

Anti-Pretexting Legislation Takes Effect – VoIP Call Records Included

On January 13, 2007, President Bush signed into law the Telephone Records and Privacy Protection Act of 2006, which was passed by Congress last month to protect consumers' phone records from the practice of "pretexting."¹ The statute makes it unlawful for persons to engage in pretexting and to buy or sell records that were obtained through pretexting. Violations are subject to criminal penalties of imprisonment up to ten (10) years, a fine, or both. The Act is effective immediately.

Pretexting Prohibited

The statute amends Title 18 of the U.S. Code to add a new section prohibiting pretexting. Specifically, the statute makes it a criminal violation if a person "knowingly and intentionally obtains or attempts to obtain" confidential phone records by (1) making false or fraudulent statements to a telephone company employee, (2) making false or fraudulent statements to a telephone company customer, (3) providing a document (such as an authorization form) knowing the document is false or fraudulent, or (4) accessing customer records via the Internet without prior authorization from the customer whose records are obtained.

Purchase or Sale of Unlawfully Obtained Records Also Prohibited

The statute also prohibits the purchase or sale of confidential phone records obtained through pretexting. The statute prohibits

such purchase or sale of confidential phone records without prior authorization from the customer to whom such records relate or "knowing or having reason to know such information was obtained fraudulently." Thus, companies that merely obtain telephone call records – such as in support of an active credit and collection department – are potentially responsible under the statute. In addition, companies obtaining telephone information in connection with investigations – such as the highly-publicized HP investigations earlier this year – also are potentially culpable under the statute. Such companies should review their information acquisition procedures to determine compliance with the new requirements.

Two important exceptions to this prohibition apply. First, the statute permits a "covered entity" – largely, but as discussed in the next section, not exclusively, telephone carriers – to use confidential phone records for purposes permitted by Section 222(d) of the Communications Act. Section 222(d) permits telephone carriers to use telephone and usage records to protect a carrier's rights (including billing and collection of telecommunications services), to respond to inbound telemarketing calls and to provide wireless caller location information to public safety agencies.

Second, the prohibition on the purchase or sale of confidential phone records excludes uses "otherwise permitted by

**For more information
please contact:**

Steven A. Augustino
(202) 342-8612
saugustino@kelleydrye.com

or

Regular Kelley Drye
Attorney Contact

¹ Telephone Records and Privacy Protection Act of 2006, H.R. 4709 (109th Congr., 2d Sess.), to be codified at 18 U.S.C. § 1039.

applicable law.” This exception likely would permit, for example, the purchase or sale of telephone directory information, which is required to be made available pursuant to Section 222(e) of the Communications Act. (Note: Directory information only includes customer name, address and telephone number; it does not include any call detail records.)

VoIP Call Records Included

The statute defines “confidential phone record information” in a manner consistent with the existing definition of private telephone-related information in Section 222 of the Communications Act, with two noteworthy changes. First, the statute gives protection not only to records of customers using traditional telecommunications services but also to most Voice over Internet Protocol (VoIP) services. Specifically, the statute uses an unusual definition of “IP-enabled voice services” to encompass any real-time voice communications offered to the public if the service can receive calls from or originate calls to the public-switched telephone network “or a successor network.” In the legislative history, Senator Ted Stevens (R-AK) acknowledged that this definition is broader than the FCC’s definition of “interconnected VoIP services” and stated that use of the definition here “should not be interpreted as a signal to the FCC that it should alter or change the definitions of Interconnected or IP-enabled voice services that it has used in other contexts.”² The pretexting definition could be interpreted to include services such as various “click-to-call” services that may not otherwise fit the FCC’s definition.

Second, the definition is silent on the treatment of telephone directory information, also

known as subscriber list information. Section 222 explicitly excludes subscriber list information from its definition of private records (customer proprietary network information or CPNI). The Telephone Records and Privacy Protection Act of 2006 does not contain this exception, although the statute permits the sale or purchase of telephone records “as otherwise permitted by law.” Despite the ambiguity created by this statute’s silence on subscriber information, it does not appear that Congress intended to restrict the publishing of directories or the provision of directory listing information in any way.

Carrier Use And Disclosure Not Affected

Despite earlier drafts of bills that would have mandated additional protection mechanisms for covered entities to implement, the Telephone Records and Privacy Protection Act of 2006 does not alter a telephone carrier’s obligations to protect phone records. These actions continue to be subject to Section 222 of the Communications Act. (The obligations of VoIP providers are subject to some uncertainty at this time given that VoIP services generally have not been classified by the FCC.) Carriers should note that the FCC is expected to release new rules for the protection of CPNI later this month or early next month. These new rules likely will include new procedures for verifying customer identity and may require carriers to implement password-protected systems to prevent unauthorized disclosure of CPNI.

Kelley Drye is actively participating in this proceeding, and we can provide additional information upon request.

² Congressional Record, S11640 (December 8, 2006).