



Tim Owens
Cronin Communications
202-232-1107

[towens@cronincom.co](mailto:towens@cronincom.com)

[m](#)

©2007 Cronin Communications

About Cronin Com

- Small independent consulting firm.
- Works with rural telcos across the United States.
- Conducts market feasibility studies for business expansion.
- Provides regulatory, operations and business planning services.
- Conducts statewide studies for South Dakota.





Agenda

1. *History of CPNI*
2. *Terms & Definitions*
3. *Changes to CPNI Policy*
4. *Restricted CPNI*
5. *Acceptable CPNI*
6. *Opt In / Opt Out*
7. *CPNI Compliance*
8. *FCC Enforcement*
9. *Marketing Around CPNI*

History of CPNI

CPNI History

- **Telecommunications Act**
 - Requires telecom carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure.
- **Privacy Groups**
 - Filings by the Electronic Information Privacy Center (EPIC) and others urging greater restrictions.
- **Competition**
 - Intended to prevent carriers from gaining a advantage over competitors.

CPNI History

- **1996.** The Telecommunications Act required carriers to protect customers' privacy.
- **1998.** The FCC required customers to "opt-in" to marketing programs for personal information contained in their CPNI to be shared or used for marketing purposes.
- **U.S. West** challenged the FCC rule, arguing for an opt-out approach. The court found that the FCC had failed to provide adequate evidence to establish the rule furthered a substantial government interest, that it materially advanced such an interest, and that it was narrowly tailored to serve that interest.

CPNI History

- **September 2001.** The FCC issued a clarification of their initial order, permitting carriers to rely on "opt-out" means to secure customer approval to use their CPNI for marketing as an interim measure.
- **July 2002.** The FCC officially adopted rules providing for opt-in customer approval for carriers' release of customer information to third parties, but permitting opt-out consent for release of information to affiliated parties.

CPNI History

- **August 2005.** EPIC urged the FCC to require security measures to protect access to CPNI from pretexters and other unauthorized parties.
- **April 2007.** The FCC issued a final order regulating access to CPNI records. At the same time, the FCC released a further notice of proposed rulemaking, seeking comments on whether it should expand its rules to protect privacy even more. Comments were due July 9, 2007, and reply comments are due August 7, 2007.

CPNI History

If a telco knew that a customer was ordering DSL, but not getting Long Distance, it could market its LD service over its competitors. The FCC concluded that this was anticompetitive.

CPNI History

More than 53 million customers have been the victims of pretexting schemes, whereby impersonators gain access to their telephone records, simply claiming to be the customer. Imagine a private investigator hired to spy on an ex-spouse.

CPNI History

Customers are bombarded with direct mail and spam to the point of harassment. CPNI restricts telcos from selling, trading and distributing customer account information to third parties.

CPNI History

Main Sources of Confusion:

- 1. What constitutes “customer approval?”*
- 2. Opt-in / Opt-out – when do they apply?*
- 3. What’s an existing customer relationship?*
- 4. What is targeted marketing vs. mass marketing?*
- 5. What’s a third party, joint-venture partner or independent contractor?*

The Gist of CPNI

- Protect the customer's privacy.
- Market products and services within the existing customer relationship.
- Do not use customer information to *target* customers for a product or service *outside* the existing customer relationship.
- Do not give customer information to other companies.

Types of CPNI

- Call Detail Records.
 - Require greatest protection of privacy.
- Purchases.
 - LD PICC, video, Internet, wireless, features.
- General account information.
 - Name, address.

Terms & Definitions

- ***Address of Record.*** An address, whether postal or electronic, that the carrier has associated with the customer's account for at least 30 days.
- ***Breach.*** A security violation occurring when a person without authorization, or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.
- ***Call Detail Records (CDRs).*** Any information that pertains to specific telephone calls, both inbound and outbound, including number called, number from which calls are received, time, location, and duration.

- ***Customer Authentication.*** Confirmation of the customer's identity, using *not-readily-available* biographical information.
- ***Customer Premise Equipment (CPE).*** Consumer electronics that connect to or function with communications and data services, such as handsets, fax machines, set-top boxes, modems, etc.
- ***Existing Customer Relationship.*** Established business relationship between the company and customer, based on the provisioning of services requested by the customer.

- ***Independent Contractor.*** A third-party company with which the telco does business.
- ***Interconnected Voice Over Internet Protocol.*** A data service that allows customers to originate and terminate phone calls over a VoIP or partial-VoIP network.
- ***Joint-venture Partner.*** A company with which the telco may be invested in ownership of a subsidiary or other third-party business.

- **Opt In.** Express written consent to receive marketing materials and sales communications about products and services *outside* the existing customer relationship, or express written consent to share customer information with third parties, joint-venture partners and independent contractors. .
- **Opt Out.** Express written consent to be *excluded* from marketing materials and sales communications about products and services *outside* the existing customer relationship.
- **Password Protection.** Establishment of a customer password to access and receive call detail records and information.

- ***Pretexting.*** Fraudulent impersonation of a customer to gain information about the customer's calls or account.
- ***Readily Available Biographic Information.*** Information about a customer that can be easily obtained by a pretexter or other party, such as address, place of birth, place of employment, etc.
- ***Section 222.*** The part of the Telecommunications Act of 1996, requiring carriers to protect customer proprietary network information. Amended several times.

- ***Telephone Number of Record.*** The telephone number associated with the underlying service, *not* a number supplied as a customer’s “contact information.”
- ***Valid Photo ID.*** A government-issued means of personal identification with a photograph, such as a driver’s license, passport, or comparable ID that is not expired.
- ***Other?***

Changes to CPNI Policy

Changes to CPNI

On April 7, 2007, the FCC adopted rules changing or adding the following:

1. Carrier Authentication Requirements.
2. Inclusion of Telephone Numbers From Which Calls Are Received.
3. Notice to Customers of Account Changes.
4. Notice of Unauthorized Disclosure of CPNI.
5. Joint Venture and Independent Contractor Use of CPNI.
6. Annual CPNI Certification
7. Inclusion of Interconnected VoIP providers.
8. Enforcement Proceedings.
9. Business Customer Exemptions.

1. Carrier Authentication

- Concerns Call Detail Records *only*.
- Requires the customer to establish and use a password to receive Call Detail Records, whether during a customer-initiated call, or on-line.
- If the customer does not supply the password, CDRs may be:
 - Sent to the address of record (email or postal).
 - Provided in a return call to the telephone number of record.
 - Provided in person upon presentation of a valid photo ID.
- Carriers may confirm CDRs supplied by the customer.

Password?

How to establish a password:

- Call the customer at the telephone number of record, or
- Authenticate the customer ***without the use of readily available biographical information or account information.***
- Have the customer select a password and establish a back-up question.
- Store the password with the customer's account.
- Provide on-line option for on-line billing, if applicable.
- You've already got passwords? No need to start over.

Password?

The carrier decides its own authentication process (open for FCC comment). Examples of information that is not readily available:

- Last four digits of the social security number.
- Mother's maiden name.
- Childhood pet.
- Services on the account.
- Other names listed on the account.
- Last PPV rented.
- Childhood street name.
- Credit information supplied for the credit check.

***Examples of readily available information that
should
not be used for authentication:***

- Phone number.
- Address.
- Previous address.
- Spouses name.
- Schools, universities.
- Cars / license plate numbers.
- Mortgage information.

Authentication Recommendation

- Call the customer at the telephone number of record.
- Ask for a password of 4-12 digits containing letters and numbers.
- Ask for two back-up questions to be used as reminders: last four digits of the social security number and mother's maiden name or childhood pet.

If the customer is not available at the telephone number of record, the authentication questions above can be used to establish a password, but also ask the customer to describe the features on their account.

2. Calling From Information

*Call Detail Records now include information about calls **received**, including time, date, duration and number calling.*

3. Notification of Account Change

- Password change.
- Address of record change.
- New address of record created.
- Lost or forgotten password.
- On-line account creation.
- On-line account change.
- Basically any new or changed information.

Customers must be notified “immediately.”

4. Notice of Unauthorized Disclosure

- CPNI Breach:
 - Customer account information is stolen.
 - CDRs are provided without authentication.
 - A pretext is attempted.
 - Databases are hacked.
- Questionable breach:
 - CPNI is sold or distributed to a third party without customer approval.
 - CPNI is used by a joint venture partner or independent contractor without customer approval.

4. Notice of Unauthorized Disclosure

- Notify law enforcement within seven days.
- Notify the customer within seven days.
- Exceptions to notification when requested by law enforcement.

Although a rules violation, it's probably not a breach when a CSR mentions a product or service outside an existing customer relationship, or when a marketing director sends a targeted mailing without opt-out notification.

***The Breach Test:
Does it require notification of law
enforcement?***

5. Joint Venture / Independent Contractors

- Opt-in now required before joint-venture partners and ***independent contractors*** can use CPNI.
- This affects giant telecom providers that use data brokers and outside firms to implement marketing campaigns, not so much the small independents.

Why Bother?

6. Annual Certification

- Already required.
- Amended to include:
 - Summary of customer complaints.
 - Actions taken against data brokers.

7. Inclusion of Interconnected VoIP Providers

- Retail VoIP providers are now classified as “carriers” for the purposes of CPNI rules.

8. Enforcement Proceedings

- Carriers are further required to take reasonable measures to discover and protect against pretexting.
- In enforcement proceedings, evidence of the precautions taken will be considered.
- Precautions and reasonable measures are not currently defined and open for comment.

9. Business Customer Exemptions

- Carriers may bind themselves contractually to authentication regimes other than those adopted in the FCC order. For example, a business might have a dedicated account representative with whom the carrier shares CPNI.

Acceptable CPNI

Acceptable CPNI

- Exchange of customer information for the purpose of inter-carrier billing.
- Marketing of services within an existing customer relationship.
- Mass marketing:
 - Bill notices
 - Bill inserts
 - Direct Mail
 - In-house telemarketing
 - Newsletter articles
 - Advertising
 - Signage

Acceptable CPNI

- Law enforcement.
- Directory listings.
- Service provisioning by independent contractors.
- In-house mailings.
- Provisioning of customer service.
- Provisioning of products and services.
- Protecting telco property.

Restricted CPNI

Restricted Use of CPNI

- Selling or distributing CPNI to a third party without customer approval.
- Selling or distributing CPNI to a joint-venture partner or independent contractor without the customer's express permission (opt-in).
- Win-back campaigns that use information about a customer's relationship with a competitor to target that customer.
- Targeted marketing without giving the customer an opt-out opportunity.
- Discussing Call Detail Records without password authentication.

Restricted CPNI

- Providing CPNI to mail houses, telemarketers or direct marketing firms (data brokers).

Opt In / Opt Out

Opt-In

Required for:

- Distribution of CPNI to a third-party.
- Use of CPNI in a joint-venture partnership or independent contractor relationship.
- Distribution of CPNI to a joint-venture partner or independent contractor.

Opt-In Process

- Mail a form to all customers requesting signature approval to share CPNI with third-parties, joint-venture partners and independent contractors.
- Receive signed approval back from customers.
- Notate opt-in approval in company billing records.
- Secure and store approval in company's CPNI files.
- Return rate will be less than 5%.

Recommendation: DON'T DO IT.

Opt-Out

Good for two years.

- *Required for **targeted** marketing of products and services **outside** the existing customer relationship.*
Example:

Mailing to all local customers without the telco's LD.

Opt-Out Process

- Mail a form to all customers notifying them that “from time-to-time the company may use your account information to promote additional products and services available from us.”
- Provide the customer the option of “opting out” by signing and returning the opt-out form.
- Allow 32 days to receive opt-out forms.
- Notate in the customer records each opt-out.
- Screen opt-outs from all future *targeted* marketing.
- Secure and store opt-out requests in the companies’ CPNI files.

Opt-Out Process

Again, why bother?

You might want to promote products and services outside the existing customer relationship and use targeted marketing campaigns for efficiency.

Opt-In and Opt-Out Require

- Easy-to-understand language.
- No misleading language.
- Easy-to-read type.
- Easily discernible packaging.
- Full translation, if any of the copy is translated into another language than English.
- Entities that will receive CPNI.
- Purposes for which CPNI will be used.
- Contact information.

Simple Solution

Send everything to everybody.

Neither Opt-In, Nor Opt-Out

Nothing is needed for:

- Direct mass mailings / mass email
- In-house telemarketing
- Customer research
- Advertising
- Signage
- Bill inserts
- Bill memos
- Newsletter articles

What's An Existing Customer Relationship?

The customer already buys something from you.

- Local voice and all related services.
- Long distance and all related services.
- Wireless and all related services.
- Video and all related services.
- DSL and all related services.
- Wireless broadband and all related services.
- Bundles and all related services.

Plus CPE for each.

CPNI Compliance

7 Steps to Compliance

1. Designate a compliance officer.
2. Train and certify employees on CPNI requirements.
3. Notify customers of any account changes.
4. Notify law enforcement *and customers* of any unauthorized disclosure of CPNI.
5. Establish disciplinary procedures for employee violations of CPNI rules.
6. Take measures to discover and protect against pretexting and unauthorized disclosures of CPNI.
7. File annual certification by March 1.

Employee CPNI Manual

Employee Manual Outline

1. Definition of CPNI.
2. Customer authentication and password protection procedures.
3. Restrictions on CPNI.
4. Acceptable uses of CPNI.
5. Reporting procedures for CPNI violations and breaches.
6. Opt-in and Opt-out forms.
7. Name and contact information of the CPNI Compliance Officer.
8. Employee disciplinary procedures.
9. Section 222 of the 1996 Telecom Act.
10. FCC CPNI Rules.

FCC Enforcement

Enforcement

- When investigating breaches and complaints, the FCC:
- Requires the carrier to prove that it has taken reasonable precautions to prevent unauthorized disclosure of CPNI.
- Prove that policies and procedures were followed, especially in the instance of pretexting.
- Sanctioning and forfeiture might follow.
- Carriers are *not* immune for consumer lawsuits for CPNI violations and breaches, even if they can show that policies and procedures were followed.

Common Violations

- Not assigning a Compliance Officer.
- Not maintaining records.
- Not training and certifying employees.
- Not filing annual certification.
- Not vetting marketing campaigns with the Compliance Officer.
- Not getting password authorization to review CDRs.
- Not authenticating customers for other account questions.
- Targeted mailings.
- Sharing of CPNI with independent contractors.

Example Fines

- March 2007. **\$4,0000**
 - PhonceCo, LP
 - Manning Municipal Communications
 - Habla Communications
 - Connect Paging
 - Burke's Garden Telephone Company
 - First United Telecom

Example Fines

- March 2007. **\$100,000.**
 - Priority One Telecom
 - Shoreham Telephone Company
 - CTC Communications
 - Easterbrooke Cellular
 - Am’p Mobile

Example Fines

- August 2006. **\$100,000**
 - AllTel
- July 2006. **\$550,000**
 - AT&T

Plus Various Citations

Marketing Around CPNI

***Primarily impacts customer service, sales,
marketing and install & repair staff.***

CPNI in Everyday Operations

CSRs. (Five things to remember)

1. Authenticate **every** customer.
2. Require a password for CDRs.
3. Check opt-out status.
4. Ask permission to discuss products and services.
5. Aggressively upsell.

Safety Net for CSRs

- Authenticate the customer.

“To protect your privacy, may I confirm that I am speaking to Mr. Jones? Could you please provide the last four-digits of your social security number?”

- Ask permission to review the customer’s account information and discuss additional products and services.

“May I have permission to review your account and discuss services you might not currently be receiving from us?”

Safety Net for CSRs

- For CDRs, a password must be established (see “Establishing a Password”) and provided, or the customer must be called back at the address of record, have the information sent to the address of record, provide a photo ID in person, or provide the call detail information for confirmation.

“To protect your privacy, may I please have your password in order to provide you with that information?”

Upselling Examples

“I see that you have caller ID. Did you know that with voice mail and call waiting, you can see who’s calling when you’re on the line, and let it ring to voice mail?”

“Would like to add a premium channel to your order?”

“I notice that you’re using dial-up Internet, have you heard about our specials on DSL?”

“As one of our triple play customers, you’re eligible to receive voice mail, high-def television and faster Internet for the same price.”

Install & Repair

Two things to remember:

1. Sell within existing customer relationship.
2. Or, ask permission to discuss additional products and services.

Install & Repair Sales Examples

“While I’m installing your new video service, would you like to add HD, DVR or a premium channel?”

“Now that you’re a triple play customer, would you like any additional calling features, such as voice mail or caller ID?”

“You can avoid future repair costs on inside wiring with Wireline Maintenance.”

“I know I’m here to repair your phone service, but may I tell you about some new services we offer?”

Marketing and CPNI

Marketing managers have it toughest.

Five items to remember:

1. Forget about Opt-IN. It's not worth it. Simply do not share CPNI with anyone outside the company.
2. Vet all marketing efforts with the CPNI compliance officer.
3. Conduct as much mass marketing as possible.
4. Avoid targeted mailings.
5. When targeting, observe the rules.

Marketing Efforts

- Media.
 - Newspaper, radio and television ads - OK.
 - Signage, banners, kiosks, displays, billboards – OK.
- Direct mail.
 - Names and addresses of customers are not considered CPNI. OK to share with independent contractors (OPINION).
 - Safety net: acquire address labels through data firms.

Marketing Efforts

- Telemarketing:
 - If conducted in-house, it requires no sharing of CPNI with a third party or independent contractor.
 - Do not give target telephone numbers to independent telemarketing firms.
 - OK to give all phone numbers to telemarketing firms (OPINION).

Marketing Efforts

- Winbacks
 - OK to generate a list of disconnected customers and attempt to win-back. Best done in-house.
 - Not OK to use port requests or cancellation codes to target competitors' customers.

Marketing Efforts

- Websites
 - General information on the website is not targeted and is OK.
 - Account information must be password protected.

Q&A?

Tim Owens

202-232-1107

towens@cronincom.com