

January 26, 2007

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

Notice of Ex Parte Communication in CC Docket No. 96-115, In the Matter of Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information

Dear Ms. Dortch,

On January 19, 2007, Luisa Lancetti, Frank Triveri, and Kent Nakamura of Sprint Nextel Corporation spoke by telephone with Michelle Carey of the office of Chairman Martin, and visited John Branscome of the office of Commissioner Copps to discuss the above-captioned proceeding. The discussion focused on (1) the adverse consequences to the public interest from customers having to give opt-in consent for their CPNI to be used by certain third parties for marketing purposes, and (2) our likely inability to comply immediately with new rules in this area. We also proposed a specific rule that would, unlike opt-in consent, better safeguard the use of CPNI by third parties.

1. Opt-In Consent Does Not Address Pretexting

During those discussions, Sprint Nextel expressed concerns over possible requirements that carriers obtain customers' opt-in consent prior to allowing independent contractors and joint venture partners to access customers' CPNI for marketing purposes. Sprint Nextel explained that an opt-in consent requirement would not address the issue of pretexting, and proposed a specific solution narrowly tailored to meet that problem. Pretexting hinges on a number of variables such as social engineering, trickery, persistence, and carrier security measures. It does not rely on "inside" information from carriers and those associated with a carrier. In fact, pretexters persist without regard to the status of any carrier representative (whether an employee, a joint venture partner, or an independent contractor) or any stated opt-in preference by a customer.

A. An Opt-In Requirement Would Create Unintended Consequences

Sprint Nextel urged the Commission to consider the unintended consequences of an opt-in requirement. For example, customers might no longer be able to receive product and service offerings tailored to their individual needs. Sprint Nextel relies on independent contractors to help tailor such offerings and binds them to strict confidentiality and security obligations. These contractors are also bound by the confidentiality and security obligations of their employer. In many cases these contractors workside-by-side with Sprint Nextel employees, performing valuable analytical, marketing, and customer care services on an as-needed basis. This benefits both carriers and customers with better service, more flexibility and lower costs. For

example, these contractors may help identify customers who would clearly benefit from a cost effective bundle of services (e.g., wireless, local, long-distance, and high-speed Internet). An opt-in requirement could prevent customers from receiving these offers. Such a requirement might also prevent carriers from identifying their most valuable customers, just as airlines do.

Sprint Nextel also explained that many carriers could be competitively disadvantaged by an opt-in requirement. This is especially true of carriers that do not offer all categories of service and which market and offer bundled services through partnering arrangements with other service providers. An opt-in requirement could effectively competitively disadvantage these carriers against carriers that offer all service categories under one roof.

B. Contractual Safeguards Would Better Advance the Government's Interest

Because opt-in consent is unrelated to pretexting and because of the potential unintended consequences of an opt-in requirement, Sprint Nextel proposed an alternative that would directly address any concerns that the Commission may have with respect to joint venture partners and independent contractors. Specifically, Sprint Nextel proposed revising existing Section 64.2007 of the Commission's CPNI Rules (47 C.F.R. § 64.2007) as follows:

Joint Venture/Contractor Safeguards. A telecommunications carrier that discloses or provides access to CPNI to its joint venture partners or independent contractors shall enter into confidentiality agreements with independent contractors or joint venture partners that comply with the following requirements. The confidentiality agreement shall: (A) require that the independent contractor or joint venture partner use the CPNI only for the purpose of marketing or providing the communications-related services for which that CPNI has been provided; (B) disallow the independent contractor or joint venture partner from using, allowing access to, or disclosing the CPNI to any other party, unless required to make such disclosure under force of law; (C) require that the joint venture partner or independent contractor provide its personnel with access to the CPNI only on a need-to-know basis; (D) require that the independent contractor or joint venture partner use administrative, physical, and technical safeguards that are ~~have~~ appropriate ~~protections in place~~ to ensure the ongoing confidentiality and security of consumers' CPNI; and (E) require that the joint venture partner and independent contractor return or destroy the CPNI in its possession at the end of its contractual relationship with the carrier.

This new provision would thus clearly articulate four duties for joint venture partners and independent contractors: (1) a duty not to disclose CPNI, (2) a duty to limit CPNI access to those personnel with a need-to-know such information, (3) an affirmative duty to prevent outsiders from gaining unauthorized access to CPNI, and (4) a duty to return or destroy the CPNI at the end of the relationship with the carrier.

These safeguards would likely avoid the thorny legal issues that an opt-in regime presents under *U.S. West, Inc. v. Federal Communications Commission*, 182 F.3d 1224 (10th Cir. 1999).

2. Compliance Timelines Must Account for Technical Limitations and the Time to Create Technical Capabilities

Sprint Nextel explained that carriers likely cannot comply immediately with new CPNI rules. As Sprint Nextel elaborated, compliance with the proposed CPNI rules cannot be achieved through changes in policies alone. Compliance would likely require carriers and their billing system

providers to (1) write new software; (2) test the software and its impacts on interdependent systems; (3) deploy the software; (4) develop procedures for any new technical capabilities; and (5) train personnel on new software and procedures.

Sprint Nextel used the following example: the Commission is reportedly contemplating requiring carriers to notify customers of any change in their contact and authenticating information. Many customers may make these changes over the phone with Sprint Nextel's customer service department or via Sprint Nextel's website. Notification of these changes could not be achieved through manual procedures given the millions of transactions that would be involved. This is especially true for online transactions, as there is no current means of keeping track of these transactions. Post-change notification would require the development of technical capabilities to enable Sprint Nextel to systematically send notifications via postal mail, text messages, and email. Sprint Nextel is already developing the capabilities to systematically notify its customers of the required changes, but it has consistently explained that it will take months to automate these capabilities.

Similarly, Sprint Nextel is developing a new password regime in anticipation of the upcoming CPNI requirements. The new password regime requires the development of a new interactive voice response mechanism to authenticate customers even before they speak with a customer representative, and the development of a shared-secret regime where customers must supply answers in response to predetermined questions (e.g., "who was your second grade teacher?"). It will take months to complete the development of, and the conversion of customers to, these new capabilities.

Accordingly, Sprint Nextel advocated that the Commission establish a compliance timeframe under which carriers must use good-faith efforts to comply within 12 months and provide an interim six-month report that details level of compliance, outstanding compliance efforts, and estimated time to full compliance. Absent such a timeline, the Commission is likely to be inundated with petitions for waiver and reconsideration.

The attached ex parte filing was sent to Ms. Carey to facilitate the discussion.

Should you have any questions, please contact the undersigned.

Sincerely,

/s/ Kent Nakamura

Kent Nakamura
Vice President and Chief Privacy Officer

Attachment

cc: Michelle Carey
John Branscome

January 22, 2007

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

Notice of Ex Parte Communication in CC Docket No. 96-115, In the Matter of Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information

Dear Ms. Dortch,

On January 19, 2007, Luisa Lancetti, Frank Triveri, and Kent Nakamura of Sprint Nextel Corporation met in separate meetings with Ian Dillner of the office of Commissioner Tate; Barry Ohlsen of the office of Commissioner Adelstein; and John Hunter, Angela Giancarlo, and Melissa Slawson of the office of Commissioner McDowell to discuss the above-captioned proceeding.

During the meeting, Sprint Nextel expressed its concerns over possible requirements that carriers obtain customers' opt-in consent prior to allowing independent contractors and joint venture partners to access customers' CPNI to provide back-office services. Specifically, Sprint Nextel explained that an opt-in consent requirement would:

- Not address the issue of pretexting—a phenomenon that relies on impersonation and not rogue joint-venture partners or independent contractors. Sprint Nextel explained that the record in this proceeding is devoid of evidence showing that an opt-in requirement would prevent pretexting. Consequently, as Sprint Nextel noted, an opt-in requirement would likely be held unconstitutional under *U.S. West, Inc. v. Federal Communications Commission*, 182 F.3d 1224 (10th Cir. 1999). Sprint Nextel further explained that security measures, and not a customer opt-in requirement, are the most effective and cost-beneficial way to advance the government's interest in preventing unauthorized access to CPNI. Accordingly, Sprint Nextel advocated that the Commission focus instead on security measures, such as a requirement to contractually bind carriers' joint venture partners and independent contractors to security obligations, in addition to the confidentiality obligations enumerated in Section 64.2007 of the Commission's Rules (47 C.F.R. § 64.2007).
- Prevent customers from receiving product and service offerings that are tailored to their needs. Sprint Nextel binds its independent contractors to strict confidentiality and security obligations; they perform valuable analytical, marketing, and customer care services that benefit customers with better service, more flexibility and lower costs.
- Potentially put some carriers at a disadvantage by virtue of their business model or corporate structure. Sprint Nextel explained that some carriers (particularly carriers that

do not offer all categories of telecommunications service) market and offer suites of services through partnering arrangements; these carriers may be competitively disadvantaged against carriers that offer all categories of service without reliance on partnering.

- Frustrate customers who want efficient customer service. Sprint Nextel discussed Section 64.2008 of the Commission's Rules (47 C.F.R. § 64.2008) to illustrate how carriers currently obtain opt-in consent. The three pages of rule provisions enumerate exacting procedures that would greatly inconvenience customers.

Sprint Nextel also:

- Expressed concerns that any new rules to combat pretexting might inadvertently affect existing well-established rules and practices concerning a carrier's total service relationship with its customers.
- Requested flexibility in managing any new password and customer notification requirements the Commission might adopt.
- Argued that certain types of customer information, such as the number of minutes remaining in a customer's rate plan in a particular month, did not require the degree of protection of other types of information such as call detail records.
- Reiterated its position that business accounts having dedicated service representatives should not require a passcode before CPNI could be shared and that certain calls whose authenticity was unquestionable should not require a passcode.
- Expressed concern about the likely unintended adverse effects of an overbroad requirement that requires carriers to notify law enforcement of *any* unauthorized access to CPNI. Sprint Nextel stated that the duty to notify law enforcement should focus on apparent or real attempts to circumvent the security of a carrier to gain access to CPNI.

Finally, Sprint Nextel explained that it would take a minimum of 12 months to implement the requirements of new rules. Sprint Nextel elaborated that compliance could not be achieved through policy changes alone; that it would require time to (1) develop software and procedures, (2) test software and system impacts, (3) deploy software, and (4) train personnel on new software and procedures.

Should you have any questions, please contact the undersigned.

Sincerely,

/s/ Kent Nakamura

Kent Nakamura
Vice President and Chief Privacy Officer

cc: Ian Dillner
Barry Ohlsen
John Hunter
Angela Giancarlo
Melissa Slawson