ELECTRONIC PRIVACY INFORMATION CENTER

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

**PETITION OF THE ELECTRONIC PRIVACY INFORMATION CENTER
FOR RULEMAKING TO ENHANCE SECURITY AND AUTHENTICATION STANDARDS
FOR ACCESS TO CUSTOMER PROPRIETARY NETWORK INFORMATION**

SUMMARY

The Electronic Privacy Information Center ("EPIC") hereby petitions the Federal Communications Commission initiate a rulemaking proceeding to establish more stringent security standards for telecommunications carriers in releasing Consumer Proprietary Network Information ("CPNI"). CPNI is sensitive information collected by carriers that includes logs of calls that individuals initiate and receive on their phones. Section 222 of the Telecommunications Act makes clear that carriers have the duty of protecting CPNI, with particular emphasis on privacy concerns for personal, individualized data.[1] In implementing Section 222, the Commission has focused on the notice and disclosure requirements necessary to disseminate CPNI data to carrier affiliates and third parties for marketing purposes.[2] However, these efforts did not adequately address third party data brokers and private investigators that have been accessing CPNI without authorization. Data brokers and private investigators 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 through dishonest insiders at carriers.[3] Prompt Commission action is necessary to insure that individualized CPNI is adequately protected from unauthorized third parties as required by Section 222.

In support, EPIC shows the following:

1. That online data brokers and private investigators widely advertise their ability to obtain CPNI without the account holder's knowledge and consent.
2. That strong evidence exists showing the information was not acquired through legal channels. This evidence includes data brokers' advertising guarantees that they can obtain individuals' CPNI in a matter of hours, and that

once obtained, the CPNI cannot be used in court.

3. That this unauthorized release of information suggests that the security and identification requirements carriers use to validate the identity of the CPNI requestor is insufficient to prevent unauthorized third parties from acquiring CPNI.

4. That the prevalence of this current practice and the possibility of further exploitation of lenient security standards create a significant privacy and security risk to carrier customers, one that must be addressed by prompt action by the FCC.

As a result of these concerns, the Commission should immediately initiate a rulemaking proceeding to (a) conduct an inquiry into the current method of security measures being used to verify the identities of those requesting individual CPNI, (b) to hear public comments in developing a security standard that would adequately address the privacy risks, and (c) establish a security standard by rule that heightens privacy of CPNI.

I. Section 222 of the Telecommunications Act requires that telecommunications carriers protect the privacy rights of customers by limiting access to CPNI

Congress enacted the Telecommunications Act of 1996, 47 U.S.C. § 222 *et. seq.*, in part to protect consumer privacy.[4] Section 222 of the Act obligates telecommunications carriers to protect the confidentiality of Consumer Proprietary Network Information ("CPNI").[5] Specifically, section 222(c)(1) states:

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.[6]

CPNI includes calling history and activity, billing records, and unlisted telephone numbers of service subscribers.[7] The Act therefore prohibits carriers from using, disclosing, or permitting access to CPNI without approval of the customer or as otherwise required by law if the use or disclosure is not in connection with the provided service, or listed as one of the exceptions provided for in Section 222(d).

In implementing Section 222, the Commission has focused on the notice and disclosure requirements necessary to disseminate CPNI data to carrier affiliates and third parties for marketing purposes.[8] Since the passage of the Telecommunications Act, the Commission has invited public comment and published orders regarding the extent to which carriers can provide aggregate CPNI to company affiliates and third parties, and what amount of customer notice and approval is necessary for providing this information.[9] However, the security standards necessary to protect against unauthorized solicitors pretending to be the customers themselves is an issue that deserves equal scrutiny, but has been inadequately addressed by the Commission thus far.

II. Congress accorded personal, individualized CPNI the greatest level of protection

The Telecommunications Act affects three categories of customer information to which different privacy protections and carrier obligations apply: (a) individually identifiable CPNI (b) aggregate customer information and (c) subscriber list information.[10] Congress afforded personal, individually identifiable information the greatest protection, and only allowed a carrier to disclose or permit access to such information, without customer approval, where necessary for providing telecommunications services, with four exceptions:

1. to initiate, render, bill and collect for telecommunications services
2. to protect the rights or property of the carrier, or to protect users and other carriers from fraudulent or illegal use of, or subscription to, such services
3. to provide inbound marketing, referral or administrative services to the customer for the duration of the call, if the call was initiated by the customer and the customer approves of the carrier's use to provide such service
4. To provide call location information concerning the user of a commercial mobile service in certain specified emergency situations.[11]

III. Unauthorized third parties are taking advantage of inadequate security and identity verification methods at the telecommunications carriers to access and sell individualized CPNI.

It is not disputed that carriers can provide individualized CPNI to the customer itself. In fact, every month, customers receive billing statements from carriers outlining their call history and rate charges. Many carriers now even have online account access, designed for customers to conveniently review their past or current account activity, billing information, addresses, etc. Carriers also have toll-free customer service numbers, which customers can call to request lost or misplaced statements and call records.

However, the security standards that carriers use to verify the identity of the CPNI requestor have been insufficient to prevent unauthorized third parties from acquiring and exploiting such data for personal and financial gain, providing a significant security loophole through which other privacy and security violations flow. Telecommunications carriers are not responsible for actively disseminating information to unauthorized third parties. Rather, unauthorized third parties have been exploiting security standards at the carriers to access and sell the information acquired through illegal means.

Online data brokers are firms that offer private investigation and other data services through Internet websites. These firms charge customers fees based on a graduated scale for the research services they provide, depending on the details of the data sought. Some offer to search for long-lost friends, relatives, or lovers. Others provide services specifically for spouses to spy on each other. Though some of the information these data brokers offer to retrieve and sell are available through public records, other information comes from proprietary sources, some of which is protected from disclosure by privacy statute or regulation.

For instance, some of these data brokers offer services to retrieve telephone call records. Some will retrieve it with only the telephone number provided, sometimes with turnaround times of 1-2 hours. For example, Intelligent e-Commerce, Inc. ("IEI"), a company that runs the online investigation website bestpeoplesearch.com, will provide detailed call records for the past 100 calls of either a business or residential phone line if the requestor provides the telephone number, name, and address of the account holder. (Attachment A and B are complaints to the Federal Trade Commission concerning this company.) Though IEI specifies 1 to 5 days as necessary to retrieve the records, another data broker, Infonowusa.com offers a 1 to 3 hour turnaround time for detailed cell phone call records. (Attachment C is a list of an additional 40 web sites offering to sell CPNI to third parties.)

These telephone call records are protected as CPNI under the Telecommunications Act, and particularly protected as individually identifiable CPNI (as opposed to aggregate customer information or subscriber list information). These online private investigators do not reveal how they actually obtain this information. However, EPIC is aware of no legal way to reliably and quickly obtain call detail information. Nor does it appear possible for them to reliably obtain this information within the time frames they claim without making misrepresentations (pretexting) to telecommunications carriers or soliciting the carriers to violate the Telecommunications Act.

Additionally, two professional licensed investigators were quoted agreeing with EPIC's assessment in recent media reports:

> [Francie] Koehler, who was part of a project to research online private investigations services, said, "I know that many of them claim to get the information legally. I don't understand how that happens." When she's tried to get someone's phone records via subpoena, she said, "Every time you try, they send the telephone company lawyer in to quash the subpoena."[12]

Washington Post journalist Jonathan Krim quoted Robert Townsend, an advocate of investigator licensure and best practices:

> "I do not know of any legal way to obtain a person's telephonic history," Robert Townsend, head of the National Association of Legal Investigators, said in an interview. Townsend added that he thinks only a small minority of licensed investigators engage in the practice of acquiring and selling the data. [13]

In addition to providing suspiciously fast "turn around times," many also represent that the information provided is "confidential" and not admissible in courts. In some cases, the sites specify that the client must employ a legal method, such as a subpoena, for obtaining the same data if the client wants to use the information in court. These practices suggest that no official process is being employed to obtain the records legally.

It also appears that these violations are occurring at an alarming rate. The cost building the infrastructure to offer call record data is substantial, yet many companies offer to sell this data. These companies must maintain a website, have contacts with investigators in many states, and process transactions quickly (some as quickly as 1-2 hours). There is a risk that there will be no "hit," resulting in the online data broker performing services without compensation. Many sites offer this service through "sponsored links" on popular search

engines and other forms of online advertising, further adding to the cost of offering the data. Combined, these factors and the large number of entities offering call records online suggests that many individuals' phone records are being illegally access and sold every day to simply cover the cost of doing business.

Telecommunications carriers are the primary source of CPNI; therefore, they should be the first line of defense against these practices of illegitimately accessing and selling CPNI. Through Section 222, Congress specifically placed the burden of protecting CPNI in their hands.[14] The Commission has recognized the importance of CPNI security, particularly with regards to the requirements for customer notification in releasing such information to allowed parties under Section 222. It is therefore alarming that these online data brokers are gaining access to these call records without the customers' consent or even knowledge. Regardless of how illegitimate the practices of the online data brokers may be, they would not be possible were it not for loopholes in the security measures that telecommunications carriers use to verify the identity of the CPNI requestor. Carriers may be contributing to this practice by only requiring a few pieces of easily-obtained biographical information (such as date of birth, mothers maiden name, or the Social Security number) to change the addresses on the phone records or requesting call history data. This type of biographical information can be easily obtained by a third party through public records and used to gain access to CPNI. Many different websites have millions of records on date of birth. And online data brokers often have access to other databases to purchase Social Security numbers or dossiers that would contain the mother's maiden name.

IV. The prevalence of this practice poses a significant privacy and security risk for telecommunications customers.

Individuals are likely to suffer injury as a result of these ongoing practices of selling CPNI. The release of such information without a customer's knowledge can lead to devastating results and create serious consequences in the area of personal privacy. With the advent of cellular phones, call records contain some of the most sensitive and private information an individual may have. Phone records can be used to track an individual's daily habits, to spy on a person's communications with others, or to stalk another person. We are also aware of data brokers who offer location tracking services for wireless phone users, even though this information, under Section 222(d), is only supposed to be used for authorized emergency purposes (See services of CSI, Attachment C).[15] Furthermore, if online data brokers are acquiring their information by accessing customers' online accounts, they might also have access to the individual's billing address, credit card information, and even their social security number. These pieces of personal information are so often used in security verification for other services that possessing this information would put the online data broker in complete control of the individual's electronic identity.

Individual phone records are not the only ones at risk. Some websites claim to be able to access any phone record with only a phone number, name, and address. Some even boast the ability to provide business telephone records (See Attachment C). Given the prevalence of phones, both wired and wireless, used for business purposes, these services could be (and most likely are being) used for industrial espionage and other illicit business activities. Business phone records yield sensitive information about client lists and contact information, resulting in privacy violations both for the businesses and the people that those

businesses have contacted. While the Commission has tried to balance competition, access, and privacy rights in determining the best method with which to enforce Section 222, the types of privacy violations described here are unauthorized, unwarranted, and serve more to promote security breaches and industrial sabotage than competition.

Furthermore, these business are operating online, and provide these data brokerage services readily at the submission of an Internet form and upon receipt of payment. They do not actually meet their clients and assess the clients' intent in trying to access these records. They have no way of screening out clients who desire access to such phone records for malicious purposes. Therefore, weak security standards may also pose as a security threat to the very customers whose privacy the Commission is striving to protect.

V. The Federal Communications Commission should immediately initiate a rulemaking proceeding to address the CPNI protection measures used by telecommunications carriers and invite comment to develop adequate safeguards for verifying the identity of parties trying to access CPNI.

Given the privacy and security issues at stake in this matter, the Commission should immediately initiate a rulemaking proceeding to investigate the following issues:

1. What security measures telecommunications carriers currently have in place for verifying the identity of people requesting CPNI.
2. What inadequacies currently exist in those measures that allow third parties outside of the realm of Section 222, such as online data brokers and private investigators, to access individual CPNI without the customer's knowledge or authorization.
3. What kind of security measures are warranted to better protect telecommunications customers from unauthorized access to personal and individualized CPNI.

Some forms of security measures that would more adequately protect access to CPNI might include the following:

1. Consumer-set passwords. Currently, there is a reliance on biographic identifiers, such as the Social Security Number and date of birth, to authenticate individuals. These biographic identifiers are inadequate for authentication, because, unlike passwords, they do not change, and they are widely available. A unique and separate password chosen by the account holder at the time of phone activation would greatly increase security of CPNI.
2. Audit trails. Carriers should be under a duty 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. Audit trails deter insiders from selling personal information, and once data is accessed without authorization, audit trails aid in investigating the security breach.
3. Encryption. When stored at the carrier, data should be encrypted. While audit trails help protect against insider abuse, encryption assists in protecting data

from security threats outside the corporation.

4. Notice to affected individuals and the Commission when there is a security breach. In many other sectors, companies must notify individuals if a security breach results in their personal information being accessed by an unauthorized person. This allows individuals to mitigate harm from the breach, and assists in the public in understanding whether data are actually secure.
5. Limiting Data retention. Call detail records should be deleted after they are no longer needed for billing or dispute purposes. Alternatively, carriers should be required to deidentify records, that is, divorce identification data from the transactional records. This will allow carriers to maintain call records for data analysis, but reduce the risk that the same records will be associated with an account holder and used to invade privacy.

Respectfully Submitted,

Chris Jay Hoofnagle
Senior Counsel
August 30, 2005

---

[1] 47 U.S.C. § 222 *et. seq.*

[2] *See, e.g.,* Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 F.C.C. Rcd 14860 (July 25, 2002).

[3] Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, Washington Post, Jul. 8, 2005, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862_pf.html.

[4] *See*Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 F.C.C. Rcd 14860, 14862 (2002).

[5] 47 U.S.C. 222(c).

[6] 47 U.S.C. § 222(c)(1).

[7] Section 222(f)(1) of the Telecommunications Act defines CPNI as follows:

> (A) Information that relates to the quantity, technical configuration, type, destination, and amount of use in a telecommunications service subscribed to by an customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of its carrier-customer relationship; and
> (B) Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

[8] *See, e.g.,*Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 F.C.C. Rcd 14860, 14862 (2002).

[9] *Id.*

[10] *See* 47 U.S.C. 222(h) (providing specific definitions of each category of information).

[11] 47 U.S.C. § 222(d).

[12] Susan Kuchinskas, *EPIC Fighting Online Phone Record Sales*, InternetNews, July 8, 2005, available at http://www.internetnews.com/ent-news/article.php/3518851.

[13] Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, Washington Post, Jul. 8, 2005, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862_pf.html.

[14] *See* 47 U.S.C. § 222(c)(1).

[15] Section 222(d)(4) of the Telecommunications Act provides that the location of a cellular phone should only be revealed in the following instances:

> (A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;
> (B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or
> (C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.
