this notification is appropriate. There is no compelling reason, however, to notify customers when information about their account has been released to the customer of record. The minimal potential benefits (if there are any) of such an approach are greatly outweighed by the very tangible costs and disadvantages. Moreover, such an approach would do nothing to address the problem of data brokers illicitly obtaining call detail records, which is the reason why EPIC filed its petition and the Commission issued the *NPRM*.

F. Other Approaches (¶ 25)

In the *NPRM*, the Commission urges carriers and other commenters to “think broadly and creatively” in developing methods to guard against CPNI abuse and to submit information about other approaches they may be employing in this regard.⁴³ In the spirit of not divulging our privacy and security practices and thereby “giving wrongdoers a roadmap,”⁴⁴ Cingular is willing to state publicly only that, consistent with Section 222, it has internal teams that focus on the privacy and security of customer data on a regular and ongoing basis. Those teams have

⁴³ *NPRM* at ¶ 25.

⁴⁴ *Id.*

recommended, and Cingular has implemented, a number of new measures to address the recent data broker issues. For a carrier to provide more specific details of this work would be tantamount to giving the “bad guys” the keys to its business.⁴⁵

Cingular believes that voluntary efforts by carriers, guided by realistic and effective policies, will work far better than prescriptive rules. As discussed in the following section, there may be a proper role for rules setting forth “safe harbor” criteria that, while not mandatory, would insulate a compliant carrier from liability. In this connection, the Commission should endorse carriers’ reliance on recommendations by other Federal information security bodies that have useful application to the telecommunications industry. For example, GAO recently responded to concerns about the security of private information held by the SEC with recommendations⁴⁶ that would be equally beneficial for telecommunications companies handling private data such as CPNI. GAO recommended as follows:

To help establish effective information security over key financial systems, data, and networks, we recommend that the SEC Chairman direct the Chief Information Officer to take the following seven actions to fully develop, document, and implement an effective agencywide information security program:

- Fully document and implement a process for assessing risks for its information systems.
- Finalize comprehensive information security policies and procedures.
- Ensure that all system users comply with annual security awareness training requirements.

⁴⁵ Certain confidential information has previously been provided to the Commission in response to a staff inquiry.

⁴⁶ U.S. Government Accountability Office, *Report to the Chairman, Securities and Exchange Commission, Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program*, GAO-06-408 (March 2006), available at <<http://www.gao.gov/new.items/d06408.pdf>>.

- Institute a testing and evaluation program that includes testing the controls within the general support system.
- Develop a mechanism to track remedial action plans that incorporates all identified weaknesses and related risks.
- Establish a program for handling security incidents with detection, response, analysis, and reporting capabilities.
- Maintain a continuity of operations program that includes fully tested plans for restoring operations.⁴⁷

G. Enforcement (¶ 26)

In the *NPRM*, the Commission requests comment on the creation of a “safe harbor” that would exempt carriers from liability if they operate within a certain set of security parameters. It is questionable, however, whether the FCC’s authority extends to mandating security requirements and punishing carriers for not meeting certain security standards. There is no specific statutory authority for such action, and the Commission’s ancillary authority is limited.⁴⁸

⁴⁷ *Id.* at 20-21.

⁴⁸ The D.C. Circuit held last year that the Commission’s “ancillary jurisdiction is limited to circumstances where: (1) the Commission’s general jurisdictional grant under Title I covers the subject of the regulations and (2) the regulations are reasonably ancillary to the Commission’s effective performance of its statutorily mandated responsibilities.” *American Library Association v. FCC*, 406 F.3d 689, 700 (D.C. Cir. 2005). The Court warned that “[g]reat caution is warranted here, because the disputed . . . regulations rest on no apparent statutory foundation and, thus, appear to be ancillary to nothing.” *Id.* at 702. While Title II of the Communications Act grants the Commission specific authority to regulate certain aspects of interstate common carrier communications services, no provision of the Act purports to grant the Commission plenary authority over common carriers. Section 2(a) of the Act, 47 U.S.C. § 152(b), provides that the Act applies to all interstate communications, but it does not, by its terms, grant the FCC regulatory powers over all interstate communications providers. The FCC has used this as the fount of its “ancillary jurisdiction,” and the U.S. Supreme Court held in *United States v. Southwest Cable Co.*, 392 U.S. 157, 172 (1968), that it “found no reason to believe that § 152 does not, as its terms suggest, confer regulatory authority over ‘all interstate . . . communication by wire or radio.’” That decision, however, pointed out that the Commission’s jurisdiction under Section 2(a) “is restricted to that reasonably ancillary to the effective performance of the Commission’s various responsibilities” under other specific sections of the Act. 392 U.S. at 178. Accordingly, courts have held the Commission to lack jurisdiction over building construction issues that would unquestionably affect communications by preventing the construction of a tower, *see Illinois Citizens for Broadcasting, v. FCC*, 467 F.2d 1397, 1400 (7th Cir. 1972), and

(continued on next page)

Nevertheless, if the Commission believes that the public interest requires the adoption of regulations in response to data security concerns, a “safe harbor” rule would be preferable to prescriptive regulations. As the foundation for a “safe harbor” rule, Cingular suggests that guidelines be adopted based on the FTC’s final Safeguards Rule,⁴⁹ which was issued pursuant to Section 501(b) of GLBA.⁵⁰ The FTC rule includes the following:

In order to develop, implement, and maintain your information security program, you shall:

- (a) Designate an employee or employees to coordinate your information security program.
- (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
 - (1) Employee training and management;
 - (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
 - (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
- (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems, and procedures.
- (d) Oversee service providers, by:

(footnote continued)

over contracts that affect the financial conditions of licensees, *see Regents v. Carroll*, 338 U.S. 586 (1950). Likewise, the D.C. Circuit has held that the FCC lacks jurisdiction under Section 2(a) to regulate the use to which communications are put after they have been received. *American Library Association*, 406 F.3d at 700-04.

⁴⁹ 16 C.F.R. § 314.4.

⁵⁰ 15 U.S.C. § 6801(b).

- (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
 - (2) Requiring your service providers by contract to implement and maintain such safeguards.
- (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.⁵¹

VII. SMALL CARRIERS VS. LARGE CARRIERS

In the *NPRM*'s discussion of encryption, and again in its discussion of reporting requirements, the Commission asks whether such requirements would place special burdens on small carriers and whether such carriers should be exempted.⁵² This issue is not unique to encryption or reporting requirements, however. All carriers should be subject to the same security and privacy requirements, including encryption, reporting requirements, and any other CPNI rules that the Commission may adopt.

As Cingular discusses above, there should be no encryption required for any carrier's stored data. If, however, the Commission believes that such data requires encryption to protect customer privacy despite the cost, or that some other rule is needed, all such rules should apply to all carriers, whether large or small, VoIP providers or traditional telephony providers. The same is true for all other CPNI privacy and security rules. If the rules are necessary for customer protection, then all customers should get the protection, rather than some customers being relegated to second-class protection of their private data. The protection is either necessary or it

⁵¹ 16 C.F.R. § 314.4.

⁵² *NPRM* at ¶¶ 19, 30.

is not. If the expense or the burden outweighs the benefits, no carriers should be subject to such rules.

CONCLUSION

For the foregoing reasons, Cingular opposes the adoption of any prescriptive rules concerning CPNI.

Respectfully submitted,

CINGULAR WIRELESS LLC

By: /s/ M. Robert Sutherland/ms
J. R. Carbonell
Carol L. Tacker
M. Robert Sutherland
5565 Glenridge Connector
Suite 1700
Atlanta, GA 30342
(404) 236-6364

Its Attorneys

April 28, 2006