

**Before the
Federal Communications Commission
Washington, D.C. 20554**

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

COMMENTS OF COMPTEL

COMPTEL, by its attorneys, hereby respectfully submits its comments in response to the above-referenced docket.¹ In this proceeding, the Commission responds to recent press accounts regarding public disclosure of customer proprietary network information (CPNI) by third party, non-telecommunications carrier entities, and asks whether its privacy rules should be updated to prevent the reoccurrence of such incidents.²

¹ COMPTEL is the leading industry association representing communications service providers and their supplier partners. COMPTEL members share a common objective: advancing communications through innovation and open networks.

² See "House Committee Fires Subpoenas at Phone-Record Data Brokers," RCR Wireless News, Apr. 6, 2006 ("In addition to legislative action, the Federal Communications Commission recently proposed strengthening the protection of customer call records. In February the commission began seeking comment on five specific measures proposed by the Electronic Privacy Information Center on the topic. Although the customer-call-records scandal erupted in early January following a segment aired on the CBS Evening News, EPIC

Specifically, the Commission asks whether it should adopt new privacy rules, such as those proposed by the Electronic Privacy Information Center (EPIC), to strengthen consumer protections against unlawful disclosure of personal communications-related information.³ Although the Commission has already asked for, and received, comments in response to EPIC's petition, this latest notice of proposed rulemaking (NPRM) again "requests[s] comments on the issues raised by EPIC."⁴ As discussed in greater detail below, COMPTTEL agrees with EPIC that protecting consumer privacy is a paramount responsibility of the Commission. At the same time, the measures proposed by EPIC in its petition would not advance the Commission's privacy protection measures, and indeed would largely impose massive additional costs on carriers and their customers without any concomitant benefits to consumers.

In its petition, EPIC asks the Commission to adopt new rules to address the practices of so-called "data brokers" and private investigators that, according to EPIC, make personal call record information available and "are taking advantage of inadequate security through pretexting, the practice of pretending to have authority to access protected records; through cracking consumers' online accounts with communications carriers; and possibly

first raised the issue last August. EPIC asked that the FCC implement rules to protect customers' call records.").

³ 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 (filed Aug. 30, 2005) (EPIC Petition).

⁴ Notice at ¶ 9; *see* Consumer & Governmental Affairs Bureau, Reference Information Center, Petition for Rulemakings Filed, RM-11277, Public Notice (CGB Sept. 29, 2005), *available at* <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-261315A1.pdf>.

through dishonest insiders at the carriers.”⁵ EPIC does not allege – nor does the Commission in its Notice suggest – that telecommunications carriers are responsible for recent incidents of disclosure of cell phone records. Rather, EPIC and the Commission both recognize that third party “data brokers,” pretextually claiming to have lawful entitlement to CPNI, are responsible for unlawful disclosure of customer information. As such, it is the pretexters – and not telecommunications carriers – that are the proper subject of the Commission’s inquiry.

COMPTEL member companies are subject to the full panoply of the Commission’s CPNI rules, including the penalties associated with violation of those rules, and thus have a powerful incentive to protect customer privacy. Ironically, the largest telecommunications companies in the country, including Verizon and AT&T, are not subject to those consumer protection rules, and thus have no incentive to protect customer privacy, thanks to the Commission’s decision to exempt Bell broadband services from common carrier regulation. For example, the Commission’s recent decision to grant Verizon’s broadband forbearance petition by operation of law removes common carrier regulation from Verizon’s broadband services.⁶ Because Verizon is no longer a “telecommunications carrier” with respect to the services for which it was granted forbearance, Verizon (alone among

⁵ EPIC Petition at 1.

⁶ *See* “Verizon Telephone Companies' Petition for Forbearance from Title II and Computer Inquiry Rules with Respect to their Broadband Services Is Granted by Operation of Law,” Press Release, WCB Docket No. 04-440, issued Mar. 20, 2006.

telecommunications companies) is exempt from section 222 of the Act, and therefore need not comply with the Commission's CPNI rules.⁷

The Commission also asks whether the current opt-out regime “sufficiently protects the privacy of CPNI in the context of CPNI disclosed to telecommunications carriers’ joint venture partners and independent contractors.”⁸ In particular, the Commission asks commenters to address whether an opt-in regime would better protect customer privacy by preventing disclosure of CPNI to third party vendors. To the extent that the Commission identifies problems with third party vendors that unlawfully obtain, by use of pretexting and other fraudulent means, access to CPNI, such instances are best addressed through Commission enforcement action. Because the specific problems identified by the Commission are the result of behavior that violates the existing CPNI rules, there is no reason to require carriers that obey the rules to radically redesign their operations support systems. As the Commission concedes in its Notice, the type of third party disclosure of CPNI described by EPIC in its petition is already a violation of the statute and the Commission's existing rules.⁹ Indeed, the wireless industry association (CTIA) conceded that the vast majority of CPNI

⁷ 47 U.S.C. § 222(a) (“Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.”). Numerous parties have challenged the Commission's decision forbearing from common carrier regulation of Verizon's broadband services.

⁸ Notice at ¶ 12.

⁹ Notice at ¶ 12, *citing* 47 C.F.R. § 64.2007(b)(2); 47 U.S.C. § 217.

disclosure violations are the result of pretexting, which is unlawful.¹⁰ For example, telecommunications carriers are permitted to disclose CPNI to their joint venture partners and independent contractors that provide communications-related services after obtaining a customer's "opt-out" consent.¹¹ Such disclosure is subject to additional Commission-mandated safeguards that require the telecommunications carrier to enter into confidentiality agreements with independent contractors or joint venture partners that protect the confidentiality of a customer's CPNI.¹² It is clear that any consumer benefits from such a wholesale reversal of the Commission's CPNI rules would be far outweighed by the additional costs imposed on the telecommunications industry and, in all likelihood, simply passed on to consumers.

In its petition, EPIC identifies five additional CPNI safeguards that it believes should be mandated under the Commission's rules. Specifically, EPIC urges the Commission to require telecommunications carriers to adopt: consumer-set passwords, audit trails, encryption, limiting data retention, and notice procedures.¹³ Although certain of these proposals may have merit, they miss the underlying issue. EPIC does not suggest that the Commission's rules fail to render unlawful the pretexting activities of data

¹⁰ See Letter from Paul Garnett to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 Attach. at 2 (filed Feb. 2, 2006) (quoting CTIA testimony before Congress that "[o]verwhelmingly, the vast majority of cell phone records are being fraudulently obtained through the use of 'pretexting.'").

¹¹ 47 C.F.R. §§ 64.2005(b), 64.2007(b)(1).

¹² 47 C.F.R. § 64.2007(b)(2).

¹³ Notice at ¶ 14.

brokers and other third parties. Nor does EPIC suggest that the Commission, or other branches of government, do not have existing enforcement authority to address such unlawful behavior. Rather, EPIC proposes steps that would greatly increase the costs of compliance with no demonstration of benefits. For example, EPIC proposes that all carriers be required to record all instances when a customer's records have been accessed, whether information was disclosed, and to whom.¹⁴ Although BellSouth, for example, already made clear to the Commission that such audit trail obligations would be hugely costly,¹⁵ EPIC simply asserts that such an audit trail requirement would deter company insiders from unlawfully disclosing information, and would aid companies in detecting such fraudulent behavior.¹⁶ But imposing massive costs on every telecommunications carrier – costs that would invariably be passed on to consumers – in the speculative hope that lawbreakers would be deterred from behavior that already violates the Commission's rules does nothing to protect consumer interests.

The same is true for encryption, another proposal set out by EPIC in its petition. It is difficult to see how data encryption will solve the problem the Commission purports to address in this Notice. Although data encryption might prevent unlawful access to CPNI by hacking or other forms of data theft, it is not clear how it would impact the disclosure of information to a

¹⁴ EPIC Petition at 11.

¹⁵ BellSouth Comments, CC Docket No. 96-115, at 5-6.

¹⁶ EPIC Reply Comments, CC Docket No. 96-115, at 7.

party that lies about its entitlement to CPNI. As with other measures proposed by EPIC, data encryption requirements would impose unnecessary and costly burdens on telecommunications carriers without any measurable impact on the type of data broker malfeasance the Commission desires to eliminate.

OTHER MATTERS THAT THE COMMISSION SHOULD CONSIDER

The Commission has asked whether there are issues other than those specifically enumerated in the NPRM that it should take into account in determining a course of action. COMPTTEL submits that there is at least one other issue that the Commission should take into account. It is an issue that has arisen in the context of the “commercial agreements” for UNE-P replacement products that the incumbent local exchange carriers have refused to negotiate. In an effort to ensure the integrity and preserve the security of CPNI, the Commission must make clear to ILECs that it will not tolerate any attempt to force CLECs to accept language in their “commercial agreements” that requires them to relinquish control over CPNI or indemnify ILECs for misuse of their customers’ CPNI. This is not a hypothetical problem but a very real situation with which CLECs that have entered into agreements with AT&T for “Local Wholesale Complete,” the UNE-P alternative offered by AT&T, must contend.

Pursuant to the requirements of Section 211 of the Communications Act and Section 43.51 of the Commission’s rules, AT&T has been filing with the Commission the “private commercial agreements” it has entered into with CLECs for Local Wholesale Complete or LWC. The agreements are thus publicly available and convenient for the Commission to review. COMPTTEL has attached as Exhibit 1

pertinent pages from the Commercial Agreement between SBC-13 State and West Telcom, Inc. filed with the Commission on September 29, 2005 to illustrate the type of contract language that the Commission should prohibit in an effort to better protect CPNI. The Commission's files demonstrate that AT&T has entered into Commercial Agreements with numerous CLECs that are virtually identical in all significant respects to the West Telcom Agreement.

In Paragraph 13.2 of the Attachment Local Wholesale Complete (LWC) to the Commercial Agreement, AT&T reserves to itself the right to provide the CPNI of the CLEC's customers to any third party as AT&T may deem appropriate to resolve traffic issues:

SBC-13 STATE may provide information on any LWC-related traffic to other telecommunications carriers *or any third party* as appropriate to resolve traffic issues, including without limitation those involving compensation.

Attachment Local Wholesale Complete, Paragraph 13.2 (emphasis added). Section 2.10 of the Appendix LWC DUF (daily usage file) requires the CLEC to indemnify AT&T from any liability arising out of the conduct of its employees in providing message data or usage data, including customer specific information, associated with the telephone numbers of the CLEC's end users:

CARRIER also agrees to release, defend, indemnify and hold harmless SBC-13 STATE from any claim, demand or suit that asserts any infringement or *invasion of privacy or confidentiality of any person(s), caused or claimed to be caused, directly or indirectly, by SBC-13 STATE employees* and equipment *associated with provision of any message data or other usage data* as part of or in conjunction with LWC. *This includes, but is not limited to lawsuits and complaints arising from disclosure of any customer specific information associated with either the originating or terminating telephone numbers or calls to a LWCAL or LWC Number.*

Appendix LWC DUF, Paragraph 2.10 (emphasis added).

Because AT&T is the wholesale provider of the UNE-P like LWC product to the CLECs, it is in a unique position to access and provide to undisclosed third parties without the CLECs' knowledge confidential and proprietary call detail and usage records relating to the CLECs' end users. The fact that AT&T not only reserves to itself the right to do so as a condition of providing LWC, but also requires the CLEC to indemnify it for any improper disclosure of the CLECs' customer CPNI is unconscionable and effectively strips the CLEC of any ability to meaningfully safeguard its customers from the misuse or improper disclosure of their call records.

In bringing this issue to the Commission's attention, COMPTTEL does not mean to imply that AT&T would intentionally misuse or improperly disclose CPNI belonging to its CLEC customers' end users. Nonetheless, the contract language in the LWC Commercial Agreements essentially gives AT&T and any unscrupulous employee who might be inclined to misuse or improperly disclose the CPNI of CLEC customers to data brokers a free pass for doing so and leaves the CLEC holding the bag. Such an approach is patently inconsistent with the Commission's expressed intent in this proceeding to strengthen the privacy protections afforded to CPNI collected and held by telecommunications carriers. For these reasons, the Commission should make clear in any Memorandum Opinion and Order issued in this proceeding that language such as that cited from the AT&T LWC Commercial Agreement is unenforceable and void as against public policy.¹⁷

¹⁷ COMPTTEL submits that any disclosure by AT&T of CLEC end user CPNI to another carrier or any other third party for any reason whatsoever should be subject to the execution of a non-disclosure agreement by the receiving party and that AT&T should not be permitted to escape liability for itself or its employees by requiring its CLEC customers to indemnify it for the misuse of CPNI.

Respectfully submitted,

/s/ Jason Oxman

Jason D. Oxman
Mary C. Albert
COMPTEL
1900 M. Street, N.W.
Suite 800
Washington, DC 20036
Ph - 202-296-6650
Fax - 202-296-7585