

FHH Telecom Law
April 2006

**Under Fire, FCC Proposes
New Customer Privacy Standards**

By Donald Evans
evans@fhhlaw.com
703-812-0430

Several well-publicized reports of the routine disclosure of customer information by persons or entities who have gained access to telecom carriers records have prompted demands on Capitol Hill and at the FCC to erect new safeguards for such information. Theoretically, the Telecom Act and the FCC's rules prevent third parties from gaining access to such material without customer consent. These "safeguards" have turned out to be very porous indeed. Congress has hauled the Chairman and several carriers to hearings to explain how and why customer information (familarly dubbed "CPNI" -- customer proprietary network information) is being divulged to third parties without customer consent. The resulting heat has prompted the FCC first to investigate the largest carriers and slap \$100,000 fines on ALLTEL and AT&T for failure to submit proper certifications of compliance. Next the FCC demanded that *all* telecom carriers file reports detailing their CPNI protection policies, with top-level management having to certify to the adequacy of the policies. (The requirement to have a privacy enforcement policy and certify to it annually had been on the FCC books for several years but had been largely ignored by the carrier community.) Finally, the FCC has initiated and placed on a super fast-track a rulemaking proceeding to impose additional protective measures on carriers.

The FCC has proposed to do some or all of the following:

1. Require consumer-set passwords for all outside access to CPNI. This would deter third parties pretending to be the customer from accessing the information but would also complicate all customer transactions and lead to lost-or-forgotten password problems.
2. Require an audit trail to be established for disclosure of CPNI to the customer herself. (Records must already be kept of disclosures to third parties or for marketing use.)
3. Encrypt all CPNI data.
4. Require the destruction of CPNI when no longer needed for billing purposes.
5. Notify the customer whenever his security has been breached.
6. Establish safe harbors from enforcement activity if a carrier complies with CPNI

requirements.

7. Require carriers to file annual reports on a date certain certifying that the company has adequate CPNI protection policies in place.

There is some question as to whether these measures significantly improve consumer protection or, if they do, whether the cost is justified. We can expect that the FCC will, at a minimum, require annual reporting since that just imposes a cost on carriers and gives the appearance of having gotten tough on the industry. The FCC is also looking for other suggestions as to how to deal with the CPNI disclosure problem.

Interested parties may file comments on or before April 14. Replies are due by May 15. We do expect the FCC to act on this proceeding by the early summer.