1401 H Street, N.W.
Suite 1020
Washington, D.C. 20005
Office 202/326-3810

ORIGINAL

Ameritech

EX PARTE OR LATE FILED

Celia Nogales
Director - Federal Relations

September 24, 1998

RECEIVED
SEP 24 1998
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
1919 M Street, NW
Room 222
Washington, DC 20554

Re: **Ex Parte Filing**
CC Docket No. 96-115, CPNI

Dear Ms. Salas:

On Wednesday, September 23, 1998, Michael Pabian, Chuck Bohl and I met, in separate meetings, with Tom Power, Legal Advisor to Chairman Kennard, Jim Casserly, Senior Legal Advisor to Commissioner Ness, Kyle Dixon, Legal Advisor to Commissioner Powell, and Paul Gallant, Legal Advisor to Commissioner Tristani to discuss issues in Docket 96-115. Ameritech provided data regarding the negative impact of the FCC's electronic safeguard requirement and offered support for the granting of a stay petition. Ameritech also provided alternatives for the electronic account flagging and access tracking requirements of the FCC's CNPI order. The attached document, which was utilized during the course of the discussions, outlines the presentation and provides additional information.

Sincerely,

Celia Nogales

Attachment
cc: T. Power
J. Casserly
K. Dixon
P. Gallant

No. of Copies rec'd 0+2
List A B C D E

Customer Proprietary Network Information
FCC Docket No. 96-115

Analysis of Electronic Safeguard Requirement

Ameritech.

September 23, 1998

Electronic Safeguard Requirement

Sec 64.2009(a):

Telecommunications carriers must develop and implement software that indicates within the first few lines of the first screen of a customer's service record the CPNI approval status.

Sec 64.2009(c):

Telecommunications carriers must maintain an electronic audit mechanism that tracks access of customer's 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.

Electronic Safeguard Effective Date

Electronic safeguards must be implemented by 1/26/1999.

Impact of the Electronic Safeguard Requirement on Ameritech

- Literally read, approximately (400) of Ameritech's systems 'open' (i.e., Access) records containing customer CPNI.
  - (87) of these are impacted by the 'Display Consent' Obligation
  - All (400) are impacted by the 'Track Access' Obligation
- Systems development for compliance estimated to be 100 person-years, which would cost:
  - $12 million to 'Display Consent'
  - $55 million to 'Track Access'
- Processing and storage required to retain a tracking audit for one year
  - 1.7 trillion tracking records
  - $500 million annual cost of processing and storage
- Represents twice the current total Ameritech disk storage for all purposes.
- Systems development would compete for human resources assigned to other critical projects, such as 'Y2K.'

Inappropriateness of the Electronic Safeguard Requirement

- Majority of the (400) systems are part of the Ameritech internal processing infrastructure not directly involving sales activity.

Example: Ameritech Customer Information System (ACIS) - Attachment A

- Contains (150) tasks which access forms of CPNI information
- Only (2) of these tasks are directly accessed in connection with potential sales activity
  - Customer Sales Inquiry (e.g., Caller ID)
  - Billing Inquiry (i.e., account inquiry which may bridge to a sales opportunity)
- Remaining tasks are not involved in potential sales activity and support system activities such as account posting, pricing, formatting, administrative reporting, error handling, cash handling, journalizing, order provisioning, etc.

- Similarly, many other Ameritech systems used for such things as finance and network management perform many tasks in which CPNI is accessed wholly unrelated to sales activity.

Conclusion Regarding the Electronic Safeguard Requirement

- The FCC's statement that the electronic safeguard obligation will not be overly burdensome (Order, para. 199) is inconsistent with the magnitude of Ameritech's projected costs.
- The vast majority of data collected under a literal interpretation would:
  - Provide no value to audit compliance
  - Create an inordinate cost without commensurate benefit
  - Require an unfathomable volume of storage
  - Create system processing overhead which could compromise customer service
- A Stay of the Electronic Safeguard Requirement is needed pending reconsideration.
- A Stay is needed now to avoid investment in systems solutions which would likely be found to be unneeded.
- In the alternative the Commission should consider the following common sense recommendations which balance customers' reasonable expectations of privacy with manageable safeguard obligations.

Common Sense Alternatives

1. Displaying CPNI Consent Status

Recommendation: Carriers should be permitted to use less costly means of compliance concerning the CPNI Consent Status of customers in lieu of software "flagging." For example:

a) No "flagging" should be required where the specific market unit is not soliciting the CPNI consent contemplated by Sec 64.2009(a) from customers ("permanent CPNI consent"). For example, Ameritech's Consumer Services unit, which provides residential telecommunications services, has concluded that it is not feasible to obtain permanent CPNI consent and has therefore instructed service representatives that they must assume "no consent" for every customer interaction.

Common Sense Alternatives (cont.)

b) Where the permission rate for permanent CPNI consent is extremely high, customers declining to grant permanent CPNI consent may be effectively handled on an exception basis. For example, Ameritech's Custom Business Services unit, which provides telecommunications services to Ameritech's largest accounts, has obtained permanent CPNI consent from over 90% of customers solicited. These are large, sophisticated customers, who understand their telecommunications needs and the value of granting permanent CPNI consent. The customer base is so small (approx 250) and the number of service representatives so limited that service representatives can be adequately informed of those customers who have declined to grant CPNI consent - without the need for "flagging." Currently the list of customers who have declined to grant permanent CPNI consent are posted on an electronic bulletin board that the service representatives have access to on a daily basis.

Common Sense Alternatives (cont.)

2. Electronic Tracking Requirements

   a) Inbound Calls

   Recommendation: Carriers should not be required to electronically track on inbound calls. Training, remote monitoring and periodic auditing should be permitted instead to ensure compliance with CPNI obligations.

   - Ameritech handles in excess of 60 million inbound calls from customers yearly.
   - Access to account information on all inbound calls is necessary in order to address the customer's inquiry and permission to do so is implicit in the customer's initiation of an inbound call.

Common Sense Alternatives (cont.)

a) Inbound Calls (cont.)

- The overwhelming majority of these calls relate to either bill inquiry or an in-category product or service inquiry for which no customer CPNI consent is required. In addition, in Ameritech's Consumer Services unit, it is estimated that less than 4% of all inbound calls results in a bridging to an out-of-category sales attempt.
- By definition these calls are customer generated for which expectations of privacy vis-a-vis access to customer account information should be minimal.
- Congress clearly recognized that customers' expectation of privacy on inbound calls are lower than for other transactions by the adoption of Sec 222 (d)(3).
- Opportunities and motive for "casual" perusal of customer accounts by service representatives on inbound calls are de-minimis because calls are subject to remote monitoring and service representatives are incented to process as many calls in the shortest duration practicable.

Common Sense Alternatives (cont.)

b) Outbound Marketing and Sales

Recommendation: Impose electronic tracking requirements only on systems used at the campaign level to identify the "list" of customers to be contacted in connection with each outbound campaign. Marketing and sales systems used in support of such activities and the personnel employing such systems should be subject to training and spot auditing.

- Customers' expectations of privacy are most acute with respect to outbound marketing campaigns. If there is any value in electronic tracking it is in connection with such outbound marketing campaigns.
- Outbound marketing campaigns can be categorized as follows:
    - Outbound telemarketing
    - Direct mail
    - Bill inserts
    - Bill messages
    - Outbound premises visits

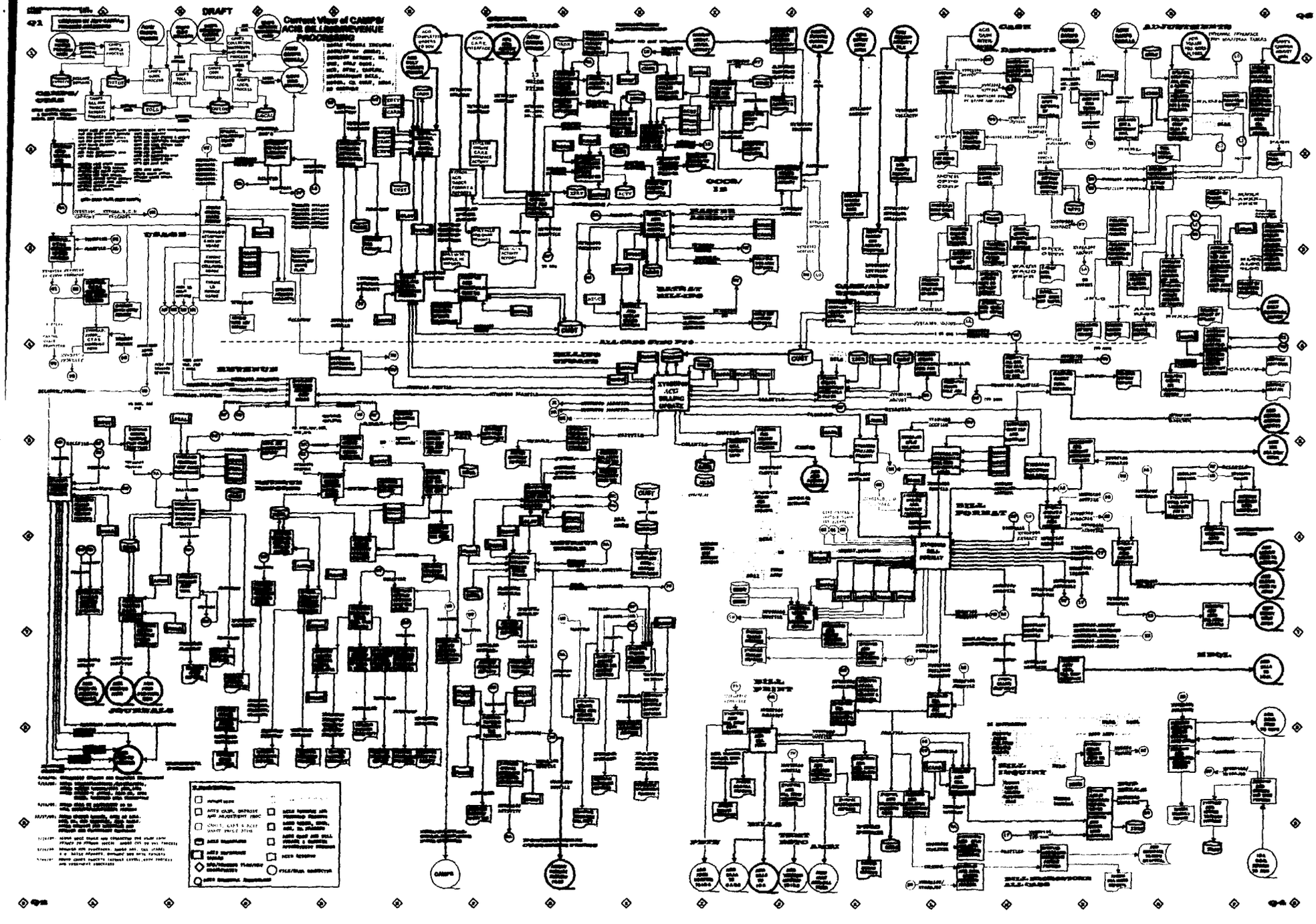
Common Sense Alternatives (cont.)

- Ameritech has approximately 132 systems which may be used in some way in support of an outbound marketing campaign. However, it is not necessary to electronically track access to all these systems in order to ensure that customers' expectations of privacy are met.
- Ameritech has created a "gatekeeper" procedure in which every outbound marketing campaign creates an electronic file which lists all customers intended to be contacted in connection with such campaign and the data elements of the customer's account which were accessed. This "gatekeeper" procedure is in addition to the supervisory review requirement for outbound marketing campaigns mandated by the Commission.
- The "gatekeepers" of this process have been specially trained and are well versed in the requirements of Section 222 of the Telecom Act and the Commission's regulations.

Common Sense Alternatives (cont.)

- This gatekeeper process generates an audit trail for each outbound customer "contact," including the personnel requesting the contact, the reason for the contact, the dates of the campaign and the customer information accessed, thereby capturing the tracking elements the Commission identified in its Rules.

- With respect to the marketing and sales systems that support this gatekeeper process, training and spot auditing are sufficient. Some of these systems already track access codes which can be used to determine who entered certain databases and on which dates but none of these systems can easily or cost effectively be modified to provide the level of detail a liberal reading of the Commission's rules would seem to suggest. This would appear unnecessary.

  The sales and marketing personnel with access to these systems are ultimately motivated by sales. If access to these databases does not pass muster with the gatekeeper and result in a CPNI compliant list with which to contact customers to make such sales, they will have failed in the discharge of their primary job responsibilities. Thus through this process sales and marketing personnel are incented to comply not thwart the CPNI requirements.

ATTACHMENT A