Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF VERIZON WIRELESS

Verizon Wireless respectfully submits these comments opposing the *Petition*[1] filed by the Electronic Privacy Information Center ("EPIC") in the captioned proceeding. Verizon Wireless urges the Commission not to initiate a rulemaking to impose new requirements on telecommunications carriers for verifying the identity of parties attempting to access customer proprietary network information ("CPNI").

Requiring carriers to file comments detailing their security practices is the wrong approach to the "social engineering" problem that EPIC identifies in the *Petition*, as such information would only serve as a roadmap for social engineers. The Commission should instead establish a joint task force with the Federal Trade Commission ("FTC") to take coordinated enforcement action against offending parties. If the Commission decides to begin a rulemaking, it will need to balance carefully whatever benefits any new rules might have with the harms that could result from standardization of carriers' procedures and the adverse impact on customer convenience. Finally, Verizon Wireless does not

---

[1] Petition of the Electronic Privacy Information Center For Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, filed August 30, 2005 ("*Petition*").

support the proposals that EPIC has recommended that carriers implement to deter social engineering.

I. VERIZON WIRELESS AGGRESSIVELY PROTECTS ITS CUSTOMERS' PRIVACY.

In its *Petition,* EPIC asks the Commission to initiate a rulemaking that would establish more stringent security standards for telecommunications carriers that release CPNI. EPIC claims that carriers' practices do not adequately address the practices of third-party data brokers and private investigators that have been accessing CPNI without authorization.[2] To combat these breaches of privacy, EPIC asks the FCC to investigate carriers' current security practices, evaluate whether there are inadequacies in these practices, and determine whether additional security measures are warranted to protect customers from unauthorized access to their CPNI.[3]

Verizon Wireless takes its customers' privacy very seriously. Amid growing concerns about how customer information is used and shared, Verizon Wireless goes to great lengths to ensure that information regarding its customers is kept private. Maintaining a reputation for the highest standards of business practice is essential to success in the competitive wireless marketplace.

As part of this commitment to safeguard privacy, Verizon Wireless provides customers notice of its efforts to protect their privacy in three separate documents: the Customer Agreement, Privacy Statement, and Privacy Policy.[4] In the Customer Agreement, Verizon Wireless pledges to protect customer information from disclosure

---

2 *Id.* at 1.

3 *Id.* at 10.

4 These documents are available online at www.verizonwireless.com through links at the bottom of the Verizon Wireless home page.

without the customer's permission, except under limited circumstances such as a requirement to produce such information when Verizon Wireless receives a subpoena or other legal process. Like the Customer Agreement, the Privacy Statement indicates that Verizon Wireless will not disclose "individual information" collected via web sites except under certain limited circumstances. The Privacy Policy states that Verizon Wireless will not disclose "personally identifiable information" except under certain limited circumstances.

Verizon Wireless also provides its customer service representatives with extensive training and detailed instructions concerning the importance of and need for customer privacy. In addition to training its customer service representatives to comply with federal law, including 47 U.S.C. § 222, Verizon Wireless trains its representatives to verify the identity of callers and to recognize the common forms of social engineering. Verizon Wireless also requires its customer services representatives to abide by its Code of Business Conduct, which provides that: (a) customer records may be disclosed outside of Verizon Wireless only with the customer's consent, in accordance with Verizon Wireless procedures or lawful process such as a subpoena, court order, or search warrant; (b) information relating to a specific customer or to customers in general, such as customer names, customer contacts, terms of customer contracts, customer proposals, types, quantities of service, calling patterns, and billing information, must not be disclosed without proper legal process or used for non-business purposes; and (c) a customer service representative may not access or disclose customer information unless there is a proper business reason or legal process, or give a customer's personal information to a third party without appropriate authorization from the customer in

compliance with Verizon Wireless guidelines. Verizon Wireless continues to receive awards for setting the industry standard for customer service.[5]

Despite these efforts, Verizon Wireless has become aware that several times a day certain individuals seek to obtain confidential customer information from Verizon Wireless by misrepresenting their identities and attempting to deceive Verizon Wireless' customer service representatives. These individuals, who advertise freely on the Internet, either pose as Verizon Wireless customers or employees seeking information on their accounts, or they claim that they are attempting to obtain the information on behalf of the customer. They employ a variety of different tactics to obtain information about a customer's mobile number, address, call detail, and copies of bills.[6]

Verizon Wireless has aggressively investigated incidents of social engineering and worked to identify individuals who have attempted to obtain customer information through deceit and trickery. Verizon Wireless recently sought and obtained a court injunction against Source Resources, Inc., a Tennessee company that advertised on its web site that it could obtain wireless telephone records and other confidential customer information.[7] Verizon Wireless is pursuing similar actions against other parties.

---

[5] For instance, in 2005 alone, Verizon Wireless: (1) ranked highest among U.S. wireless service providers for customer satisfaction based on the latest American Customer Satisfaction Index; (2) scored an "A" in caller satisfaction in Vocal Laboratories' Q1 2005 SectorPulse Wireless Report, leading all wireless carriers; and (3) according to the FCC, had the lowest rate of complaints among wireless carriers.

[6] EPIC suggests that some data brokers are offering location-tracking services for wireless phone users. *Petition* at 9. Verizon Wireless is not aware of how a social engineer could have access to location tracking information because this is not available to customer service representatives.

[7] *Cellco Partnership d/b/a Verizon Wireless v. Source Resources,* Permanent Injunction on Consent, Docket No. SOM-L-1013-05 (Sup. Ct. of N.J.; Law Div.: Somerset County, Sept. 13, 2005).

II. THE COMMISSION SHOULD NOT INITIATE A RULEMAKING TO INVESTIGATE CARRIERS' SECURITY PRACTICES.

Given the sensitive nature of carriers' privacy practices, EPIC's request for the Commission to initiate a rulemaking to examine them in the public domain through notice and comment procedures is not in the public interest. Requiring carriers to detail and defend their security practices under the lens of a public proceeding would only serve to provide a roadmap for individuals aiming to exploit these practices. For example, if "private investigators" know that one carrier requires customers to provide social security number but another uses date of birth to verify a customer's identity, these individuals will be able to tailor their efforts and make it more likely that they will evade carriers' efforts to control unauthorized disclosure. Commission rules that standardize carriers' practices would have the same effect, which would be to make social engineering easier.

Rather than initiating a rulemaking aimed at imposing requirements on carriers, the Commission should focus its efforts on the parties who are engaged in wrongdoing, in this case the social engineers. This Commission should coordinate with FTC to develop a joint enforcement task force to address these matters. In addition to the FCC's authority under Section 222 to regulate the action of carriers, FTC maintains broad authority under Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), to police unfair or deceptive acts or practices. It is therefore appropriate for the FCC and FTC to coordinate, investigate, enjoin, and otherwise prevent these individuals from accessing customer private information.

III. ANY RULES THAT THE COMMISSION CONSIDERS MUST BALANCE THE NEED FOR SECURITY AND CUSTOMER CONVENIENCE.

If the Commission decides to undertake a rulemaking on these issues, it must balance the benefits of requiring specific customer information security measures with the costs that they would almost certainly impose on customers and carriers.

In a world where information security has begun to overwhelm the average individual, customers should not be forced to provide a life history to conduct ordinary business with their carrier. Carriers should be permitted to rely on common authentication procedures that consumers follow such as providing the carrier with mobile number, address, social security number, and/or passcode. These procedures have protected consumers and will continue to do so, as long as they are coupled with training of customer service representatives and policies that promote security such as the refusal to provide call detail information over the phone.

The FCC should avoid measures that require customers to take complicated steps to access data. Although procedures such as mandatory passcodes may enhance security, they might also be burdensome for subscribers who have legitimate reasons for making inquiries about their account activity. Consumers who are denied access to their own information when it is needed for a legitimate purpose blame their carrier, which generates calls to customer service, and this in turn imposes costs on carriers. The Commission should avoid mandatory requirements that engender complaints and that create costly systems requirements for carriers. Instead, it should rely on carriers' own incentives to protect their customers and the importance of allowing carriers to tailor their security procedures to the services they offer and the customers they serve.

As demonstrated below, even the best security measures are subject to incursion. The FCC should not adopt burdensome rules that apply to the whole industry when the better course would be to deal with the actions of a few through the enforcement avenues referenced above.

IV. VERIZON WIRELESS DOES NOT SUPPORT THE RULES PROPOSED BY EPIC TO ENHANCE SECURITY.

In the *Petition*, EPIC suggests a number of proposed rules that the Commission could adopt to protect access to CPNI.[8] Verizon Wireless urges the Commission to reject these proposals.

Consumer-set passwords: Although they are not fail safe,[9] a unique and separate password chosen by the account holder at the time of phone activation increases the security of CPNI. It is for this reason that Verizon Wireless provides customers with the option to add a passcode to their accounts. At the same time, customers' tolerance for maintaining a passcode varies, and the Commission should not require carriers to force customers to have passcodes on their accounts.

Audit trails: Verizon Wireless requires customer service representatives to record all instances when a customer's record is accessed, the subject of the discussion with the customer, and whether they have disclosed any information to the customer. This type of recording is important for purposes of customer service, and it is also helpful in investigating security breaches. It is unclear whether EPIC intends for the FCC to impose any requirements beyond this type of recording, and if so, Verizon Wireless would oppose such requirements.

---

[8] *Petition* at 11.

[9] Passcodes are simply another data element that if obtained provide social engineers with access to customers' accounts.

Encryption: Verizon Wireless uses encryption when it sends customer records to outside sources such as credit bureaus. Encryption is relevant to preventing "hacking" into records from outside sources, but it does not assist carriers in preventing social engineering. The Commission should not impose encryption requirements on carriers.

Customer notice: Verizon Wireless notifies its customers if it becomes aware of a security breach. Not only is it a good business practice to notify customers that their privacy has been compromised, several states require it.[10] FCC rules are not necessary to force carriers to implement practices that any company with good business sense has already implemented.

Limiting data retention: EPIC proposes that carriers eliminate call detail records after they are no longer needed for billing or dispute purposes.[11] EPIC does not specify a time that carriers should retain these records, but one problem with EPIC's proposal is that carriers would be hesitant to destroy or "divorce" identification data from transactional records because it is always unclear when disputes might arise. The Commission would also need to evaluate EPIC's proposal in light of its Part 42 rules that

---

[10] This year alone, five states passed such notice laws: Arkansas, Georgia, Montana, North Dakota, and Washington.

[11] *Petition* at 11-12.

require common carriers to preserve records.[12]

CONCLUSION

For the foregoing reasons, the FCC should deny the *Petition.*

Respectfully submitted,

VERIZON WIRELESS

John T. Scott, III
Charon H. Phillips
1300 I Street, N.W.
Suite 400 West
Washington, D.C. 20005
202-589-3740

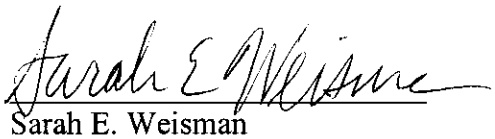
October 31, 2005

[12] *See* 47 C.F.R. § 42.01 *et seq.*

Certificate of Service

I hereby certify that on this 31st day of October, a copy of the foregoing "Comments of Verizon Wireless" in RM-11277 was sent by first class mail to the following party:

Chris Jay Hoofnagle
Electronic Privacy Information Center
West Coast Office
944 Market Street, #709
San Francisco, CA 94102



Sarah E. Weisman