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

In the matter of Implementation of the
Telecommunications Act of 1996:

Petition for Rulemaking to Enhance
Security and Authentication Standards
For Access to Customer Proprietary
Network Information

CC Docket No. 96-115
RM Docket No. 11277

REPLY COMMENTS OF THE
ELECTRONIC PRIVACY INFORMATION CENTER

The Electronic Privacy Information Center (EPIC) respectfully submits these reply comments concerning enhanced security and authentication standards for access to Customer Proprietary Network Information (CPNI).[1]

On July 8, 2005, EPIC filed a complaint with the Federal Trade Commission concerning Intelligent E-Commerce, a company that offers online to sell both wireline and wireless phone records without the consent of the account holder. It soon became clear that this company was just one of dozens of "online data brokers" that advertise the ability to engage in this practice. The prevalence of phone record advertisements, and the apparent ease with which these companies could obtain records from carriers, made it clear that carriers' practices are to some extent responsible for these security problems. Accordingly, EPIC has urged the FCC to initiate a rulemaking to enhance security and authentication standards for CPNI.

I. General Comments

Generally, the carriers responding to the EPIC Petition expressed concern regarding the security of customers' records. Pious referrals were made to privacy policies, existing access policies, and a panoply of privacy laws that apply to carriers in one way or another. One carrier even pointed out that their corporate e-mail is protected with spam filtering.[2] But even the best privacy policy or anti-spam filter cannot address the matter at hand: the fact that 40 different online data brokers are advertising to the general public their ability to gain access to both wireline and wireless phone records. And these are just the companies that advertise this ability online--many others may be obtaining records without proclaiming to the public their ability to do so.

Investigators interviewed by news media concerning these practices claim that obtaining phone records is "easy," and several reporters have ordered phone records on their own to demonstrate how vulnerable the system is.[3] CNN did both:

CHRIS HUNTINGTON, CNN CORRESPONDENT (voice-over): Anthony De

Lorenzo tracks down cheating spouses for a living, a very good living.

(on camera): Is it like shooting fish in a barrel?

ANTHONY DE LORENZO, PRIVATE DETECTIVE: Oh, it's just getting easy now.

HUNTINGTON (voice-over): DeLorenzo says cell phone records are the most valuable tools of his trade. And while he would not give details on just how he gets them, he said they are a synch to obtain.

DE LORENZO: We have the sources already, who are already tied into their contacts. And we could probably get them, if we really need a rush on it, probably within 30 minutes.

HUNTINGTON: It took us only slightly longer. We went to one of the dozens of Web sites that offer a full menu of personal data searches, paid $125 and gave only the name and mobile phone number of a CNN colleague. Six hours later, we were e-mailed a complete and accurate log of his wireless phone calls for the past month.

[Chris] HOOFNAGLE: The sheer number of Web sites offering the cell telephone records suggests that there is a live traffic in this personal information. It also suggests that the carriers aren't adequately protecting personal information.

HUNTINGTON (on camera): There are two main ways that so-called data researchers get cell phone records. The first is by simply tricking the phone companies. Using little more than a name address and a date of birth, they obtain the records under the pretext of being the actual account holder. That's called pretexting.

The second way is from company insiders on the take who sell call logs, typically for a 50 percent cut of the research fee.

The researchers have contact within the phone company to accept the fee to give out the information.

DE LORENZO: Right. I feel that they're either paying for it from an inside source, or they're doing pretext and trying to get that information that way. I figure that's 90 percent of the way how they're getting it.

HUNTINGTON: We called the major wireless companies: Verizon, Cingular, T-mobile and Nextel, which is the carrier of the CNN staffer's cell phone we told you about. All of them told CNN they do not sell customer information. And that they are taking steps to fight pretexts.

Senator Chuck Schumer of New York says selling cell phone records is an unacceptable invasion of privacy and could contribute to crimes like corporate espionage or even help stalkers find their victims.

A company employee who sells phone records is already breaking the law, and now Schumer has introduced legislation to make pretexting for phone records also a federal crime.

SEN. CHUCK SCHUMER, (D) NEW YORK: If you do it for financial records, it's

illegal. If you do it for phone logs, it is not. We should make it illegal right away.

HUNTINGTON: But as things stand...

DE LORENZO: It's amazing how easy it is, just amazing.

HUNTINGTON: And those who trade in the murky market for your cell phone records say business will continue to boom.[4]

We agree with the carriers that the FCC should increase its enforcement efforts to curb these practices. But thus far, carrier enforcement has not chilled this market for phone records. In fact, some still hold that the practice of obtaining wireless records is not illegal.[5]

We again urge the FCC to probe and enhance protections for CPNI. The carriers have rightly pointed out that attention should be focused on the wrongdoers who obtain CPNI. However, the carriers have a duty to protect the confidentiality of CPNI. Thus, regulatory attention should be focused both on punishing wrongdoers, but also on determining whether carriers have adequate systems to protect personal information.

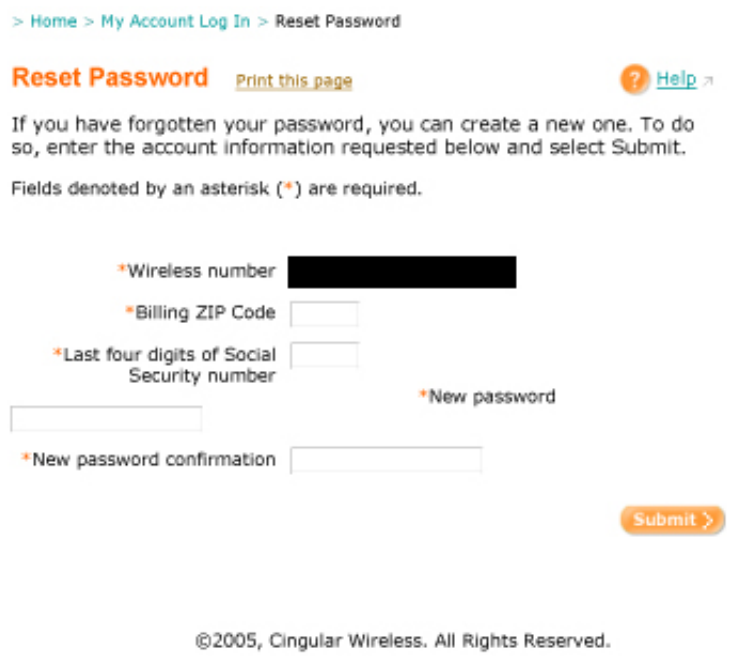
II. Specific Reply Comments

Overall, the CTIA comments fail to recognize that good security is created by the adoption of a number of approaches, and that no one procedure can produce a secure system. Further, EPIC recognizes that no system has perfect security. We seek sensible procedures that enhance security protections, because it is "easy" for online data brokers to crack the current system.

CTIA employs the "straw man" tactic to incorrectly characterize the EPIC Petition by stating that we seek "to require carriers to identify their security procedures on the record and to actually identify the inadequacies in those procedures.[6] EPIC's Petition called for the FCC to investigate current security measures, and inadequacies in those security measures.[7] Obviously, this does not require that these specific procedures and weaknesses be published in the public record.

The CTIA notes that there are weaknesses in password authentication systems.[8] Specifically, there is well-known problem that individuals sometimes forget passwords. But there are ways to manage this problem. For instance, "shared secrets" systems can be developed where the carrier asks the account holder a series of questions, i.e. "what was the name of your first pet," "on what street did you grow up," "what was the name of your grade school," etc. There are many different "shared secrets" questions that can be asked and answered reliably by an account holder.

Carriers are currently managing password problems through practices that are easy for online data brokers to circumvent. For instance, this system employed by Cingular Wireless allows an individual to specify a new password for online account access. In order to choose a new password, one need only submit the billing zip code and the last four digits of the Social Security number. Both identifiers are readily identifiable to online data brokers, as these companies have subscriptions to services that sell Social Security numbers, mother's maiden names, dates of birth, addresses, and other information.



The CTIA next turns to audit trails, claiming that "auditing is no panacea for fraud prevention." [9] But no one procedure is a panacea for security. Auditing can place a significant deterrent against insider abuse, and help individuals determine how their information was obtained after a violation has been detected. Auditing is one piece of effective security procedures.[10]

CTIA continues: "An audit trail…is only of use when someone complains about or reports a violation."[11] This comment illustrates the reactive nature of some in the telecommunications industry on addressing security. Audit trails can be used to proactively detect fraud, even in absence of a specific consumer complaint. For instance, statistical data showing how frequently a customer service representative accesses account records can be tracked. If a certain customer service representative is accessing an abnormally high number of records, that is a sign of fraud that can be investigated.

In the lawsuit brought by Verizon Wireless to prevent a Tennessee company from accessing phone records, Verizon's complaint alleged that the company "made numerous contacts to Verizon Wireless's CSRs in an attempt to deceive a CSR into providing the confidential consumer information…"[12] This behavior, where the data broker makes many attempts to access the same information, is another example of fraudulent activity that can be deterred by audit trails. A log showing many attempts to access a specific customer's information is a sign of fraud.

Additionally, there is a weakness in the current CPNI auditing regulations. 47 CFR 64.2009(c) only requires auditing for specific types of disclosures involving marketing use and third party disclosure of CPNI. The problem articulated by EPIC in the Petition, and replicated by news reporters, concerns impostors who pretend to be the account holder. Under the current auditing regulations, carriers do not have to keep an audit log when they disclose a phone record to an apparent account holder. Audit logs are needed for all situations where the record is accessed.

Finally, CTIA urges the FCC to defer to the FTC, and allow the FTC to enforce laws against online data brokers.[13] FTC, however, has never taken action publicly against a company for selling phone records. FTC has taken action against data brokers for selling financial records, but despite those cases, there still appears to be a robust trade in phone records. As Verizon

Wireless notes, the carrier has "become aware that several times a day certain individuals seek to obtain confidential customer information from Verizon Wireless by misrepresenting their identities…"[14] If Verizon Wireless is aware of several attempts to obtain phone records a day, this is a problem that enforcement alone will not address. There needs to be both an increase in enforcement, and enhanced security measures in order to protect phone records.

Verizon notes that "federal legislative initiatives are underway, or already in effect, to address the notification companies must give of security breaches."[15] While this is technically true, not all security incidents trigger a notice to the consumer. Under the California security breach law, which has served as a model for other states, notice must be given where one of three identifiers is released: the Social Security number, a driver's license number, or a financial account number. [16] Therefore, the improper release of a phone record that is divorced from these three key identifiers does not trigger the notice requirement.

III.Conclusion

There appears to be a healthy trade in phone records by "online data brokers." These companies obtain phone records without the knowledge or consent of the account holder. Existing carrier practices and regulations to protect CPNI are inadequate to stop this trade in personal information. Enforcement actions alone have not, and are unlikely to prevent sale of phone records. FCC intervention is necessary to enhance security standards and authentication standards for access to CPNI.

Respectfully Submitted,

/s

Chris Hoofnagle
Senior Counsel
Electronic Privacy Information Center West Coast Office
944 Market St. #709
San Francisco, CA 94102
415-981-6400

---

[1] Petition of EPIC for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, filed Aug. 30, 2005. EPIC maintains a repository of information about access to phone records online at http://epic.org/privacy/iei/ ("EPIC Petition").

[2] Opposition of Bellsouth Corporation at 6, filed Oct. 31, 2005.

[3] *Ruth To The Rescue Reveals Cell Phone Privacy Issues*, Detroit 4 NBC News, Oct. 19, 2005, available at http://www.clickondetroit.com/money/5127640/detail.html ("Web sites such as one called, "Locate Cell," will sell the last 100 hundred phone numbers you've dialed to anyone who knows your phone number, according to Ruth to the Rescue. Ruth Spencer paid the $110 fee and inputted her own phone number on Locate Cell's Web site, and sure enough, she received an e-mail with the results."). Separately, EPIC has been contacted by two television news producers who claim to have successfully purchased phone records through online data brokers.

[4] Aaron Brown, *Your Privacy at Risk*, CNN, Aug. 12, 2005.

[5] *Id*. (comments of Sen. Schumer). Verizon's lawsuit against Source Resources for obtaining phone records only articulated common law claims (fraud, conversion, and civil conspiracy) rather than a violation of a specific statute. *Cellco Partnership v. Source Resources*, Complaint, No. SOM-L-1013-5 (Sup. Ct. of N.J; Law Div; Somerset County, Jul. 8, 2005), available at http://www.epic.org/privacy/iei/verizonwscomplaint.pdf

[6] CTIA Comments in Opposition to EPIC Petition for Rulemaking at 2, filed Oct. 31, 2005 ("CTIA Comments").

[7] EPIC Petition at 2, 10.

[8] CTIA Comments at 18.

[9] CTIA Comments at 19.

[10] While Bellsouth Corporation complains that it would cost hundreds of millions of dollars to comply with basic auditing procedures, Verizon Wireless notes that it already audits access to records. According to the company, customer service representatives "record all instances when a customers' record is accessed, the subject of the discussion with the customer, and whether they have disclosed any information to the customer." Comments of Verizon Wireless at 7, filed Oct. 31, 2005 ("Verizon Wireless Comments").

[11] CTIA Comments at 19.

[12] *Cellco Partnership*, Complaint at ¶ 26.

[13] CTIA Comments at 20-21.

[14] Comments of Verizon Wireless at 4, filed Oct. 31, 2005 ("Verizon Wireless Comments").

[15] Comments of Verizon at 2-3, filed Oct. 31, 2005 ("Verizon Comments").

[16] Cal Civ. Code § 1798.29.
