NEWS

Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action.
See MCI v. FCC. 515 F 2d 385 (D.C. Circ 1974).

FOR IMMEDIATE RELEASE:
February 10, 2006

NEWS MEDIA CONTACT:
Mark Wigfield, 202-418-0253
Email: mark.wigfield@fcc.gov

FCC EXAMINES NEED FOR TOUGHER PRIVACY RULES

Comment Sought On Measures Proposed by EPIC, Commission

Washington, D.C. – The Federal Communications Commission today launched a proceeding to examine whether additional security measures could prevent the unauthorized disclosure of sensitive customer information held by telecommunications companies.

In a Notice of Proposed Rulemaking (NPRM) adopted today, the Commission seeks comment on a variety of issues related to customer privacy, including what security measures carriers currently have in place, what inadequacies exist in those measures, and what kind of security measures may be warranted to better protect consumers' privacy. The Notice grants a petition for rulemaking filed by the Electronic Privacy Information Center (EPIC) expressing concerns about whether carriers are adequately protecting customer call records and other customer proprietary network information, or CPNI. EPIC claims that some data brokers have taken advantage of inadequate security standards to gain access to the information under false pretenses, such as by posing as the customer, and then offering the records for sale on the Internet. The practice is known as "pretexting."

In its petition, EPIC proposed five additional security measures that it says will more adequately protect CPNI. The NPRM specifically seeks comment on these five measures, which are:

- Passwords set by consumers.
- Audit trails that record all instances when a customer's records have been accessed, whether information was disclosed, and to whom.
- Encryption by carriers of stored CPNI data.
- Limits on data retention that require deletion of call records when they are no longer needed.
- Notice provided by companies to customers when the security of their CPNI may have been breached.

Section 222 of the Communications Act requires carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure. Current rules require carriers to certify compliance with the Commission's CPNI rules and make that certification available to

the public, but the Commission observes that a lack of uniformity in these certifications could be an obstacle to effective enforcement. The Commission seeks comment on a tentative conclusion that it should amend its rules to require carriers to file annual compliance certificates with the Commission, along with a summary of all consumer complaints received in the past year concerning the unauthorized release of CPNI and a summary of any actions taken against data brokers during the preceding year.

The Commission also seeks comment on other ways to protect customer privacy, including whether carriers should be required to take the additional step of calling a subscriber's registered telephone number before releasing CPNI in order to verify that the caller requesting the information is actually the subscriber.

Action by the Commission, February 10, 2006 by Notice of Proposed Rulemaking (FCC 06-10). Chairman Martin, Commissioners Copps, Adelstein and Tate.

Docket No.: 96-115; RM-11277

Wireline Competition Bureau Staff Contact: Tim Stelzig at 202-418-0942

-FCC-

News about the Federal Communications Commission can also be found on the Commission's web site www.fcc.gov.