

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996;)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information)	
)	
IP-Enabled Services)	WC Docket No. 04-36

COMMENTS OF SPRINT NEXTEL CORPORATION

Kent Y. Nakamura Frank P. Triveri Anthony M. Alessi Sprint Nextel Corporation 2001 Edmund Halley Drive Reston, VA 20191	Douglas G. Bonner Kathleen Greenan Ramsey Sonnenschein Nath & Rosenthal LLP 1301 K Street, N.W. Suite 600, East Tower Washington, D.C. 20005 (202) 408-6400 Counsel for Sprint Nextel Corporation
--	--

Dated July 9, 2007

SUMMARY

On March 13, 2007 the Commission adopted a comprehensive set of new rules designed to protect customer proprietary network information (“CPNI”). These new rules are scheduled to take effect in December, 2007, and Sprint Nextel, like other telecommunications carriers, is undertaking extensive measures to implement new systems and procedures to comply with the new rules. When considering additional new CPNI and “customer information” protections due to the illicit activities of “data brokers,” the Commission should await full implementation of the recently adopted new rules and take into account carrier and customer experience alike before deciding on any additional carrier requirements. Millions of Sprint Nextel customers and those of other carriers will be greatly affected by the implementation of the new rules. Prematurely imposing additional requirements on carriers may have the unintended effect of undermining the efforts of Sprint Nextel and other carriers to effectively implement the new rules and impose unnecessary additional costs on customers. In brief, the Commission should not rush to impose any additional requirements on carriers, but undertake a measured and thoughtful deliberative process that balances ongoing carrier implementation efforts, additional costs of new regulation, and the carrier-customer relationship against any incremental benefits that might result from imposing additional rules.

Moreover, Sprint Nextel believes that additional mandatory regulation is unnecessary in the following areas where comment is now sought by the Commission: (1) additional CPNI protective measures, such as password protection

for non-call detail CPNI, audit trails, physical safeguards governing the transfer of CPNI, and limitation of data retention; and (2) protection of non-CPNI customer information in mobile communications devices. The burden and cost on the carrier and customer of any such additional rules would far outweigh any possible benefit beyond the protections currently in place under Section 222(a) of the Act and existing Commission Rules, which obligate carriers to protect customer CPNI. In fact, Sprint Nextel has invested significant financial and human resources to protect CPNI on many fronts, and is substantially increasing that investment to implement the Commission's new Rules. Further, additional regulations are not necessary because carriers are implementing aggressive measures on an accelerated basis under the recently adopted rules to protect CPNI. However, should the Commission feel compelled to adopt additional requirements, Sprint Nextel urges the Commission to adopt narrowly tailored regulations that recognize the vast differences that exist in systems, network, and corporate infrastructures, and avoid the diversion of valuable resources toward solutions that are unlikely to provide real benefits in protecting CPNI.

TABLE OF CONTENTS

	<u>Page</u>
I. ADDITIONAL RULES FOR NON-CALL DETAIL RECORD CPNI SHOULD BE UNNECESSARY UPON CARRIER IMPLEMENTATION OF THE NEW CPNI RULES	2
A. Adequate Safeguards Currently Exist To Protect Non-Call Detail Record CPNI Making Further Mandatory Password Protection Unnecessary	6
B. Audit Trails Are of “Limited Value” in Addressing Pretexting and Would Require Costly Generation of Excessive Data Associated with “Legitimate Customer Inquiry”	10
C. Implementation of the New CPNI Rules and the Criminalization of Pretexting Adequately Protect the Transfer of CPNI, Alleviating Any Need for Additional Physical Safeguards.....	12
D. The Commission Should Not Establish New Rules Limiting CPNI Data Retention	14
1. Limiting Data Retention is Unnecessary and will Not Reduce Pretexting	16
2. Limiting Data Retention Will Conflict With Various Federal And State Statutory Limitations Periods.....	17
II. PROTECTION OF CUSTOMER INFORMATION STORED IN MOBILE COMMUNICATIONS DEVICES	19
1. “Customer Information” Stored in Handsets Is Neither CPNI Nor Proprietary Information Protected under Section 222 of the Act ...	19
2. Carriers Already Delete Customer Information from Handsets that are Returned for Recycling, Obviating the Need to Regulate Carriers	21
3. Carriers are Not Positioned to Guarantee the Security of Information Contained On Handsets	22
III. CONCLUSION	23

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act)	CC Docket No. 96-
115		
of 1996;)	
)	
Telecommunications Carriers' Use of Customer)	
Proprietary Network Information and Other)	
Customer Information)	
)	
)	
IP-Enabled Services)	WC Docket No. 04-
36		

COMMENTS OF SPRINT NEXTEL CORPORATION

Sprint Nextel Corporation (“Sprint Nextel”), through its undersigned counsel, respectfully submits its comments to the Commission’s Further Notice of Proposed Rulemaking (“*Further NPRM*”) released on April 2, 2007, in the above-captioned proceedings.¹ Sprint Nextel applauds the Commission’s efforts to ensure the protection of customer proprietary network information (“CPNI”). At the same time, when the Commission acts on the issues raised in the Further NPRM, Sprint Nextel asks that the Commission be sensitive to the “burdens” that new regulatory requirements may impose on carriers, and recognize that additional rules at this time may

¹ *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115 and WC Docket No. 04-36, Notice of Proposed Rulemaking (rel. April 2, 2007).

be of “limited value in ending pretexting.”² In fact, Sprint Nextel believes it best for the Commission to refrain from imposing additional rules until there is full implementation of the recently-adopted CPNI rules. Sprint Nextel values its customers and has a vital interest in ensuring that CPNI is protected from disclosure to unauthorized parties. Sprint Nextel, through its legacy companies,³ has invested a substantial amount of time and resources studying and implementing extensive security measures to protect sensitive customer data, including CPNI. To that end, Sprint Nextel continues to assess how best to improve its protection of sensitive customer data.

I. ADDITIONAL RULES FOR NON-CALL DETAIL RECORD CPNI SHOULD BE UNNECESSARY UPON CARRIER IMPLEMENTATION OF THE NEW CPNI RULES

The Commission has taken aggressive measures in the recently released April 2, 2007, Report and Order (“*Order*”) to respond to the fraudulent practice of “pretexting” to obtain access to customer’s call detail or other private communications records.⁴ These measures impose on carriers

² *Further NPRM* at ¶¶68-72.

³ Sprint Corporation and Nextel Communications, Inc. closed the merger of their two companies, including their various operating entities, in August 2005. The integration of the two companies’ operations, and merger of various Sprint and Nextel operating affiliates, has also continued since August 2005.

⁴ *Order*, ¶1 & n.1. Earlier this year, Congress responded to this problem by making pretexting a crime punishable by fines and imprisonment. Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. §1039).

the following new requirements to secure CPNI: (1) authentication standards for the release of call detail records to customers based on customer-initiated telephone contact, which the Commission concluded presents “an immediate risk to privacy;”⁵ (2) immediate notification of account changes to customers; (3) immediate notification of unauthorized disclosure of CPNI to law enforcement and customers; (4) opt-in consent for disclosure of CPNI to joint venture partners or independent contractors for the purpose of marketing communications-related services; (5) enhanced annual CPNI certification requirements whereby carriers must report individual complaints about CPNI breaches to the Commission; and (6) “reasonable measures” to discover and protect against pretexting, which will be necessary to document in order to rebut an Enforcement Bureau “inference from evidence of unauthorized disclosures of CPNI that reasonable precautions were not taken.”⁶

As Sprint Nextel informed the Commission in its filed comments and numerous *ex parte* presentations in this proceeding, Sprint Nextel supports the Commission’s goal of safeguarding CPNI. Since early 2006, Sprint Nextel has been planning, and is now implementing, a new systems-based platform to unify pre-merger wireless billing and customer service platforms for its

⁵ *Order* at ¶13.

⁶ *Id.*, *see also*, Executive Summary.

approximately 53 million customers. This new wireless customer-service uniform billing platform (Sprint UBP) will substantially enhance Sprint Nextel's existing authentication capabilities to meet the directives of the *Order*. The Sprint UBP will provide the following: (1) phased implementation of passwords and shared-secret authentication (*i.e.* What was your first pet's name?) and a phased elimination of social-security number authentication; (2) auto-generated notification to the customer to confirm account changes; and (3) enhancement of existing audit-tracking capabilities to show all instances where customer service representatives view customer records.⁷ As Sprint Nextel advised in meetings with the Commission, the human and financial resources involved in this deployment are daunting. Following design of the information technology architecture with Sprint Nextel's billing platform vendor (that started in September, 2006), Sprint Nextel began with these essential implementation steps:

- (1) collaborating with the billing system vendor to write the software code;
- (2) testing the new software's capabilities, and its impact on interdependent company systems;
- (3) deploying the software in Sprint Nextel's billing system;
- (4) developing Sprint Nextel procedures for new technical capabilities designed to satisfy the requirements of the new Rules;

⁷ November 1, 2006 *Notice of Ex Parte Communication* by representatives of Sprint Nextel Corporation with the Legal Advisors to Commissioners McDowell, Copps and Tate, Docket No. 96-115 at 1.

- (5) designing a migration plan to convert all customers to the new authentication regime; and
- (6) providing over 130,000 hours of training for 34,000 customer care representatives.⁸

Even with its September 2006 “running start” to develop and deploy its own automated customer authentication technical solution, full deployment is not expected until year-end, 2007, because of the complexity of the implementation process. Additionally, it will take at least until mid-2008 to educate its approximately 53 million existing customers about the Sprint UBP, to migrate them to the Sprint UBP, and to provide new passwords under the new authentication regime.⁹ Therefore, it is important for the Commission to weigh the impact that any additional requirements may have on carrier efforts to first implement the current set of new CPNI rules, in particular the new password protection regime. Indeed the new CPNI rules

⁸ February 12, 2007 *Notice of Ex Parte Communication* by representatives of Sprint Nextel with Commissioner Deborah Tate and Ian Dillner of the Office of Commissioner Tate, and John Hunter of the office of Commissioner McDowell, Docket No. 96-115 at 3-10.

⁹ *Id.* at 3-4, 7 & 10. Sprint Nextel has also proposed that the Commission establish a technical “compliance timeframe” under which carriers would be required to use good-faith efforts to comply within 12 months of the new rules, and provide an interim six-month report detailing their “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” of the new authentication requirements. January 26, 2007 *Notice of Ex Parte Communication in CC Docket No. 96-115* by representatives of Sprint Nextel via telephone communication with Michelle Carey of the Office of Chairman Martin, and a meeting with John Branscome of the Office of Commissioner Copps, at 3.

are comprehensive and robust and thus obviate the need for further regulation, at least until the effectiveness of the new CPNI Rules is gauged.

A. Adequate Safeguards Currently Exist To Protect Non-Call Detail Record CPNI Making Further Mandatory Password Protection Unnecessary

Sprint Nextel supports solutions that improve data security in a manner that addresses the problem of “pretexting” without compromising the quality of the customer’s overall wireless experience. As the Commission states in the *Order*, the release of call detail or call records, which have been the object of fraudulent activities by pretexters and data brokers, are the “immediate risk” to customer privacy.¹⁰ Accordingly, the Commission “. . . limit[ed]...[its] rules to the disclosure of call detail information,” thereby, “narrowly tailor[ing]” its rules “to address the problem of pretexting.”¹¹ With no record of pretexter targeting of non-call detail record (“non-CDR”) CPNI, the Commission’s expansion of its password requirement to non-CDR CPNI would have undermined the Commission’s goal of “narrowly tailor[ing]” its rules, and would have subjected the Commission’s rules to legal challenge. Sprint Nextel believes that the record will continue to show there has been no unauthorized access by pretexters to non-CDR CPNI. Thus, the Commission

¹⁰ *Order*, ¶13.

¹¹ *Id.* at n.46.

should not expand its password requirement to non-CDR CPNI. As explained below, non-CDR CPNI is already adequately protected. In any event, it is beyond the scope of CPNI that the record suggests has been targeted by pretexters.

As a threshold matter, it is important that the Commission appreciate the wide-ranging nature of non-CDR CPNI and the fact that much of this non-CDR CPNI is in very high demand by consumers. Carriers require flexibility to balance the appropriate level of protection for this particular class of CPNI with customer demands for prompt and convenient access to non-CDR CPNI.¹² While the *Further NPRM* does not discuss the range of all non-call detail CPNI, this includes relatively benign categories of CPNI for which carriers must have flexibility in managing security requirements, such as (1) the remaining minutes of use (“MOU”) on a customer’s calling plan;¹³ (2) the financial balance on an account; (3) the customer’s rate plan; and (4) the date and amount of last payment. Sprint Nextel Customer Care receives millions of calls per month from its wireless customers seeking immediate

¹² See, e.g., December 11, 2006 *Notice of Ex Parte Communication* by Sprint Nextel representatives with Michelle Carey of Chairman Martin’s Office; Scott Bergmann and Chris Reichman of Commissioner Adelstein’s Office; Bruce Gottlieb and John Branscome of Commissioner Copps’ Office and Tom Navin, Julie Veach, Marcus Mayer, Adam Kirschenbaum and Melissa Kirkel of the Wireline Competition Bureau, Docket No. 96-115 at 1.

¹³ *Further NPRM* at n.45 (“Remaining minutes of use is an example of CPNI that is not call detail information.”).

access to remaining monthly MOU under the customer's calling plan. Access to this information is allowed from the customer's telephone number of record without use of a password. Further, there is no record of CPNI abuse of this type information. And to the best of Sprint Nextel's knowledge there is no professed interest by pretexters to use this information to the detriment of a customer. Therefore, it would be unnecessary, burdensome, and potentially damaging to the carrier-customer relationship¹⁴ to impose a password requirement on customer access to monthly remaining MOU, as the customer expects ready access to this type of information. Accordingly, the Commission was entirely correct to adopt the following standard for customer authentication for the release of non-call detail CPNI: "*[w]e rely on carriers to determine the authentication method for the release of non-call detail CPNI that is appropriate for the information sought and which adheres to section 222's duty.*"¹⁵ In addition to the pre-existing duty under Section 222(a) of the Communications Act of 1934, as amended, "to protect the confidentiality" of proprietary information, including CPNI, the Commission adopted a rule requiring carriers to "take reasonable measures to discover and protect

¹⁴ See, *id.* at n.49 discussing Verizon Wireless Comments at 9 ("arguing that 'passcodes' can lead to a frustrating experience for customers seeking answers to simple billing questions").

¹⁵ *Id.* at n.50 (emphasis added).

against attempts to gain unauthorized access” to all CPNI.¹⁶ Since this rule applies to all CPNI, the Commission should conclude there is ample protection of non-CDR CPNI, and continue to give carriers the required flexibility to balance customer demand for convenience with the appropriate level of protection needed for a particular form of non-CDR CPNI.

Allowing Sprint Nextel and other carriers flexibility does not mean that Sprint Nextel and other carriers will discount using passwords as an effective method for protecting CPNI and other types of customer information.¹⁷ For example, Sprint Nextel currently requires a customer password for such customer information as (1) address or account changes (even though “subscriber list information” such as customer address and telephone number is not CPNI¹⁸); (2) payment status and payment history; and (3) rate plan information and price plan changes. At the same time, Sprint Nextel recognizes that passwords have limitations and are not a panacea. Independent research confirms, as the Commission has recognized

¹⁶ 47 CFR § 64.2010(a).

¹⁷ To the best of Sprint Nextel’s knowledge, most wireless carriers already require the use of a password for account access via the Web, and many require passwords for other methods of account access as well. These password regimes are presumably created in a manner that considers the needs of the customer, and most importantly, the customer’s need for timely and efficient handling of inquiries.

¹⁸ *See*, 47 U.S.C. § 222(f)(3)(A).

in its *Order*, that consumers find mandatory passwords to be inconvenient.¹⁹ Inevitably, the majority of customers forget their passwords once or more when attempting to access their accounts. Thus, Sprint Nextel urges the Commission not to adopt rules mandating that consumers use a password for access to non-CDR CPNI. Instead, the Commission should allow carriers to tailor the appropriate level of protection to non-CDR CPNI by balancing the sensitivity of the information in question with the convenience to that information demanded by customers.

B. Audit Trails Are of “Limited Value” in Addressing Pretexting and Would Require Costly Generation of Excessive Data Associated with “Legitimate Customer Inquiry”

Although the EPIC Petition recommended that carriers record all instances of access to a customer record, the Commission correctly declined to adopt rules requiring audit trails in its *Order*. While Sprint Nextel believes audit trails are of very limited or no benefit in tracking *customer* contacts, Sprint Nextel will sometimes use an audit trail that documents employee access to a customer account as a means of facilitating internal investigations into how certain fraudulent activity may have taken place.²⁰ However, audit

¹⁹ “The Ponemon Report: Those Pesky Passwords,” Larry Ponemon, *available at* www.csoonline.com/read/030106/ponemon (“Too many and too complicated to remember, passwords make users crazy and incur help desk expense. What should you do about it?”).

²⁰ Sprint Nextel Comments at 11-12.

trails will not help to prevent the unauthorized release of CPNI. For example, an audit trail system that tracks each and every question asked by a customer service representative during the course of an inbound call would not identify a pretexter or prevent one from illegally obtaining CPNI. If a pretexter knows the answers to the authentication questions (whatever they may be), the audit trail indicates only that correct answers were provided during an apparently legitimate transaction.

Pretexter access is the perceived vulnerability that the new authentication measures for CDR CPNI are intended to fix. Under the password/backup authentication and customer notification regime that is now being implemented, the utility of and need for audit trails will diminish. Even now, audit trails appear to be of limited benefit to law enforcement in criminal investigations against pretexters. The audit trail results merely confirm in most cases that the pretexter gave correct answers to the authentication questions. They are, however, of limited value in isolating the pretexting party. This explains why, in Sprint Nextel's experience, law enforcement authorities rarely subpoena audit trails in criminal investigations.

Additionally, the costs involved in implementing extensive audit trails across different systems are considerable, and could substantially outweigh

any benefits of implementation. The Commission has previously recognized, in its *1999 Reconsideration Order*, that requiring carriers to implement audit trails to track all access to CPNI would place too great a burden on carriers:

[T]he *CPNI Order's* electronic audit trail requirement would generate "massive" data storage requirements at great cost. As it is already incumbent upon all carriers to ensure that CPNI is not misused and that our rules requiring the use of CPNI are not violated, we conclude that, on balance, such a potentially costly and burdensome rule does not justify its benefit.²¹

These burdens are further complicated by the fact that the technical requirements of implementing audit trails vary widely among different internal operating systems and applications, many of which are siloed and "hard-wired," thus requiring costly replacement of otherwise effective systems.

Finally, audit trails should not be required because the Commission's CPNI rules already provide adequate safeguards. The rules now enumerate robust and comprehensive requirements on security, access, use, disclosure, due diligence, and certification.²² For these reasons, Sprint Nextel

²¹ *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 171 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, ¶127 (1999).

²² See 47 C.F.R. § 64.2009 (c) & (e).

recommends that the Commission refrain from adopting any new rules requiring audit trails.

C. Implementation of the New CPNI Rules and the Criminalization of Pretexting Adequately Protect the Transfer of CPNI, Alleviating Any Need for Additional Physical Safeguards

In addition to audit trails, the Commission requests comment on whether it should require further physical protections such as encryption when CPNI is transferred or accessed by the carrier, its affiliates, or third parties. Sprint Nextel believes that existing physical safeguards and network security management, combined with the Commission's new rules addressing CPNI access, and the criminalization of pretexting activity, eliminate any need for additional physical safeguards.

Sprint Nextel ensures the security and confidentiality of CPNI when transferring or allowing access to CPNI data through a series of reinforcing safeguards. First, Sprint Nextel restricts access by classifying all CPNI data as "restricted data." Access is only on a "need-to-know" basis. Second, Sprint Nextel has implemented a host of IT security measures to ensure a well-hardened and highly-alarmed defense. For example, all billing system data resides in a Sprint Nextel data center based in the United States and dedicated circuits have been installed between Sprint Nextel and its billing service vendors. Firewalls have been implemented at all points of entry to

the Sprint Nextel network. Tight access controls are in place for the transfer of CDR information from carrier switches to Sprint Nextel's billing vendors. Moreover, intrusion detection systems are maintained at all Internet points of entry, including encryption of user log-in credentials. Sprint Nextel has implemented company-wide procedures requiring management approval for the on-boarding or off-boarding of users, implemented fraud alert and incident response procedures, and required security awareness training for its employees. It has a centralized security department responsible for the oversight of security policy, awareness, and enforcement throughout the company. Sprint Nextel continuously reassesses its technology and processes to ensure that the security of customer data remains robust and state-of-the-art.

The Commission should take note that pretexters generally secure access to CPNI information through "low-tech" social engineering ruses of "front-end" authentication protocols (e.g. customer-service representatives), not by "high-tech" cracking of carrier networks. Therefore, encryption of stored CPNI would not have prevented the pretexting incidents that gave rise to the Commission's Rulemaking. In fact, Sprint Nextel is unaware of any instances of data brokers gaining unfettered access to electronic customer databases. In brief, even if carriers had encrypted all CPNI data stored in

databases, data brokers could still have theoretically gained access to CPNI at the precise point at which it was converted to plain text—the point where a purportedly authorized person or pretexter requested it. Accordingly, encryption would not provide meaningful protection against pretexting attempts.

In addition, enterprise encryption solutions are extremely expensive and would be difficult to implement across Sprint Nextel's different platforms and systems. Furthermore, Sprint Nextel believes financial and personnel resources would be better used to implement, maintain, and upgrade Sprint Nextel's new uniform billing platform and the authentication systems established to comply with the recently adopted CPNI rules.

D. The Commission Should Not Establish New Rules Limiting CPNI Data Retention.

Requiring data deletion or data de-identification after a specified period of time would not prevent or reduce the unauthorized disclosure of CPNI. Data deletion and data de-identification would be most effective against those who seek such information on a large scale, using high-tech means (e.g., hacking). However, as the Commission now knows, the most highly valued CPNI sought by those who illicitly purchase such records²³ is

²³ Bob Sullivan, *Who's Buying Cell Phone Records Online? Cops*, MSNBC (May 1, 2006), <http://www.msnbc.msn.com/id/12534959/>.

what is most recent, and available through low-tech means, like social engineering. Thus, older records diminish in value over time, and more recent records would not in any event be impacted by limits on data retention, unless the Commission required the immediate destruction of CPNI—a requirement that would plainly not serve the public interest.²⁴

In addition, limiting the period of time for retaining CPNI would create conflicts with federal and state laws,²⁵ inhibit law enforcement and other investigative activities,²⁶ frustrate customers who need historical information for customer service, and deny carriers the information they need to defend lawsuits and satisfy tax authorities. Even though it would be more cost-effective to destroy data, thus avoiding the high costs of storage and maintenance, any requirement for data deletion or data de-identification would, in one fell swoop, eviscerate information that is crucial to serving the

²⁴ Missouri PSC Comments at 4; T-Mobile Comments at 17; Cingular Comments at 24; Charter Communications Comments at 30; CTIA Comments at 16.

²⁵ For example, the Commission's existing rules require carriers to retain for a period of *18 months* all records necessary to provide billing information associated with a call, including: name, address, telephone number of caller, telephone number called, date, time and length of call. 47 C.F.R. § 42.6. The same is true under certain state regulations. Ohio Commission Comments at 16 ("In Ohio, telecommunications service providers must maintain customer billing records for 18 months." O.A.C. 4901:1-5-15(E)).

²⁶ United States Department of Justice and Homeland Security Comments ("DOJ/DHS Comments") at 3-4.

public interest. Accordingly, the Commission should not impose CPNI data destruction or de-identification requirements.

1. Limiting Data Retention is Unnecessary and Will Not Reduce Pretexting

Limiting data retention of CPNI, whether through destruction or de-identification, would not reduce pretexting in any appreciable manner. Pretexting is generally a “low-tech” phenomenon, involving social engineering to trick carrier customer-service representatives into providing the most recent call-detail records.²⁷ This means any requirements to destroy CPNI data to eliminate pretexting would be effective only if implemented in a draconian manner: by requiring immediate CPNI data destruction. Yet, immediate destruction of CPNI would harm the public interest. It would deny customers access to their records to satisfy billing inquiries, resolve disputes, and satisfy a host of other customer needs. Accelerated destruction of CPNI would harm law enforcement investigative needs, deny taxing authorities the information they need to perform audits or take other actions, deny carriers the information they need to protect themselves from lawsuits, and potentially conflict with numerous federal and state laws, including the

²⁷ Bob Sullivan, *Who’s Buying Cell Phone Records Online? Cops*, MSNBC (May 1, 2006), <http://www.msnbc.msn.com/id/12534959/>; *see also*, Cingular Comments at 25-26 (in Cingular’s experience, most data brokers focus on the “last 100 calls made or calls within the last 90 days.”).

Commission's own 18-month data retention requirement for telephone toll records.

A rule on CPNI destruction is simply not necessary in light of robust new laws governing CPNI, namely the Commission's new CPNI rules arising from this proceeding, and Congress's enactment of the Telephone Records and Privacy Protection Act of 2006, which criminalizes pretexting.²⁸ Under these new laws, carriers must ensure that only those who are authenticated under a new information-security regime may access customer records. Moreover, pretexters now know that they will be prosecuted if they try to breach that regime. These two factors alone obviate the need for further regulation, which would prove costly and only marginally beneficial.

2. Limiting Data Retention Will Conflict With Various Federal And State Statutory Limitations Periods

There are a host of federal and state laws for which the Commission must account before implementing any CPNI data destruction requirements. State laws would have to be preempted.

Currently, Commission rules impose specific record retention requirements on carriers.²⁹ The record retention requirements require that

²⁸ Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. § 1039).

²⁹ 47 C.F.R. § 42.6

carriers retain for a period of 18 months all records necessary to provide billing information associated with a call: name; address; telephone number of caller; telephone number called; and date, time and length of call.³⁰ Some states require carriers to maintain CDRs for at least an equal period of time.³¹ Businesses retain and manage data to satisfy a host of other legal concerns. Breach-of-contract limitations periods in many states are as much as five years. A carrier thus must maintain customer data to defend contract-based and other suits. Tax audits necessitate CDR or invoice data retention on a years-long schedule. Carriers thus must have access to such historic customer revenue and other data to satisfy the concerns of taxing authorities. Finally, carriers must have access to historical customer data to deliver the assistance that law enforcement needs.

In short, the confluence of so many legitimate and compelling needs—the consumer’s, law enforcement’s, taxing authorities’, and the carriers’—militates against any CPNI data destruction requirements. Sprint Nextel’s data storage policies are carefully scheduled to meet these compelling needs. And they are kept in check by the countervailing need to destroy such

³⁰ *Id.*

³¹ For example, Ohio has a statute requiring telecommunications service providers to maintain customer billing records for 18 months. O.A.C. 4901P1-5-15(E).

information quickly to protect privacy and ensure cost savings, as data storage is a costly practice.

At a minimum, any rules requiring the deletion of customer call records must account for the myriad conflicting requirements to retain records, and the consequent preemption that would be necessary to overcome the many conflicts. Because data destruction requirements would not address pretexting and would undermine clear benefits to the public interest, the Commission should refrain from implementing any such rules.

II. PROTECTION OF CUSTOMER INFORMATION STORED IN MOBILE COMMUNICATIONS DEVICES

The FCC seeks comment on “what steps the [FCC] should take, if any, to secure the privacy of *customer information* stored in mobile communications devices.”³² Wireless carriers are not well-positioned to guarantee the privacy of customer information stored on devices that suppliers manufacture and which are in the physical control and custody of customers. Moreover, carriers cannot determine what information is proprietary. In fact, information in the handset is neither CPNI nor proprietary information protected under section 222 of the Act.

³² *Further NPRM* at ¶72 (emphasis added).

1. “Customer Information” Stored in Handsets Is Neither CPNI Nor Proprietary Information Protected under Section 222 of the Act

The Commission does not define the “customer information” that the Commission believes warrants protection. In fact, all kinds of information may be stored in a customer’s mobile handset: missed calls, outgoing calls and incoming calls (together “call history”); contact names and numbers; music; voice notes; task lists; ring tones; maps; search queries and results; and instant messages. While all of this information may constitute “customer information” of sorts, not all of this information is “confidential.” Most important, none of this information is CPNI. CPNI is defined by statute as follows:

(A) information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the customer-carrier relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. CPNI does not include subscriber list information.³³

In sum, none of the information generated by the customer and stored in the handset is CPNI because (a) it is not available to the carrier by virtue of the carrier/customer relationship; (b) the information is not in possession of

³³ 47 U.S.C. §222(h)(1) (emphasis added).

the carrier; and (c) with the exception of an abbreviated call-history list which the customer may delete, none of the information relates to the “quantity, technical configuration, type, destination, location and amount of use” of the subscribed telecommunications service. Nor does it constitute information that carriers include in their bills to customers.

2. Carriers Already Delete Customer Information from Handsets that are Returned for Recycling, Obviating the Need to Regulate Carriers

Sprint now accepts handsets of all makes from all carriers.³⁴ Sprint then erases the data from those handsets, and in turn recycles or refurbishes them. Depending on the origin of the handset (*e.g.*, manufacturer, model, year, carrier service associated with handset, etc.), Sprint Nextel has various programs in place for disposing of, destroying or refurbishing and recycling the equipment. Each program requires the removal of customer data from the equipment.

³⁴ The New York "Wireless Telephone Recycling" statute, effective January 1, 2007, requires any entity which "provides wireless telephone service" (NY CLS ECL § 27-2301) to "accept, at no charge, up to ten used wireless telephones from any person during the normal business hours of such business...." (NY CLS ECL § 27-2303). Similarly, California's "Cell Phone Recycling Act of 2004," 2204 Cal ALS 891, makes it unlawful for a retailer to sell a cell phone in the state after July 1, 2006, "unless the retailer" has in place a system for "take-back from the consumer of a used cell phone" that (1) either the retailer sold or previously sold to the consumer, or (2) is returned by a consumer who is purchasing a new cell phone from that retailer, "at no cost to that consumer." 2004 Cal ALS 891, § 42494(a)&(b).

The removal of customer data from mobile equipment is accomplished through the use of software developed and produced by equipment manufacturers or other vendors. Sprint Nextel uses the best available software to remove customer data from the mobile device. Sprint Nextel is unaware of any customer complaints about handsets that have been cleaned with this software. However, the removal capabilities are only as effective as the available software. Thus, an absolute requirement imposed on carriers to remove customer information at the customer's request would be unworkable.

Due to the extensive costs associated with on-demand removal of customer information or more onerous removal requirements, a carrier would be forced to consider simply destroying used handsets in accordance with applicable laws, rather than continuing with refurbishing programs that require the removal of customer information. Given carrier efforts to use the best available removal software to clean returned devices, and the recognized environmental benefits of recycling, Sprint urges the Commission to refrain from any requirement that carriers remove customer data from the handset at the customer's request.

3. Carriers are Not Positioned to Guarantee the Security of Information Contained On Handsets

Not all handsets are returned to carriers. Mobile-phone users are not obligated to return their handsets to their carrier at any point in time. They

have various options once finished with their handset. Customers may donate their handsets to charity, give them to friends or family, keep them, sell them online, discard them, or deliver them to a carrier for recycling. Any requirement placed on carriers would thus account for only a fraction of unwanted handsets. Consequently, any Commission regulation that strives to address this issue comprehensively would have to address the vast proliferation of handsets beyond the carrier's control. Anything else, such as carrier-focused regulation, would result in only a partial solution. Thus, should it decide to act in this area, the Commission should avoid regulation that targets carriers.

III. CONCLUSION

The protection of CPNI is a serious issue, and is clearly one for which the telecommunications industry already has strong incentives to self-police. As discussed herein, Sprint Nextel believes that the *Order*, together with the deployment of, and transition of millions of customers to, a new uniform authentication platform, and the criminalization of pretexting activities, sufficiently protect CPNI without additional Commission rules. Given carriers' current systems and network management security regimes, the complexity and variety of carrier billing systems, and customers' demand for convenient access to information, it is best to allow carriers maximum

flexibility in determining the best way to protect against unauthorized access to non-CDR CPNI. Finally, customer information on mobile communications devices is not CPNI, and carriers are not in the best position to guarantee the privacy and security of information contained on these devices. Customers have the manufacturer-supplied tools to delete information on mobile devices. When these mobile devices are returned to Sprint Nextel for recycling or refurbishing, Sprint Nextel uses the best available industry software to clean the devices of customer information before they are re-used.

Respectfully submitted,

Kent Y. Nakamura
Frank P. Triveri
Anthony M. Alessi
Sprint Nextel Corporation
2001 Edmund Halley Drive
Reston, VA 20191

Douglas G. Bonner
Kathleen Greenan Ramsey
Sonnenschein Nath & Rosenthal LLP
1301 K Street, N.W.
Suite 600, East Tower
Washington, D.C. 20005
(202) 408-6400

Counsel for Sprint Nextel
Corporation

Dated July 9, 2007