



## **FCC Toughens Telephone Privacy Requirements**

By [Brian J. Hurh](#), [K.C. Halm](#) and [John D. Seiver](#)  
[April 2007]

On April 2, 2007, the Federal Communications Commission (FCC) released a Report and Order and Further Notice of Proposed Rulemaking (“Order”) in response to a petition filed by the Electronic Privacy Information Center (EPIC) addressing the practice of “pretexting” and privacy concerns over customer proprietary network information (CPNI). This Order substantially amends the FCC’s existing rules governing the use and disclosure of CPNI by imposing more stringent access and authentication standards and procedures on telecommunications carriers.

The Order also extends the same obligations to interconnected VoIP service providers. Relying on its ancillary authority under Title I of the Communications Act, the FCC imposed these new privacy obligations on interconnected VoIP providers without classifying VoIP as a telecommunications service, or subjecting that service to other Title II obligations. In addition, the Order solicits additional comment on related implementation issues.

### **Password requirement for release of CPNI**

Under the new rules, carriers may not release call detail information during a customer-initiated telephone contact unless the customer provides a password. Non-call detail CPNI may be released without a password, but the carrier is still under a duty to authenticate a customer prior to disclosure. (Non-call detail is information that does not pertain to the transmission of specific telephone calls. For example, while the number called and the duration of the call are considered “call detail” information, remaining minutes of use would not be.) If a customer forgets his or her password, the carrier may use backup customer authentication methods, but these methods may not rely on readily available biographical information or account information. If the customer does not provide a password, then the carrier may only release call detail information by sending it to the address on the account or calling the customer at the telephone number on the account. Carriers must also establish a password protection mechanism for online account access, although for in-store visits, carriers may release CPNI if the customer presents a valid, government-issued photo ID that matches the name on the account.

## **Customer notification**

Carriers will be required to notify customers immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. Such notification may be in a voicemail, text message, or by mail to the address on the account.

In the event of an unauthorized disclosure of CPNI, carriers must first notify the United States Secret Service (USSS) and the FBI and then the customer, unless urgency requires immediate notification to the customer or the public. These new requirements do not alter existing law regarding access by law enforcement to customer records (e.g., ECPA), nor are they intended to mandate customer notice when a carrier is permitted by law to disclose customer personal information without subscriber notice in order to protect its property or users of its services and other carriers.

## **Disclosure to joint ventures and independent contractors**

In a major change, carriers must have customer consent to share CPNI with their joint venture partners and independent contractors for purposes of marketing communications-related services. This essentially rejects the ruling in *U.S. West v. FCC*, 182 F.3d 1224 (10 th Cir. 1999), in which the U.S. Circuit Court of Appeals for the Tenth Circuit threw out the FCC's earlier rules implementing an opt-in regime for CPNI use and disclosure.

## **Annual certification and continued vigilance by carriers to protect CPNI**

Carriers will now have to file an annual certification with the FCC that includes an explanation of any action taken against a data broker and a summary of all consumer complaints received in the previous year regarding the unauthorized release of CPNI. Under prior rules, carriers were only required to certify annually that the company had established procedures to protect CPNI. Carriers must also now take reasonable steps to protect CPNI from hackers and other unauthorized attempts by third-parties to access CPNI, although the FCC is not requiring encryption of CPNI in storage.

## **Further notice of proposed rulemaking**

The FCC is seeking additional comment on several other issues related to these new rules, and specifically whether there is a need for additional privacy protections, including: (1) additional password protections; (2) audit trails; (3) physical safeguards; (4) limits on data retention; and (5) protection of information stored on mobile communication devices.

The FCC's Order reflects the growing concern surrounding the privacy and protection of CPNI and customer information generally. Telecommunications carriers and interconnected VoIP providers will need to pay even more attention to how they maintain customer data and

who has access to it, in addition to determining how these new rules apply to carriers' relationships with joint venture partners and independent contractors.

Davis Wright Tremaine counsels interconnected VoIP service providers and telecommunications carriers on these and other issues. If you would like additional information or assistance with these matters, please contact us.



For coverage of this and other issues of interest, please visit <http://www.privsecblog.com>.

---

For more information, please contact:



[John D. Seiver](#)  
Washington, D.C.  
(202) 973-4212  
[johnseiver@dwt.com](mailto:johnseiver@dwt.com)



[Charlene A. Brownlee](#)  
Seattle, Washington  
(206) 628-7616  
[charlenebrownlee@dwt.com](mailto:charlenebrownlee@dwt.com)



[James M. Smith](#)  
Washington, D.C.  
(202) 973-4288  
[jamesmsmith@dwt.com](mailto:jamesmsmith@dwt.com)

***Other DWT Contacts:***

[K.C. Halm](#), Washington, D.C., (202) 973-4287, [kchalm@dwt.com](mailto:kchalm@dwt.com)

[Treg Tremont](#), San Francisco, (415) 276-6521, [tregtremont@dwt.com](mailto:tregtremont@dwt.com)

[Brian J. Hurh](#), Washington, D.C., (202) 973-4279, [brianhurh@dwt.com](mailto:brianhurh@dwt.com)

This advisory is a publication of the Privacy/Security and Communications Groups of Davis Wright Tremaine LLP. Our purpose in publishing this advisory is to inform our clients and friends of recent legal developments. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations. Attorney Advertising. Prior results do not guarantee a similar outcome.

Copyright © 2007, Davis Wright Tremaine LLP.