Tough New FCC Rules on Customer Call Records

ROSALIND K. ALLEN

Living in the information age continues to broaden our perspective of how we view ourselves and our place in the world. Telecommunications and information technologies promote data centralization and fluidity, helping us achieve increasing levels of efficiency and productivity. But these dynamic technologies also make data more vulnerable, creating increased opportunities for unauthorized access, use, disclosure, and alteration, as well as accidental loss and deletion. Of particular concern is the apparent ease with which personally identifiable information is collected and shared, often without the subject's knowledge or permission. Federal and state governments have responded with a flurry of data protection and privacy laws. Enabling people to exercise greater control over collection and use of their personally identifiable information is now a well-established consumer priority.

Recent high-profile incidents have focused attention on whether our laws afford adequate and effective protection for personal call records. When private investigators hired by Hewlett-Packard (HP) officials were easily able to identify the source of information leaks by obtaining call records of targeted reporters, privacy of personal call records became a national issue. The HP investigators gained unauthorized access to the personal call records through a practice known as pretexting. Pretexting is the practice of gaining access to an individual's sensitive personal information under false pretenses. For example, the HP investigators impersonated the reporters when they contacted telecommunications companies to get the call records.

The online environment has given rise to an industry of data brokers selling records of phone calls with dates, times, durations, and locations. To draw further attention to the unauthorized marketing of personal information, a blogger randomly contacted an online data broker and purchased General Wesley Clark's mobile phone records for 100 calls made during a three-day period in November 2005.

The legislative response to these revelations was quick and decisive. Congress enacted and the president signed into law the Telephone Records and Privacy Protection Act (TRPPA) of 2006, which criminalizes the practice of fraudulently obtaining another person's phone records, either directly or through the purchase of such information. Approximately twenty-four states have enacted or are proposing to enact antipretexting laws. A number of telecommunications providers have filed suits against numerous entities for fraudulently obtaining phone records.[1] The Federal Trade Commission (FTC) has also prosecuted pretexting to obtain consumer phone records as a deceptive and unfair trade practice under Section 5 of the FTC Act.[2]

In the wake of all these crackdowns on the pretexters, the Federal Communications Commission (FCC or Commission) decided more needed to be done. Section 222 of the Communications Act imposes obligations on telecommunications carriers to protect and control the use of the proprietary information (otherwise known as customer proprietary network information, or CPNI) derived from customers. The FCC already had CPNI rules in place but recently took steps to bolster them. Prompted by the high visibility of the phone record pretexting problem, as well as by a petition filed by the Electronic Privacy Information Center (EPIC) seeking stronger security and authentication standards for accessing CPNI, the Commission initiated a rulemaking proceeding that proposes additional safeguards to protect CPNI from unauthorized access and disclosure.

The FCC issued its revised CPNI rules on April 2, 2007.[3] The new CPNI rules take effect within six months of approval by the Office of Management and Budget. Compliance will require significant changes in the ways telecom providers protect and disclose customer data, as well as how the providers interact with their marketing contractors and joint venture partners. The FCC also broadened the universe of providers subject to Section 222 to include interconnected providers of Voice over Internet Protocol,[4] which will no doubt trigger renewed complaints that legacy regulations are burdening this competitive new market sector. Strict enforcement of the new rules is expected. Because some of the new regulations are overly broad and vague and do not appear to be narrowly tailored solutions that meet identified governmental interests, the new CPNI regime is likely to be challenged.

Call Detail Records

The FCC's new rules are premised on the belief that inadequate protection of CPNI by carriers has directly contributed to pretexting. Accordingly, as a starting point in its analysis, the FCC recognizes a new subset of CPNI, i.e., call detail records (CDR), which comprise the most sensitive types of CPNI. Specifically, CDR

> includes any information that pertains to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.[5]

By way of example, the FCC notes that remaining minutes of monthly use for a wireless customer qualify as CPNI but do not fall within the sensitive CDR category.

Safeguarding Access

Providers are prohibited from disclosing CDR unless specific authentication requirements are followed. First, the provider must establish a password for each customer account by authenticating

Roz Allen (rosalind.allen@hklaw.com) is a partner, specializing in communications and privacy law, in the Washington, D.C., office of Holland & Knight LLP.

Published in Communications Lawyer, Volume 25, Number 1, Spring 2007.

the customer without using "readily available biographical information," such as the last four digits of a customer's Social Security number, mother's maiden name, or date of birth. Accepted methods of authentication include

(1) calling the customer at the telephone number of record for the service purchased. This means that if the customer is purchasing wireless service, the provider must call the customer at the wireless phone number associated with that service, not a home or work number; or
(2) sending the customer a personal identification number (PIN) by voice mail or text message to the telephone number of record, or by mailing the PIN to the address of record for the account. This could be an e-mail address.

If the provider receives a phone call from an individual seeking CDR, the provider cannot disclose the CDR unless the caller shares the preestablished password or PIN with the provider. This requirement is unnecessary if the caller volunteers all of the CDR needed to address a customer service issue during the call. Nonetheless, the provider must limit the discussion of CDR only to that volunteered by the caller and must not disclose any additional CDR without first obtaining a password.

Providers must also require passwords for customers seeking to access CDR through an online customer account. Furthermore, customers have the option of accessing all their CPNI (including CDR) by visiting a provider's retail location and presenting a valid government-issued photo ID that matches the account information.

It is inevitable that customers will forget passwords; therefore, the provider must create a backup method of authentication for use under these circumstances. Although the FCC is not specific about the correct backup method, this secondary form of authentication also cannot involve readily available biographical information or account information. Use of a "shared secret question" (e.g., "What is your favorite color?") chosen by the provider or the customer is suggested as an acceptable form of backup authentication.

Business Customers

It is not uncommon to give business customers the leverage to make sure they get the full range of their telecommunications services needs met. For that reason, if a business customer is assigned a dedicated account representative by the provider and the negotiated service agreement specifically addresses protection of the business's CPNI, the authentication requirements need not be followed. The business customer may, of course, negotiate more stringent authentication procedures that integrate well into the business's enterprisewide information management procedures. This exemption is only limited to the new authentication rules and does not relieve the provider from compliance with all other CPNI requirements.

Notification of Account Changes

Providers must notify customers immediately of significant account changes, such as password changes, online account changes, mailing address changes, or changes to the backup authentication method. This requirement will likely prove to be of significant practical value as an early warning system to consumers because these types of changes are often associated with identity theft. Notification to the customer may be via a voice mail or text message to the telephone number of record, or written notification to the address of record.[6]

Breach Notification

For purposes of CPNI, a breach is viewed as any intentional and unauthorized act of access, use, or disclosure. Timely breach notification is widely viewed as the most important and effective response to a compromise of personally identifiable information because it enables the consumer to minimize resulting damage. Breach notification has also come to define the reasonable standard of care for entities storing personally identifiable information. Approximately thirty-five states have enacted some form of a data breach notification law, and Congress is considering a federal privacy law that would include data breach notification.[7] Making breach notification a legal requirement protects consumers and makes clear that if consumers are not notified of actual (or, under some state laws, potential) data breaches, then those consumers have been injured. Moreover, if an entity storing personally identifiable information promptly reports the breach to affected consumers, data breach laws provide a measure of protection from further allegations of consumer harm. The new FCC rules, however, appear to frame breach notification primarily as a law enforcement tool rather than a means of avoiding customer harm.

Providers are prohibited from disclosing CDR unless specific authentication requirements are followed.

Once a provider establishes that a security breach of CPNI has occurred, both the U.S. Secret Service and the FBI must be notified of the breach within seven business days using an online site developed by the FCC. The customer may be notified of the breach only after seven business days following notification to the federal law enforcement agencies, unless one of the law enforcement agencies decides that customer notification would impede or compromise an ongoing or potential criminal investigation or national security matter. In that event, law enforcement agencies may direct the provider not to notify the customer for an additional period of up to thirty days, subject to extension if the federal law enforcement agency believes it is reasonably necessary. If the provider believes that there is "an extraordinary and urgent need to notify" in order to avoid an immediate harm, then the provider may notify the customer but must also inform the federal law enforcement agencies that notification has occurred.[8] The same approach must be followed whether there is a single incident compromising CPNI or a group of such incidents.

Although two of the FCC commissioners disagreed with the provision that federal law enforcement should be given the discretion to prevent, without explanation, a customer from learning that sensitive, personally identifiable information has been compromised, the new rules do not appear to provide for the FCC or any other third party to independently verify the need to withhold

consumer notification. This aspect of the decision can be directly attributed to a recommendation submitted into the record by the Department of Justice, and it is far from clear whether the implications of notification delay were fully considered.

The FCC also expressly preempts state law requirements that are inconsistent with the new rules.

The FCC does not define the federal law enforcement interest that would justify failure to notify a customer that unauthorized entities are accessing sensitive personal information and potentially allowing continuation of a dangerous activity without the customer's knowledge. Unauthorized access to call records has been associated with stalking and other threatening behavior. Under those circumstances, it is likely the customer is aware of the problem and has contacted the police. If not, warning a customer of an immediate threat to his or her safety would appear to justify the provider's immediate and extraordinary need to notify.

The FCC also expressly preempts state law requirements that are inconsistent with the new rules. This aspect of the FCC's rulemaking order is likely to become a substantial source of confusion and potential litigation. For example, apart from state antipretexting laws, some types of CPNI breaches would also be reportable under state data breach laws. Would the FCC rules preempt state law provisions that require notification of state law enforcement authorities? If federal law enforcement decided to prohibit or delay breach disclosure, would the provider be deemed in violation of state data breach laws that establish deadlines for breach notification? Risk-management considerations will likely cause providers to devote further resources to monitoring state law and establishing reliable procedures for tracking the specifics of each breach. The most efficient and effective way to modify risk management considerations would likely involve adjustments to current procedures for ensuring the security and integrity of the entity's information inventory.

Joint Venture and Third-Party Contractors

The FCC generated controversy with its decision to require an opt-in from customers before providers can share CPNI with joint venture partners or independent contractors for marketing purposes. Current rules allow such sharing unless the customer opts out of CPNI sharing within thirty days of provider notification. The opt-out process can continue to be used for sharing CPNI with provider agents and affiliates to market telecommunications-related services.

Obtaining customer opt-in is extremely difficult, and unless this aspect of the decision is modified or stayed, many providers may decide to reformulate their arrangements with third-party marketing entities into agency agreements. There is reason to believe, however, that the constitutionality of this rule will be challenged.

In *US West, Inc. v. FCC*,[9] the Tenth Circuit held that an opt-in requirement for disclosure of CPNI to joint venture partners and independent contractors violated the First Amendment because the FCC failed to satisfy the *Central Hudson*[10] test for permissible restrictions on commercial speech. *Central Hudson* provides that if commercial speech concerns lawful activity and is not deceptive or misleading, the government may impose restrictions only if

(1) It has a "substantial" state interest in regulating the speech,
(2) The regulation directly and materially advances that interest, and
(3) The regulation is "not more extensive than necessary to serve that interest."[11]

The Tenth Circuit expressed skepticism about the first and second prongs but concluded that even assuming those were satisfied, the opt-in rule was not narrowly tailored and the FCC had failed to show why notification followed by an opportunity to opt out would not be equally effective.

In resurrecting the opt-in proposal in the new CPNI order, the FCC argued that the record of this most recent proceeding differs substantially from prior proceedings and now supports opt-in. That argument might be supportable if the FCC decided to adopt an opt-in rule for CDR only rather than for all CPNI. The record of this proceeding does show that unauthorized disclosure of CDR violates personal privacy and may also facilitate domestic violence or stalking and endanger law enforcement officers, victims of crimes, witnesses, or confidential informants. The governmental interest in preventing unauthorized disclosure of CDR is therefore substantial, and the recent passage of TRPPA further supports that argument.

The Commission's decision, however, to extend opt-in to CPNI that is not CDR is difficult to support. First, as the Commission admits, the record of this new proceeding does not show that sharing of CPNI for marketing purposes with joint venture partners and third-party contractors leads to misappropriation of personal call records. There are no known instances of CPNI being compromised through these types of marketing activities. In fact, the record has little to say about this aspect of CPNI because the stated focus of this proceeding is safeguarding CDR. It appears that the FCC decided to extend opt-in to all CPNI based on an assumption that once CPNI is transferred to joint venture partners and third-party contractors, the provider loses control over the information. Taken as a whole, the record no more supports applying opt-in to CPNI that is not CDR than it did ten years ago.

Whether an opt-in is more extensive than necessary remains somewhat debatable. There is support in the record for measures stronger than the current opt-out but more narrowly tailored than the opt-in, such as use of a password for transferring CPNI to third-party contractors and joint venture partners.

Annual Certification

The FCC emphasizes that all carriers must take "every reasonable precaution" to prevent unauthorized disclosure of CPNI. Carriers are affirmatively on notice that they have not taken sufficient steps to adequately protect CPNI if even a single pretexter obtains unauthorized access to a customer's CPNI. The FCC declined to adopt specific safeguards at this time but indicated that

carriers must do more than comply with the requirements set forth in the new rules. Furthermore, the FCC explicitly rejected adopting a regime equivalent to the Gramm-Leach-Bliley safeguards rule for protection of personal financial information, based on the misperception that this would either insulate the provider from liability or provide pretexters with instructions for circumventing the safeguards. Nonetheless, carriers will be faulted if they do not adopt whatever additional safeguards are "feasible" to detect and prevent pretexting. The further notice for proposed rulemaking accompanying this order does give the FCC an opportunity to comprehensively explore the track record of a safeguards approach in other areas of privacy enforcement.

Carriers are now required to file an annual CPNI certification every March, reporting information for the preceding year. New information for the certification must include

(1) a summary of all customer complaints concerning unauthorized use of CPNI;
(2) a report of each breach, including dates of discovery and notification;
(3) any enforcement measures undertaken against data brokers;
(4) pretexting techniques observed; and
(5) measures taken to protect CPNI.

The enforcement scheme is unusual. Providers are required to detect and report pretexting with the knowledge that the disclosure will always trigger enforcement action.

Conclusion

An analysis of the FCC's new rules for protecting consumer call records strongly suggests that the regulatory scheme will continue to evolve. Apart from the fact that the FCC initiated a further notice of proposed rulemaking that is likely to better define carrier compliance requirements, it is entirely possible that the new rules will be challenged. If federal legislative developments come to fruition, it is also conceivable that the FCC will be required to reexamine its approach to ensure that treatment of CPNI is consistent with overall federal protections accorded personally identifiable information. An important takeaway is that the federal and state focus on protecting personally identifiable information will only expand over time. Many companies have recognized this trend and are undertaking the task of developing an enterprisewide, holistic approach to all information collected, used, and stored during the ordinary course of business. With each new legal development in the area of consumer privacy, adopting clear processes for information handling must be given priority.

Endnotes

1. *See, e.g.,* Cingular Wireless LLC v. Data Find Solutions, Inc., No. 1:05-CV-3269-CC (N.D. Ga. filed Dec. 23, 2005); Sprint Nextel Corp. v. All Star Investigations, Inc., No. 06 01736 (Fla. Cir. Ct. filed Jan. 27, 2006); T-Mobile USA, Inc. v. C.F. Anderson, No. 06-2-04163 (King County Super. Ct. Feb. 2, 2006) (stipulated order and permanent injunction); Cellco P'ship Verizon Wireless v. Data Find Solutions, Inc., No. 06-CV-326 (SRC) (D.N.J. Jan. 31, 2006) (order).

2. *See, e.g.,* Fed. Trade Comm'n v. Info. Search, Inc., No. 1:06-CV-01099-AMD, FTC File No. 062 3102 (N.D. Md. settlement entered Feb. 22, 2007); s*ee also Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act: Hearing Before the H. Comm. on Energy and Commerce,* 109th, 1st Sess. (Mar. 9, 2007) (statement of Lydia Parnes, Director, Consumer Protection, Federal Trade Comm'n).

3. In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information (report and order and further notice of proposed rulemaking), FCC 07–22 (released Apr. 2, 2007). The FCC also adopted a further notice of proposed rulemaking that seeks comment on whether: (1) password requirements should be expanded further; (2) audit trails for CPNI should be established; (3) physical safeguards for transfers of CPNI are necessary; (4) time limits should be imposed on retention of CPNI; and (5) information stored on mobile devices should be subject to controls. Comments were due on July 9, 2007, and reply comments on August 7, 2007. This article will focus solely on the rules actually adopted.

4. An interconnected VoIP service (1) enables real-time, two-way voice communications, (2) requires a broadband connection from the user's location, (3) requires Internet protocol-compatible customer premises equipment, and (4) permits users generally to receive calls that originate on the public switched telephone network (PSTN) and to terminate calls to the PSTN. 47 C.F.R. § 9.3.

5. 47 C.F.R. § 64.2003(d).

6. Such provider notification must be limited to the fact that a change was made and cannot reveal the specifics of that change.

7. On May 3, 2007, several federal privacy laws, including data breach notification provisions, received committee approval in the U.S. Senate: Personal Data Privacy and Security Act of 2007, S. 495 (co-sponsored by Senators Patrick Leahy and Arlen Specter) and Notification of Risk to Personal Data Act of 2007, S. 238, S. 239 (sponsored by Senator Dianne Feinstein).

8. Presumably, if the provider finds out about the breach from the customer, the notification to law enforcement would also explain that the customer knows about the breach.

9. 182 F.3d 1224 (10th Cir. 1999).

10. 447 U.S. 557, 564–65 (1980).

11. *Id.*