Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2016 covering the prior calendar year 2015

1. Date filed: February 16, 2016
2. Name of companies covered by this certification: Harron Communications LP, and its affiliates listed below
3. Form 499 Filer IDs:

MetroCast Cablevision of New Hampshire, LLC	826744
MetroCast Communications of Connecticut, LLC	827638
MetroCast Communications of Mississippi, LLC	826516
Gans Communications, LP	827893

4. Name of signatory: Steven Murdough
5. Title of signatory: Senior Vice President of Operations
6. Certification:

I, Steven Murdough, certify that I am Senior Vice President of Operations and thereby an officer of Harron Communications LP, and that I am also Senior Vice President of Operations and thereby an officer of each of its affiliates listed above. Acting as an agent of each of these companies (collectively, "Harron"), I certify that I have personal knowledge that Harron has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the customer proprietary network information ("CPNI") rules as set forth in Part 64, Subpart U of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how Harron's procedures ensure that the it in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

During 2015, Harron divested all of the cable systems that were owned by its affiliates, MetroCast Communications of Connecticut, LLC and MetroCast Communications of Mississippi, LLC. Therefore, this certification will be the final CPNI report on behalf of those two entities.

Harron has not received any customer complaints in the past calendar year concerning unauthorized release of CPNI. Harron does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. Harron has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed with either state commissions, the court system, or the Commission.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the

Commission are punishable under Title 18 of the U.S. Code and may subject Harron to enforcement actions.

Steven Murdough
Senior Vice President of Operations
Harron Communications LP
Executed February 16, 2016

CPNI Compliance Procedures

The following statement is provided pursuant to 47 U.S.C. §64.2009(e) to explain how the operating procedures of Harron Communications ensure compliance with the applicable rules affecting use of customer proprietary network information ("CPNI"). CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the 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."

Harron Communications' policies and procedures to meet the CPNI rules include:

Use, Disclosure of, and Access to CPNI:

- Harron may use, disclose, or permit access to CPNI without customer approval in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of Harron, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to market services within the category or categories of services to which the customer already subscribes; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

- Except as provided above, Harron does not use CPNI for marketing. In the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process. If such use is approved, Harron shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

- Harron does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

- When Harron receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

Company-Wide Training:

- All employees with access to CPNI must complete a CPNI training course prior to accessing CPNI and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. Harron continually tracks employee compliance. Training for customer service representatives emphasizes, among other points, that they be

cognizant that some unauthorized persons may have significant apparent familiarity with a customer's biographical and account information.

- Managers and customer service representatives renew confidentiality training on an annual basis.

- Managers monitor and coach employees on maintaining customer confidentiality.

- Employees must sign an acknowledgement that they have been advised of and understand the importance of customer privacy every time they receive training involving confidentiality issues.

Account Protections:

- Customers are required to establish account passwords upon account activation. Customers are advised not to use as their password a portion of their social security number, telephone number, street address, date of birth, or a string of the same four numbers (i.e., 1111).

- Customers are required to provide their account passwords before access to CPNI is granted, or, in the case of customers who request access in person at a Harron location, are required to present valid, non-expired, government-issued photo identification.

- Customers who are unable to supply a correct password are permitted to access their CPNI only by a return telephone call made to the telephone number on the account of record.

- Harron notifies customer immediately by voicemail to the telephone number or by mail to the address of record whenever a password, online account, or address of record is created or changed. These notifications are not required when the customer initiates service. The notification does not reveal the changed information.

- Employees must use passwords to access any Harron system where CPNI is stored.

- Computerized backup of data are kept off-site in the hands of a bonded and reputable business specialized in maintaining confidential data. Any paper documents are converted to electronic facsimiles and stored in the same manner. Originals of paper documents are then shredded.

Marketing Safeguards:

- Harron does not use CPNI information in any sales or marketing campaigns.

- Harron has a supervisory review process to ensure compliance with CPNI restrictions when conducting outbound marketing, including review of all direct marketing by the Marketing Manager who receives CPNI training.

- The Marketing Manager has safeguards to prevent cross-product information sharing that would be in violation of CPNI rules.

- Harron does not sell customer lists to third parties.

Customer Service Safeguards:

- Customers must verify their personal account information before an employee can provide comments or take requests for any changes to an account. At a minimum, customers must provide their name, address and a password of their choice.

- Detailed customer call detail records, which are considered particularly confidential, are accessible only by employees or agents with a need to know and are provided to customers only after receipt of the customer's password or, in the case of a request made in person at a Harron retail location, after the customer presents valid, non-expired, government issued photo identification. If a customer is unable to supply the password or valid identification, as appropriate, call detail records are not disclosed.

- Customers are permitted to access their online accounts only after supplying their account password.

- Customer service representative interactions with customers are monitored, and the monitoring includes evaluation of compliance with privacy requirements.

- Above and beyond the specific FCC requirements, Harron will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Harron's existing policies that would strengthen protection of CPNI, they should report such information immediately to Harron's Director of Customer Service so that Harron may evaluate whether existing policies should be supplemented or changed.

Notification of CPNI Security Breaches

- Harron notifies federal law enforcement of all breaches of its customers' CPNI pursuant to the procedures and timeframes described in Section 64.2011 of the FCC's rules. A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

- Harron notifies customers of all breaches of their CPNI pursuant to the procedures and timeframes described in Section 64.2011 of the FCC's rules.

Accountability:

- Customer privacy is a part of all job descriptions.
- Persons who fail to comply with Harron CPNI procedures are subject to a disciplinary process.
- Compliance with CPNI safeguards is part of each employee annual performance evaluation. Compliance can affect employees' raises, promotions, or continued employment.

Recordkeeping:

- The Customer Service Manager in each system maintains a record of training and it is filed in the personnel file of each employee.
- Harron maintains for 2 years (minimum) a record of all discovered breaches of CPNI and breach notifications to law enforcement and customers. The records include, to the extent possible, the dates of discovery and notification, a detailed description of the CPNI that was breached, and the circumstances of the breach.
- Harron maintains a record of all customer complaints related to their handling of CPNI, and records of Harron's handling of such complaints, for at least two years. All complaints are reviewed and Harron will consider any necessary changes to its policies or practices to address the concerns raised by such complaints. If Harron's practices outlined herein change to permit any of the following, Harron would maintain a record, for a period of at least one year, of: those limited circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI; supervisory review of marketing that proposes to use CPNI or to request customer approval to use or disclose CPNI; its sales and marketing campaigns that use its customers' CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, and the products and services offered as a part of the campaign; and records associated with customers' approval or non-approval to use CPNI, and of notification to customers prior to any solicitation for customer approval of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.