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

In the Matter of	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information	)	RM 11277

COMMENTS OF VERIZON[1]

EPIC's petition[2] rightly points out a growing problem, which the Commission should address: the existence of "data brokers" that claim they can obtain access to customer proprietary network information ("CPNI") and sell it to third parties on demand. To the extent these companies are using unlawful methods to obtain confidential customer information, such as misrepresenting themselves as authorized customers ("pretexting") in order to get the information from carriers, or hacking into consumers' online accounts, *see* EPIC Petition, at 6-7, the Commission should assist the industry in bringing such wrongdoers to justice. However, the Commission should not adopt EPIC's suggestion to "conduct an inquiry into the current method of security measures being used to verify the identities of those requesting individual CPNI," *id.* at 2. Doing so likely would be giving wrongdoers a roadmap of how to more easily obtain confidential customer information, and may lead to unnecessary burdens on carriers and their customers. The Commission should instead work with carriers and the Federal Trade Commission ("FTC") on ways to track and combat actions by those persons that unlawfully obtain and sell this information.

---

1 The Verizon telephone companies ("Verizon") are the local exchange carriers affiliated with Verizon Communications Inc., and are listed in Attachment A.

2 Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, RM 11277 (filed Aug. 30, 2005) ("EPIC Petition").

It is true that carriers are the "first line of defense" against those who would access and sell CPNI illegitimately. *See* EPIC Petition, at 8. Verizon is committed to protecting the privacy of confidential consumer information, and continues to review its methods and procedures for protecting such information to see whether those processes can be improved. However, the unfortunate fact is that no method of defense can stop all criminals who are willing to engage in fraud and theft. This is not something that is unique to carriers, or to CPNI; perpetrators steal confidential customer information of all types through Internet "phishing" scams, telemarketing fraud, hacking into computer systems, and any other number of methods.[3]

Because the problem is not a CPNI-specific one, the Commission should not adopt a solution that is tailored only to protecting customer proprietary network information. Carriers such as Verizon already have in place protections for encryption of sensitive data.[4] State and federal legislative initiatives are underway, or already in effect, to address the notification

---

[3] *See* Fed. Trade Comm'n, *Take Charge: Fighting Back Against Identity Theft* (June 2005), *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf; Fed. Trade Comm'n, *Information Brokers Settle FTC Charges* (rel. March 8, 2002), *available at* http://www.ftc.gov/opa/2002/03/pretextingsettlements.htm; OnGuard Online, *Stop-Think-Click: 7 Practices for Safer Computing* (Sept. 2005), *available at* http://onguardonline.gov /stopthinkclick.html; Verizon, *Verizon Warns Customers: Beware of On-line "Phishing" Scam* (rel. Apr. 21, 2004), *available at* http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=84720; SBC, *SBC Internet Services Warns Customers to Protect Personal Information and Credit Card Numbers Against "Phishing" Scams*, (rel. July 19, 2005), *available at* http://www.sbc.com/gen/press-room?pid=5097&cdvn=news&newsarticleid=21747.

[4] *See, e.g.,* Verizon, *Privacy and Customer Security Policies* (Jan. 2005), *available at* http://www22.verizon.com/about/privacy/customer/; Verizon Wireless Privacy Statement, *available at* http://www.verizonwireless.com/b2c/footer/privacy.jsp; Qwest, *Online Privacy Policy* (Sept. 29, 2005), *available at* http://www.qwest.com/legal/privacy.html; Sprint Nextel, *Sprint Privacy* Policy (Sept. 1, 2005), *available at* http://www.sprint.com/legal/sprint_privacy.html#principles; *see also* SBC, *Online Privacy Policy* (Sept. 19, 2005), *available at* http://www.sbc.com/gen/privacy-policy?pid=2506.

companies must give of security breaches.[5] Adoption of requirements specific to protecting only CPNI thus are unnecessary, and likely would require carriers to adopt expensive solutions that are apt to be, at best, duplicative of other requirements, and at worst, in conflict with measures adopted more generally to protect confidential customer information.

In addition, any rulemaking proceeding to consider whether to implement more stringent regulations on the manner in which carriers protect CPNI will be a lengthy process and, ultimately, is not likely to solve the problem. Indeed, setting particular guidelines on the types of measures carriers must take to protect CPNI might actually make the problem *worse*, because it would give wrongdoers a roadmap of the information they need in order to obtain access to CPNI.

The only alternative "security" measure that EPIC proposes is the establishment of customer-set passwords in order to obtain CPNI. EPIC states that, "[a] unique and separate password chosen by the account holder at the time of phone activation would greatly increase security of CPNI." EPIC Petition, at 11. While it is unclear whether such a requirement would provide more complete protection of customer data, it also brings the potential to hamper a customer's ability to transact legitimate business. After service has been established, a customer may not need to contact his carrier for many months, and when he does have a need to talk to the carrier, may have forgotten the password he selected. EPIC does not suggest what carriers would do in response to a customer that calls to request confidential data if he or she has forgotten the password. If the customer cannot obtain any information unless he remembers the now-forgotten password, this risks creating unnecessary burdens on the customer; for example, a

---

[5] *See, e.g.*, summaries of pending and current federal and state laws regarding security breach notification, at http://www.pirg.org/consumer/credit/statelaws.htm, http://www.namic.org/compliance/DataSecurityBreach.pdf, and http://media.gibsondunn.com/fstore/documents/pubs/072705-SecurityBreachCHART.pdf.

customer that has misplaced his bill and calls to find out information from the carrier would likely be frustrated if he were informed that he may face disconnection of service for nonpayment, but the carrier cannot tell him how much he owes, or when payment is due. The alternative – having the customer identify certain, objective information in lieu of a password – sets up the same problems raised by EPIC in its petition, of creating a system that can be circumvented by industrious criminals. In addition, instituting an industry-wide mechanism that requires the adoption of password-protected accounts is unlikely to deter wrongdoers; industrious scammers will likely simply just shift techniques, by posing as the carrier and emailing or calling the customer to request his password. The balance between protecting customer data with password-only protection, and allowing for customer convenience in maintaining flexible authentication procedures for obtaining such data through other means, is a difficult one; the Commission should continue to allow carriers and their customers to develop the most appropriate solutions, rather than imposing a one-size-fits all mandate that would give wrongdoers a roadmap of the types of data they need to collect to obtain CPNI.[6]

EPIC also proposes a number of other carrier-based requirements that would be incredibly burdensome. For example, to the extent new rules would impose requirements for specific procedures that are different from those already in place, the document retention and encryption proposals likely would cost the industry hundreds of millions of dollars to develop

[6] The carrier may choose, for example, to allow customers to obtain password protections upon request; however some customers, such as large businesses that authorize many persons to obtain information on their accounts, may find a password-based system difficult to administer.

and implement.[7] In addition, the requirement that carriers give notice to the Commission and other individuals when there is a "security breach" resulting in the release of CPNI to an unauthorized recipient, EPIC Petition at 11, likely will be ineffective at combating most fraudulent practices because, if the data broker or investigator is posing as a carrier's customer, the carrier may have no way of knowing that a "security breach" occurred.

Rather than a carrier-centered approach, the best way to attack the problem is to go after its source: the wrongdoers themselves. As the petition points out, many of the "data brokers" are readily identifiable, because they advertise on the Internet about their purported ability to obtain confidential calling data. *See* EPIC Petition, at 6 & attachments. Verizon Wireless, EPIC, and others have brought actions in the courts and before the Federal Trade Commission, seeking to stop some of the more egregious violators.[8] The Commission should work with the FTC on developing a joint method for bringing these parties to justice. For example, the agencies could create a hotline or website link to report suspected illegal activity, and create a joint task force to

---

[7] For example, EPIC proposes that carriers be required to "record all instances where a customer's record is accessed, whether there has been a disclosure of information, and to whom the information has been disclosed"; encrypt CPNI stored within the carrier's systems; and delete call detail records "after they are no longer needed for billing or dispute purposes." EPIC Petition, at 11.

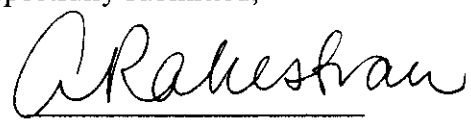
[8] *See, e.g.*, Verizon Wireless, *Theft of Verizon Wireless Customer Records by Tennessee Company Halted* (rel. Sept. 15, 2005) *available at* http://news.vzw.com/news/2005/09/pr2005-09-15.html; Electronic Privacy Information Center, *Complaint and Request for Injunction, Investigation and for Other Relief in the matter of e-Commerce, Inc.* (Fed. Trade Comm'n July 7, 2005) *available at* http://www.epic.org/privacy/iei/ftccomplaint.html; *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (N.H. 2003); *FTC v. Information Search Inc.*, Stipulated Final Judgment and Order, No. AMD01-1121 (D.Md. Mar. 15, 2002), *available at* http://www.ftc.gov/os/2002/03/infosearchstip.pdf; *FTC v. World Media Brokers Inc.*, Memorandum Opinion and Order, No. O2 C-6985 (N.D.Ill. Mar. 1, 2002), *available at http://www.ilnd.uscourts.gov/racer2*.

examine the best ways to shut down such actions.[9] By acting aggressively to investigate and prosecute those parties that use illegal methods to obtain CPNI without customer consent, the Commission and FTC can eliminate any economic incentives for bad actors to trade in such data. A strong offensive strike at the wrongdoers will be far more effective at eliminating the problem than any defensive measures that carriers or the Commission can adopt.

CONCLUSION

The Commission should not initiate a rulemaking proceeding on EPIC's petition, but should instead work with the Federal Trade Commission to take action to stop third party data brokers and private investigators from engaging in unlawful conduct.

Respectfully submitted,

By: 

Michael E. Glover
Of Counsel

Edward Shakin
Ann Rakestraw
VERIZON
1515 N. Court House Road
Suite 500
Arlington, VA 22201-2909
703.351.3174

Counsel for the Verizon
telephone companies

October 31, 2005

---

[9] The Commission and the FTC have worked together on several initiatives in the past, including the creation of a do-not-call registry, and a joint policy statement and public forum about the advertising of long distance services. *See Federal Trade Commission and Federal Communications Commission to Hold Joint Public Form on Advertising of Long Distance Services* (rel. Sept. 23, 1999), *available at* http://ftp.fcc.gov/Bureaus/Common_Carrier /News_Releases/1999/nrcc9070.html; Kathleen Abernathy, *FCC and FTC Establish National Do-Not-Call Registry*, Focus on Consumer Concerns, Vol. 3, No. 2, (Sept. 2003) *available at* http://www.fcc.gov/commissioners/abernathy/news/donotcall-registry.html; *Federal Communications Commission and Federal Trade Commission Issue Joint Policy Statement on Deceptive Advertising of Long Distance Telephone Services* (March 1, 2000), *available at* http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/2000/nrmc0009.html.

ATTACHMENT A

THE VERIZON TELEPHONE COMPANIES

The Verizon telephone companies are the local exchange carriers affiliated with Verizon Communications Inc. These are:

Contel of the South, Inc. d/b/a Verizon Mid-States
GTE Southwest Incorporated d/b/a Verizon Southwest
Verizon California Inc.
Verizon Delaware Inc.
Verizon Florida Inc.
Verizon Maryland Inc.
Verizon New England Inc.
Verizon New Jersey Inc.
Verizon New York Inc.
Verizon North Inc.
Verizon Northwest Inc.
Verizon Pennsylvania Inc.
Verizon South Inc.
Verizon Virginia Inc.
Verizon Washington, DC Inc.
Verizon West Coast Inc.
Verizon West Virginia Inc.