

Darlene P. Richeson
Director of Regulatory
and Legislative Policy Matters



GTE Service Corporation

1850 M Street, N.W., Suite 1200
Washington, D.C. 20036-5801
202 463-5294
202 463-5239 - fax
e-mail: dricheson@dcoffice.gte.com

EX PARTE OR LATE FILED

August 18, 1998

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
1919 M Street, N.W.
Washington, DC 20554

RECEIVED

AUG 18 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Re: CC Docket No. 96-115
Telecommunications Carriers' Use of Customer Proprietary Network Information
(CPNI)

Dear Ms. Salas:

Today, Darlene Richeson of GTE Service Corporation and David Foster of Arthur Anderson LLP, met with Tom Power of Chairman Kennard's office, The purpose of the meeting was to reiterate GTE's concerns regarding the electronic safeguard requirements adopted in the *Second Report and Order* of the above referenced proceeding, and to discuss GTE's conceptual alternative. The attached material was used to facilitate the discussion of these issues.

Please include this letter, and the attached discussion material, in the record of this proceeding in accordance with the Commission's rules concerning ex parte communications. Please call me if you have any questions.

Sincerely,


Darlene P. Richeson

Attachments

C: Tom Power

No. of Copies rec'd 021
List A B C D E

**CPNI METHOD OF COMPLIANCE WITH ELECTRONIC SAFEGUARDS
GTE and ARTHUR ANDERSEN
MEETING WITH THE FEDERAL COMMUNICATIONS COMMISSION
AUGUST 1998**

BACKGROUND

On February 26, 1998 the FCC released Order 96-115 (the "Order"), "Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information." The Order amends certain sections of Part 64 of the Code of Federal Regulations. The purpose of this paper is to discuss the implications of the amended Part 64.2009 entitled "Safeguards Required for Use of Customer Proprietary Network Information" ("the electronic safeguards section") on telecommunications carriers, and specifically GTE.

The Order requires carriers to either modify or implement systems that will ensure two mechanized safeguards. First, the Order requires carriers to implement software that will "flag" whether or not a customer has given approval to use CPNI. This information must be clearly visible to the system's users, along with the customer's existing service subscriptions, within the first few lines of the initial screen. Second, carriers must maintain an electronic access history recordkeeping system that tracks access to customer accounts, including when a customer's record is accessed, by whom, and for what purpose. These access histories must be maintained for at least one year.

Even though the FCC did not intend for these requirements to create significant cost burdens to the carriers, studies performed by GTE indicate that the costs of complying with the provisions of the Order would be substantial. In fact, GTE has estimated that the implementation cost alone for modifying its legacy systems to accommodate the "flagging" safeguard would be \$26 million, with annual recurring maintenance costs of \$4 million. The estimated implementation cost to accommodate the electronic access history recordkeeping requirement is \$16 million, with annual recurring maintenance costs of \$13 million. Obviously, the most troubling of these costs to GTE are the recurring costs that will be required to maintain compliance in the future. In addition to the initial and ongoing cost burden, the requisite system changes to accommodate the electronic safeguards section of the Order could not be accomplished without a massive re-deployment of those scarce IT resources within the company that are already at full capacity to accommodate other FCC-mandated system initiatives such as universal service, local number portability, and open market transition. In addition, IT personnel in all companies are heavily involved in efforts to make their systems Year 2000 compliant.

PROPOSED ALTERNATIVES TO IMPLEMENTATION

Introduction

In conjunction with the release of the Order, Subject Matter Experts (SMEs) from a sampling of CPNI systems at GTE were interviewed to assess the implications of the Order on GTE's operations, and to explore valid alternatives to a full implementation of the electronic

safeguards section of the Order. Six systems were studied; three "high risk" and three "low risk," (see risk classification definitions below under "Systems Reviewed") to determine if it would be possible to develop alternative methodologies and approaches towards securing all GTE business processes and systems to ensure CPNI is safeguarded against unauthorized use of the records for purposes of sales and marketing.

We based these alternatives on the "risk" classifications of each system as defined by what data is contained within the system, who accesses the system, and for what purpose they access the system. The objective in selecting the sample was to assess if it would be rational and cost effective to take a risk-based approach which would allow a carrier to utilize other methods of compliance with the electronic safeguards sections of the Order for systems with different levels of risk of misuse of CPNI data. A risk-based approach assesses all systems individually and determines the risk of CPNI misuse inherent within each system. System controls for CPNI would have to be unique for each system depending on the risks of misuse of the data. Utilizing a risk-based approach is advantageous because it results in expenditure of fewer resources to implement controls on those systems where risks are low, and more on systems where risks are high.

Additionally, as discussed in the chart below, we identified three types of controls that could be effective in mitigating the risk of misuse of CPNI. These controls, and a brief explanation of each, are as follows:

- Process Controls: These are non-mechanical controls that are accomplished through effective supervision of employees, training, incentives to proper behavior, compensation, etc. This control focuses on the design of the process and ensuring that it adequately includes the necessary controls.
- Systems Controls: These are mechanized controls accomplished through the computer such as limiting query capabilities and limiting access to only certain systems and data. The benefit of this control technique is that it limits the risk of human intervention in circumventing the control structure.
- Audit Controls: These controls are accomplished through audits of employee use of data by such means as observation (direct or remote), interviews with employees, procedural reviews, and sampling of specific records or activities. This control technique is effective because it tends to promote incentives to proper behavior.

Summary of Risk-Based Approach

The alternative procedures that would comprise a risk-based approach to the implementation of the Order can be illustrated as follows:

<i>Risk Categories</i>	<i>No Risk</i>	<i>Low Risk</i>	<i>Highest Risk</i>
<i>Basis for Risk Category</i>	No CPNI data	CPNI data present, but its primary use is NOT sales or marketing related	CPNI data specifically used for sales or marketing purposes
<i>Process Controls</i> (Supervisory and training)	No training required	CPNI training	CPNI training Increased Supervision
<i>Systems Controls</i> (CPNI flags, query controls, access restrictions, and electronic access history recording)	No CPNI flags No query controls No access restrictions	CPNI flags displayed Implement query controls Group profile access limitation	CPNI flags displayed Implement strict query controls Group profile access limitation Electronic access history recording
<i>Audit Controls</i> (Observations, interviews, procedural review, statistical sampling)	No audit required	Periodic process audits by interview and remote observation Periodic independent audit tests tailored to specific system risks	Continuous process audits by interview and remote observation Frequent independent audit tests tailored to specific system risks

We recommend that the most effective and efficient approach is to select a balanced set of process, system, and audit controls for each system based upon the risk of misuse of CPNI data present in each.

Systems Reviewed

We believe that the sample used provides a valid basis for moving forward with an expanded evaluation of this approach. The table below gives a general description of three of the specific systems that we reviewed, users of that system, types of CPNI (if any) housed within each system, and each system's associated risk classification. Risk classifications are based upon the following definitions:

No risk: Any system that does not contain CPNI.

Low risk: Any system that is accessed by employees whose primary duty is other than sales or marketing and that contains meaningful and significant CPNI which is valuable for these purposes.

High risk: Any system that is accessed by employees whose primary duty is sales or marketing and that contains meaningful and significant CPNI which is valuable for these purposes and is stored for a material amount of time.

Proposed Alternative Methods of Compliance

After interviews with the SMEs of each system selected and an assessment of other methodologies for maintaining control over CPNI, we believe that there are several logical alternatives to a full implementation of the electronic safeguards section of the Order. These alternatives would provide the same level of assurance over the unauthorized use of CPNI that the Order sought to accomplish, with a substantially reduced cost and time burden to the carriers. Our alternative compliance procedures take a risk-based approach in that we considered the relative risk of each system in determining the necessary controls. Based upon the results of the information compiled during the interview process, we have identified three alternative methods based upon "risk" classifications of the systems as defined by what data is contained within the system, who accesses the system, and for what purpose they access the system.

Systems reviews, on a test basis, to assess the ability to utilize this approach are as follows:

SYSTEM FUNCTION	USERS	TYPES OF CPNI	RISK CLASSIFICATION
General ledger system	Finance Support staff	None	No
System used primarily in customer care centers to assist in testing residential and business services and in generating trouble tickets	Primarily customer care center representatives Support staff and other	Customer name Types of service Quantity of service Technical configuration of service	Low
System used for profiling customers for product management and marketing	Primarily Marketing Information Mgt. (MIM) Support staff	Customer name Type of service Quantity of service	High

Following is a discussion of the methods that we believe could be implemented in lieu of a full implementation of the electronic safeguards section of the Order for the systems that we reviewed. We believe that each is a valid alternative in providing assurance that CPNI is not being misused:

No Risk System:

This system is deemed “no risk” because it does not contain any form of CPNI. There is literally no risk of CPNI misuse by users of this system.

Access Restrictions

- No access restrictions necessary because the system does not contain CPNI.

CPNI Flags

- Flags would not be necessary because the system does not contain CPNI.

Audit Approaches

- Audits would not be required for this system because it does not contain CPNI.

Low Risk System:

This system is deemed “low risk” because although it does access CPNI, it does so only through a graphical user interface with other mainframe systems (i.e. the system extracts data from the mainframe and reformats that data on the computer screen; data is not stored within the system itself). Also, the users do not have a primary objective of selling or marketing.

Access Restrictions

- Limit access to the systems by implementing group profile access limitations. Group profile access limits a user to only those systems that are approved for the user’s work group. Thus, a user can only gain access to those systems that have been approved for the group to which the user belongs.

CPNI Flags

- Build CPNI flags on all systems containing CPNI information

Audit Approaches

- **Periodically** conduct manual observation audits by listening/remote viewing of system screens during conduct of business.
- **Periodically** perform independent audits which would focus on the following control areas:
 1. Do the supervisors at the customer care center understand the guidelines of the Order as it relates to their work group’s normal business activities?

2. Are these guidelines conveyed to the customer care representatives through formal and informal training?
3. Are the CPNI flags displayed correctly on the affected system?
4. Do the representatives market services (outside of the customer's existing service subscriptions) to customers with CPNI flags marked "No," meaning the customer has not given consent? Examine a statistical sample of sales originating from these centers in relation to CPNI restrictions on the use of the data.

On an annual or semi-annual basis, independent auditors could interview supervisors and customer care reps to gain an understanding of their knowledge on this topic. The independent auditor could also review training and new hire orientation materials to ensure that the spirit of the Order is explained regarding its influence on daily operations. Finally, independent "surprise" tests could be performed to observe the representative's interaction with the system screens and with customers via remote terminals, or in person. From the data gathered during these audits, internal control reports could be issued by the independent auditor and communicated to the FCC annually.

High Risk System

This system is deemed "high risk" because it actually stores large amounts of CPNI, which is used primarily by marketing personnel for the purpose of sales and marketing. This CPNI is stored within the system for material periods of time.

Access Restrictions

- Limit access to the system by implementing group profile access limitations and/or
- Limit access to the systems by implementing query controls for queries which extract significant and meaningful CPNI so that customers who have "No" flags can only be accessed by users to market the customer's existing services.

CPNI Flags

- Build CPNI flags on all systems containing CPNI.

Audit Approaches

- Conduct **continuous** manual observation audits by listening/remote viewing of system screens during conduct of business.
- Conduct **frequent** independent audit control tests which focus on the following areas:

1. Do the queries prevent users from using CPNI for sales or marketing purposes outside of the customer's existing service subscriptions when a customer has NOT given consent?
2. Are ad hoc reports that are queried from the system stored and filed and periodically reviewed to ensure no misuse of CPNI is occurring?
3. Do the supervisors and actual users of this system understand the Order and its requirements on their daily activities?
4. Are ad hoc reports monitored frequently to ensure that customers with "No" flags are not marketed services outside of their existing service subscriptions.
5. Utilize statistical sampling to test reports that are generated from the system and review query programs to ensure they prohibit misuse of CPNI that has been flagged "No."

The above alternative approach is far more cost effective than electronic access history recordkeeping system changes, because marketing personnel use this database everyday in the normal course of business. Without conducting the manual audits of the report outputs and queries used, there is no way to gain assurance that the requirements of the electronic safeguards section of Order are being met. These process and output audits assure the FCC that the correct controls are in place to prevent GTE from using non-consenting customer CPNI. Based upon the success of the above controls, the carrier could evaluate the need to build full electronic access measurement and reporting systems called for by the Order.

REGULATORY ANALYSIS

We believe that the methods proposed above represent logical and viable alternatives to the full implementation of the electronic safeguards section of the Order that will not compromise the spirit of the Order's objectives. Regulatory oversight and controls will continue to be maintained, at a significantly lower cost to the carriers and the ratepayers. The proposed methodology above for CPNI is not unlike the procedures that have been accepted by the FCC and utilized by carriers and auditors for many years on cost allocation manual audits.

The Commission addressed the allocation of costs between regulated and non-regulated operations in Order 86-111. In Order 86-111, the Commission established the general principles of cost allocation to be followed but not the specific methods of allocation. The methods to be applied were developed by the carriers and filed with the FCC in the Cost Allocation Manuals (CAM). The CAM developed allocation approaches and methods that considered both the Commission's cost allocation objectives and the unique and changing circumstances of each carrier. The CAMs were modified from time to time to reflect changes in both the unique circumstances of each carrier and changes in Commission procedures. This method allowed the carrier to develop its allocation procedures to consider its unique facts and circumstances rather than imposing a single set of methods to all carriers.

The results of the allocations were then audited each year by the independent accountants of the carrier and the results were reported to and reviewed by the FCC audit staff. These audits involve the auditor reviewing and testing the process and the controls surrounding cost separations. Affiliate transactions are tested on a rotational, three-year basis because the costs of performing 100% audits every year would simply be too costly and unnecessary.

BENEFITS

Consumers

Consumers would benefit from our suggested compliance procedures, because these procedures would result in stronger controls over CPNI misuse, ensuring consumer privacy. Our recommendations focus on training employees and performing periodic audits that will give incentive to proper employee behavior, rather than after-the-fact monitoring.

FCC

The FCC also benefits from the alternative compliance procedures. These procedures will help to ensure that the spirit of the Order is maintained by providing for a balanced set of both system and behavioral controls. The proposed approach emphasizes training employees about the implications of the Order on their daily activities and giving them incentives to respond properly. Additionally, the alternative compliance procedures would benefit the FCC by providing for a shorter implementation period; employee training and manual audits could begin (and be completed) relatively soon, while massive systems changes would likely require several months to be implemented and tested.

Carriers

By utilizing a risk-based approach in implementing the electronic safeguard provisions of the Order, carriers will be given the flexibility to consider the uniqueness of each system that contains CPNI data and will be allowed to design controls that are the most effective and efficient in monitoring the risks of CPNI misuse inherent within each system. By using this approach, carriers will be able to avoid unnecessary and overly burdensome costs of modifying all of their systems in order to be in compliance with the electronic safeguards section of the Order. Estimated annual recurring audit fees to perform these alternative compliance tests could range initially from \$1.5 million to \$2.0 million (not including systems modification costs that would be required based upon the unique risk assessment of each system). As the audit approach and system and manual controls are proven to be effective these costs could decline. These costs are significantly less than what would be required if the full provisions of the electronic safeguards section of the Order were implemented.

We believe that the compliance methods discussed above would not compromise the controls effectiveness over CPNI misuse and in fact, would likely provide better controls in the long run. In addition, the alternative compliance procedures would likely provide for a much quicker implementation of the controls sought by the Order and should provide for more timely audits of the affected systems and users. Lastly, the alternative compliance procedures will be

beneficial in limiting the amount of stranded costs associated with making massive changes to existing systems that have short remaining useful lives before scheduled replacement.

This alternative method of compliance makes much more sense than a total implementation of the electronic safeguards section of the Order given the rapidly changing system environments that carriers operate in today. As carriers implement new systems (either large or small), they should have the ability to design unique controls for each system, consistent with how system controls are normally implemented in today's environment.

CONCLUSION

As a result of our sample studies of various systems at GTE and our understanding of Order 96-115, we believe that there are valid and logical alternatives to the procedures outlined in the electronic safeguards section of the Order. We urge the FCC to consider staying the electronic safeguards section of the Order and giving telecommunications carriers the option to determine and implement unique control structures to mitigate the risk of CPNI misuse.



FCC Order 96-115

CPNI Electronic Safeguard Requirements

“Telecommunications carriers must maintain an electronic audit mechanism that tracks access to customer accounts, including when a customer’s record is opened, by whom, and for what purpose. Carriers must maintain these contact histories for a minimum period of one year.”¹

Note 1: Part 64.2009, section (c)



Executive Summary

- Impact of the Electronic Safeguard Requirements of the Order on GTE
- Proposed Alternative Methods of Order Compliance
- Proposed Systems Risk-Based Approach
- Benefits of Proposed Alternative Implementation Options
- Summary



Impact of the Electronic Safeguard Requirements of the Order on GTE

- **Electronic Safeguard Provisions are very costly to implement and maintain (electronic audit mechanism + display of CPNI flags)**
 - Estimated development costs associated with “flagging” safeguard = \$26 million¹
 - Estimated development costs associated with electronic audit = \$16 million¹
 - Estimated annual recurring maintenance costs for “flagging” safeguard = \$4 million¹
 - Estimated annual recurring maintenance costs for electronic audit = \$13 million¹
- **Electronic Safeguard Controls may not meet the cost vs. benefit test**
 - Focus is on tracking access versus incenting proper employee behavior
- **Current IT staff must be re-deployed to satisfy the requirements of the Order**
 - Existing resources dedicated to Y2K , Local Number Portability, Universal Service, and Open Market Transition
 - Questionable as to whether time frame of the Order can be met
 - There are currently 346,000 unfilled IT positions in the U.S.²

Note 1: Cost estimate provided by GTE Systems personnel (these costs DO NOT include costs to implement the Order for outsourced systems)

Note 2: Results are part of a recent survey released by the Information Technology Association of America and Virginia Polytechnic Institute

**ARTHUR
ANDERSEN**



Proposed Alternative Methods of Order Compliance

Alternative: Risk-based controls and audit approach

- Carrier bases the level of process, system, and audit controls on the risk of misuse of CPNI data
 - Don't apply a single approach to all systems
 - The audit will be a control measure to discourage the improper use of CPNI
- Rather than implementing an inflexible “electronic envelope” around all systems, add a balanced set of supervisory, training, behavioral, access and query control capabilities as needed to ensure compliance
- Audit both the system's controls and the behavior of the system's users
- Provides feedback since the burden is on the carrier, not the FCC



Proposed Systems Risk-Based Approach

Risk Categories	No Risk	Low Risk	Highest Risk
Basis for Risk Category	No CPNI data	CPNI data present, but its primary use is NOT sales or marketing related	CPNI data specifically used for sales or marketing purposes
Process Controls (Supervisory and/or Training issues)	No training required	CPNI training	CPNI training Increased Supervision
Systems Controls (CPNI flags, Query controls, Access restrictions and / or Electronic Audit Mechanism)	No CPNI flags displayed No query controls No access restrictions	CPNI flags displayed Implement query controls Group profile access limitation	CPNI flags displayed Implement strict query controls Group profile access limitation Electronic Audit Mechanism
Audit Controls (Observations, Interviews, Procedural Reviews and / or Statistical Sampling)	No audit required	Periodic process audits by interview and remote observation Periodic independent audit tests tailored to specific system risks	Continuous process audits by interview and remote observation Frequent independent audit tests tailored to specific system risks

SELECT A BALANCED SET OF PROCESS, SYSTEM AND AUDIT CONTROLS FOR EACH SYSTEM



The alternative audit options benefit ALL parties involved:

- **For Consumers**
 - Meets the Order's objective of ensuring consumer privacy
- **For the FCC**
 - Complies with the spirit of the Order
 - Provides a balanced set of both system and behavioral controls
 - Shortens implementation time
- **For Carriers**
 - Provides stronger controls to prevent CPNI misuse
 - Allows control solutions to be tailored to system risks and planned future use
 - Shortens implementation time and requires fewer IT resources
 - Consistent with how system controls are normally implemented



The proposed alternative options will meet the requirements of FCC Order 96-115:

Section 222(a) of the Telecommunications Act of 1996 stipulates..." [e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers."

GTE
Proposed Alternatives to Electronic Audit and Flag Requirements

Low	National Open Market Centers - Process service requests from CLEC - Administrative responsibility only, no sales	Ordering Systems (e.g. SIGS)	<ul style="list-style-type: none"> * Internal training of center employees and supervisors to ensure understanding of CPNI rules * Group profile access limitations * Periodic interviews by independent auditors of center employees including observations on statistically valid data to ensure employees understand and are in compliance with the CPNI order * No CPNI flags required
Low	Installer, Repair Man	Work distribution systems (e.g. AWAS)	<ul style="list-style-type: none"> * Internal training of employees and supervisors to ensure understanding of CPNI rules * Periodic reviews by independent auditors of training program documentation and schedules * Group profile access limitations * Periodic interviews by independent auditors of center employees including observations on statistically valid data to ensure employees understand and are in compliance with the CPNI order * CPNI flags required unless non-durable consent is required on every contact, then no CPNI flag is required
High	Front line consumer and small business sales / Care	Ordering, billing and repair systems (e.g. TAS, CBSS, NOCV, Starnem, MARK)	<ul style="list-style-type: none"> * Internal training of user groups accessing the system * Group profile access limitations * Schedule statistically valid random samples of activity via remote observation * Continuous interviews by independent auditors of employees accessing the system to determine whether they understand and are in compliance with the CPNI order * CPNI flags required
Highest	Marketing, Sales Account Reps	Marketing Databases (e.g. Powerbase) Used for the purposes of outbound sales or sales proposals to larger customers	<ul style="list-style-type: none"> * Significant training of user groups accessing the database * Group profile access limitations * Schedule statistically valid random samples of a database storing contents of query requests * Continuous interviews by independent auditors of employees accessing the system to determine whether they understand and are in compliance with the CPNI order * Electronic audit mechanism * CPNI flags required