

Understanding and Complying with CPNI Rules

**Tom Karalis
Fred Williamson & Associates, Inc.**

Brief History of CPNI

September 2001

The FCC issues their initial Order regarding CPNI rules, which permits carriers to rely on an "opt-out" means to secure customer approval in regards to using CPNI for marketing.

July 2002

This Order included a provision for carriers to release customer information to third parties (with opt-in customer approval).

August 2005

A few months after the infamous HP Scandal rocked the media, *EPIC files their Petition that starts the CPNI movement. This Petition, lamenting the liberal rules governing consumer protection, forces the FCC to take action.

**Electronic Privacy Information Center – consumer group*

February 2006

The FCC releases an NPRM, requesting Comments on what steps can be taken to ensure the security of customer information.

April 2, 2007

The FCC issues the Final Order regulating access to CPNI records. At the same time, the FCC releases a FNPRM seeking Comments on whether it should expand its rules to protect privacy even more.

FCC Order #96-115

July 9, 2007

32 Comments are filed - of which only 2 filings support the notion of expanding the existing CPNI rules to include:

- Password Protection for *Non-CPNI* information
- Audit Trails
- Physical Safeguards
- Limiting Data Retention
- Information Stored in Cellular Devices

So What Exactly Is CPNI?

A simplified CPNI definition of Section 222 of the 1996 Act is:

“The data collected by a telecommunications provider regarding the telephone calls made by a consumer”

CPNI Make-Up

CPNI is comprised of 3 categories:

Call Detail Records / Call Information

- In-depth information about every call a customer makes
 - Time
 - Date
 - Number called
 - Duration of call
- Requires the greatest protection of privacy
- Most often leaked information to Data Brokers
- Most often fined violation by the FCC - \$100K+

CPNI Make-Up *(continued)*

Subscribership

- Services a Customer Subscribes to:
 - IPTV
 - Long Distance
 - Broadband, etc.
- Often used to market other services without a customer's permission – practiced shunned by the FCC.

General Account Information

- Name / Address / Phone Number / Personal Information (maiden name, SS#, etc), *Bill amount (\$\$)
- Least protected information

Different Kinds of CPNI?

We can classify CPNI into 2 categories:

- Call Detail CPNI
- Non-Call Detail CPNI

Call Detail CPNI includes:

- Time of call
- Date of call
- Duration of call
- Destination number of each call
- The type of services a consumer subscribes to
- Any additional Call Detail information that appears on the phone bill.

This category is strongly monitored and protected by the FCC & LEAs

Non-Call Detail CPNI

Non-Call Detail CPNI

Compared to

Call Detail CPNI

- | | | |
|--------------------------|--|-----------------------|
| ◦ Name | | ◦ Time of call |
| ◦ Address | | ◦ Date of call |
| ◦ Phone Number | | ◦ Duration of call |
| ◦ * Bill Amount (\$\$) | | ◦ Destination number |
| ◦ Social Security Number | | ◦ Consumer's services |

This Non-Call Detail CPNI information, though considered private by our standards, does not fall under the FCC's guidelines regarding Call Detail CPNI. It does not have the stringent guidelines and security concerns, probably because it can be found on the Internet if you know where to look.

What Does CPNI Do?

Protects the Customer's Privacy

- ✓ By restricting unauthorized access to private information.
- ✓ By verifying picture / Government issued IDs
- ✓ By Calling the Consumer @ their Telco-issued Telephone #
- ✓ By asking Security Questions if Password is forgotten.

What Does CPNI Do? *(continued)*

Allows the Marketing of Products

- ✓ With prior Customer approval, information can be sent to 3rd Party Vendors so as to allow consumers a greater choice of products for their home or business.
- ✓ As long as a customer has Opted-In, a CSRs can market additional services that a customer does not currently subscribe to.
- ✓ With Opt-In approval, Telco can mail out flyers, newsletters, bill inserts promoting the new offerings / savings for consumer.
- ✓ A well trained CSR can find a way to promote their service offerings when a customers calls about another issue...

Acceptable CPNI Marketing Practices

- **Directory Creation – *Name / Address / Phone #***
- **Law Enforcement Assistance – *Assist in Ongoing Investigations / Breaches***
- **Providing Customer Protection – *IDs / Security questions / Verifications***
- **Providing Company Protection – *Implementation of Company CPNI Rules***
- **Exchanging of information for billing purposes – *Telco Affiliates***
- **Marketing of additional services as requested or approved by customer – *Bill Inserts, Newsletters, Direct Mail, etc. (with customer opt-in approval)***
- **Marketing of additional services – *From 3rd Party Providers or Joint Venture Partners (with prior written approval)***

*Unacceptable CPNI Practices

- Releasing CPNI information – *Without Customer Verification or Password.*
- Providing / Selling CPNI information – *To Telemarketers or Data Brokers.*
- Distributing CPNI information to 3rd Party Vendors or Joint Venture Partners – *Without Prior Customer Approval.*
- Using a Competitor's CPNI Information – *To Win Back Customers That Were Previously Yours.*
- Mass Marketing – *w/o Providing the Consumer an Opt-Out Opportunity.*
- Using CPNI Information – *To Push Additional Services that Were Never Requested / Inquired About...*

**These violations will incur the wrath of the FCC with heavy fines...*

The FCC Does Not Allow...

- ...the use of CPNI Information to Target other customers.

One cannot use the billing information of a company to lure their customers to your company.

- ...the use of CPNI Information to Be shared with other companies.

One cannot pass on customer information to their affiliates (3rd Party) w/o prior customer approval.

- ...the use of CPNI Information to Get back a customer lost to another provider.

One cannot lure another company's customer by promising them a better rate.

The FCC Does Not Allow: *(continued)*

- ...the use of CPNI Information to Include a customer on mailing lists, newsletters, or mass marketing campaigns.

One cannot add a customer to a mailing list when that customer has opted out.

- ...the use of CPNI Information to Market additional services when a customer calls about another service he subscribes to.

One cannot talk about offering a DSL package when the customer called about his Long Distance bill...

What is a Breach / Facts & Figures

Personal information (on a disk, paper, electronic equipment) that is stolen or ends up in unauthorized hands.

Types of Breaches

- Lost or stolen laptop / computer equipment / CDs
- Hackers breaking into system
- Employees stealing customer information
- Information disposed of improperly

Cost of a Breach

- 2006: Average cost \$90 - \$120 per record
- 2007: Average cost \$197 per record

Breach Data:

2005: 158 Breaches affecting more than 68M people

2006: 315 Breaches affecting more than 20M people

2007: 448 Breaches exposing more than 127M records

2008: 449 Breaches exposing over 22M records (as of September)

3 Recent and Infamous Breaches

Charter Communications - Cable Provider - July 2008

- Laptops were stolen from the Greenville, NC location that housed over 9000 employees' personal information.

AT&T – Telecommunications - May 2008

- A laptop with information on 113,000 AT&T employees was stolen. Information included SS#, salaries and bonuses.

TJ Maxx – Retailer - December 2007

- 45M Credit & Debit Card records were stolen.
- Thieves encrypted the data so that TJX + LEAs could not access the info!
- Data stolen from TJX surfaced at Wal-Mart stores in Florida
- Used to help steal about \$8 million in merchandise from Wal-Mart stores.
- The thieves used the stolen TJX customer data to create dummy credit cards for purchasing Wal-Mart and Sam's Club gift cards, and then used those to hit stores in 50 of Florida's 67 counties.
- U.S. Secret Service advised TJX officials that disclosure of the suspected intrusion might impede their criminal investigation and requested that the company keep a lid on the incident until law enforcement gave them the green light to announce the breach.
- The company disclosed the breach on Jan. 17
- TJX believes it "may never be able to identify all of the stolen information.

Information Week - March 2007

How To Avoid the Previous Fiascos...

Implementing the following steps would assure a Telco's compliance with the FCC regarding CPNI and avoid any MAJOR headaches...

Provide training for all employees regarding CPNI Rules

- All employees must receive yearly CPNI Training Sessions
- All employees should sign a * Company Waiver stating their knowledge & Compliance with the Company's CPNI Policies
- Apply CPNI rules to every customer that calls in regarding access to their account
- Know when to apply CPNI rules and what to do if a breach occurs

*FWA Client recommendation

Complying With the FCC's CPNI Rules *(continued)*

Implement Company disciplinary measures for employee violations of Company CPNI procedures.

- Establish disciplinary procedures for CPNI violations – In severe cases, up to employment termination...
 - Retrain employee(s) after CPNI violation
 - Disciplinary actions must be in line with violation
 - *Document the violation and include in yearly filing...
- ★ Always discuss any incident with your Manager before contacting the FCC or LEAs

Complying With the FCC's CPNI Rules *(continued)*

Designation of Compliance Officer + Responsibilities

- Point of contact for all employees regarding Telco's CPNI procedures
- Assures all employees have attended training classes and have signed Company CPNI Waiver
- Reports to General Manager / Senior Management
- Tracks all CPNI violations + outcomes
- Assists LEA Officers if breach occurs
- Reviews and updates CPNI manual for employees
- Attends yearly CPNI training

Complying With the FCC's CPNI Rules *(continued)*

Company Requirements for CSR Reps

- Creation of password for all customers
- Verify customer after password implementation
- Create back-up question(s) for forgotten password
- Document every CPNI transaction
- Keep CPNI records for 2 years
- Inform customer that the CPNI procedures are for their protection
- Inform customer of password, address or account information change.

Complying With the FCC's CPNI Rules *(continued)*

Law Enforcement Notification Procedures

- Must notify LEAs by email within 7 days of breach discovery
- Obtain LEA approval BEFORE notifying customer – unless irreparable harm is possible for customer – then ask LEA permission to contact customer and report breach.
- Document all information regarding breach and keep records for 2 years
- Be available for all FBI, Secret Service + FCC questioning.
- Don't Crack under the pressure of LEA / FCC questioning!!!

Complying With the FCC's CPNI Rules *(continued)*

Annual CPNI Certification

Annual Filing MUST include:

- Details of established company procedures
- Company Officer signature
- Data regarding CPNI breaches
- Data regarding CPNI customer complaints
- Must be filed in FCC Docket #06-36 by March 1st of following year.
- Keep Copies in Company Files Dating Back to 2001

New Requirements on the Horizon?

Consumer Groups (NASUCA, NJ Rate Council, etc) are lobbying the FCC for more stringent requirements for Carriers regarding CPNI. Some of those regulations would include:

Password Protection

A further mandate for use of passwords in the provision of *non-call detail CPNI* and account changes. The cost and time spent would be enormous and wasteful to say the least...

Audit Trails

Documented by rural carriers to track customer contact. Keeping records of disclosure of *non-CPNI information* and of all customer contact would be fruitless and expensive. Recordkeeping does not protect CPNI. Audit trails do not prevent unlawful disclosure. The benefit to law enforcement is speculative and the cost to carriers would be prohibitive.

New Requirements on the Horizon? *continued*

Limiting Data Retention

The length of time carriers retain customer records. This issue should remain at the carrier's discretion, not limited by federal mandate.

Physical Safeguards

Rules governing physical transfer of CPNI among companies authorized to access or maintain CPNI. Physical safeguards should be left to the companies, including their chosen methods of encryption. It is in their interest to protect the material. Mandated forms of security would simply invite pretexters to anticipate and defeat the security system.

New Requirements on the Horizon? *continued*

Protection of Information Stored in Cellular Devices

Carriers' requirement to erase a customer's personal information. This requirement should not fall on the carrier's shoulders. Customers should follow instructions from the manufacturer of the device. The customer thereby avoids the circumstance of other parties having access to the information before erasing it, and carriers avoid the risk of false accusations of misuse. The easier manufacturers make it for customers to permanently erase information, the better. Users would benefit from not having to be dependent upon the honesty and expertise of another entity to erase the data.

What Does The Future Hold?

The FCC will review all Annual Certifications that were filed and will investigate any breaches that were documented.

Possibly (within the next 6 months) expect a Public Notice - asking the Industry for Comments – Are additional safeguards required for CPNI protection?

EPIC, NASUCA and other Consumer groups will push the FCC to administer more regulation and stiffer penalties regarding CPNI violations.

What Can We Do?

- Continue to provide our Customers with the Privacy & Protection they expect from us
- Adhere to all FCC & Company rules regarding CPNI
- Industry will decide whether additional regulations will be required or are we “OK” with the status quo.
- Important to file Comments / Reply Comments to voice our position regarding additional CPNI regulations.
- If we don't voice our preferences as to which way we want to go, others (consumer groups, etc.) will decide for us...

Questions?

Thank you

Tom Karalis

FWA, Inc.

918.298.1618

tkaralis@fwainc.com