Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
CTIA Petition for Rulemaking	)	WT Docket No. 01-72
	)	
Establishing Fair Location Information Practices	)	
	)	
	)	

SPRINT PCS COMMENTS

Luisa L. Lancetti
Vice President, PCS Regulatory Affairs
401 9th Street, N.W., Suite 400
Washington, D.C. 20004
202-585-1923

Joseph Assenzo
General Attorney, Sprint PCS
Mailstop: KSOPHI0414-4A426
6160 Sprint Parkway, Building 9
Overland Park, KS 66251
913-762-7728

April 6, 2001

Table of Contents

INTRODUCTION AND SUMMARY……. 3

DISCUSSION…….. 6

I. Rigid, Detailed Privacy Rules Are Inappropriate at This Time, As They Could Needlessly Stifle Development of Robust New Services…. 7

II. Sprint PCS Supports the Fair Information Practices Policies ……. 10

III. A Comprehensive Federal/Global Framework Is Needed for Wireless Location Information …….. 14

A. State Laws Are Not Workable and Must be Preempted ……. 14

B. The Commission's Privacy Authority Appears to be Limited…. 17

IV. A Recommended Course of Action…….. 18

A. Adopt the Fair Information Practices Policies……. 18

B. Preempt State Laws Addressing Wireless Location Information 19

C. Expand the Scope of the CMRS Annual Reports to Include Developments with Wireless Location Information… 20

D. Jointly Host with the FTC a Wireless Location Information Workshop…….. 20

CONCLUSION…… 21

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
CTIA Petition for Rulemaking	)	WT Docket No. 01-72
	)	
Establishing Fair Location Information Practices	)	
	)	
	)	

SPRINT PCS COMMENTS

Sprint Spectrum, L.P., d/b/a Sprint PCS ("Sprint PCS"), submits these comments in support of the Cellular Telecommunications & Internet Association ("CTIA") petition seeking adoption of Fair Information Practices concerning wireless location information.[1] Sprint PCS agrees with the two chief points that CTIA makes in its petition: (1) the subject of wireless location information is sufficiently complex that it should be addressed separately from other customer proprietary network information ("CPNI") issues involving all telecommunications carriers — including providers of landline fixed services for whom the subject of wireless location has no relevance; and (2) the Fair Information Practices policies should apply uniformly to all entities that generate or have access to wireless location information.

Sprint PCS is not convinced, however, that a rulemaking at this time will completely meet the needs of the American public. Consumers will expect that their sensitive location information will be subject a core set of privacy protections *regardless*

[1] *See* CTIA, Petition for a Rulemaking to Establish Fair Location Information Practices, WT Docket No. 01-72 (Nov. 22, 2000)("CTIA Petition"). *See also Public Notice,* WT Docket No. 01-72, DA 01-696 (March 16, 2001).

of the firm (carrier or non-carrier) obtaining access to their information. However, the Commission's jurisdiction is limited to a small subset of firms that will generate or gain access to location information — namely, providers of commercial mobile radio service ("CMRS"), and this authority does not extend to the many non-carrier firms that will gain access to location information.

It is already clear that consumer interests will be met only by adoption of a single set of uniform rules, and that disparate state privacy laws would not meet the needs of the mobile public (even if CMRS carriers could implement a patchwork of different laws) and would have the potential to seriously harm this nascent industry. The Commission must, therefore, preempt state laws concerning the subject of wireless location information.

There is already broad consensus over the privacy standards that should apply to sensitive personal data — the Fair Information Practices policies of notice, consent, access and security. The challenge for governments here and abroad is to find a means to apply these standards uniformly to all entities generating or gaining access to location information, so that consumers have an effective means of redress should any firm contravene these standards.

The immediate question facing the Commission is whether it should adopt rules governing that portion of the location information industry over which it has jurisdiction — namely CMRS providers. Sprint PCS supports the Fair Information Practices standards, and it would, therefore, support incorporation of these policies into Commission rules — notwithstanding the inequities and consumer confusion that might result. But if the Commission takes this step, it must resist the temptation to adopt rigid,

detailed rules, for such rules could easily stifle the natural development of a market in its embryonic stage. And if it takes this step, the Commission must recognize that the job is not finished and will not be finished until all location information handlers are subject to the same set of privacy requirements. The needs of the American public will not be met until a uniform and comprehensive set of privacy policies is in place.

INTRODUCTION AND SUMMARY

The importance of wireless location privacy cannot be understated, and it is becoming one of the most critical issues facing the CMRS industry. The Council of Economic Advisors has concluded that "3G" technology "promises substantial benefits to consumers, producers, and the economy as a whole."[2] 3G-based applications will achieve these benefits only if consumers are assured that handset-based transactions are secure and that their privacy is not infringed upon. As CTIA correctly notes, "privacy concerns regarding location information must be addressed if new services and applications are to be accepted by consumers."[3] In a real sense, the very success of 3G will depend in large part on the location privacy practices that carriers and other location information handlers implement.

---

[2] Council of Economic Advisors, "The Economic Impact of Third-Generation Wireless Technology," at 1 (Oct. 2000)("The annual consumer benefit from today's wireless telephone services is estimated at $53-$111 billion. The consumer benefits from 3G services will likely be of this order of magnitude.") The CMRS industry is poised to spend billions implementing this new technology so that these benefits can be realized. For example, Sprint PCS has already announced it, alone, will spend over $700 million by the end of next year to increase data rates tenfold (from 14.4 kbps to 144 kbps) and to double its voice capacity. *See* Sprint PCS Press Release, "Sprint Leads Evolution to 3G with Nation's Clearest, Fastest, and Most Economical Migration Strategy" (March 20, 2001). Sprint PCS will be introducing even more advanced capabilities, with data rates of 3 Mbps to 5 Mbps available beginning in 2004. *See id.*

[3] CTIA Petition at 5.

This Commission, unquestionably, has an important role to play in the location privacy debate, given its expertise with mobile services and its responsibilities over CPNI. Congress has, moreover, charged the Commission with the responsibility of facilitating the development of new and innovative advanced services,[4] and it can discharge this responsibility in the context of wireless location-based services by proactively preempting state law in this area. As discussed below, a patchwork of disparate state laws would stifle industry from introducing new services and inhibit consumers from benefiting by these services.

Sprint PCS supports Commission confirmation of the Fair Information Practices policies (notice, consent, access and security) — whether by rule or *via* a policy statement. However, for two reasons, Sprint PCS submits that the Commission must resist the temptation to adopt new detailed regulations at this time.

First, the provision of location-based services is at an embryonic stage. It would be foolhardy for anyone (service provider or regulator) to predict today with confidence what location-based services the public will, or will not, find of value — and it is impossible to predict what level of privacy protections the public will demand or need with these location-based services. The premature adoption of rigid, detailed government rules could easily stifle the development of an entirely new market, either by precluding the introduction of certain new services altogether or by preventing the public from receiving desired services in the manner they deem most appropriate.

Thus, while Sprint PCS supports Commission adoption of privacy principles — specifically, the Fair Information Practices policies — it should resist the temptation to

[4] *See* Section 706 of the Telecommunications Act of 1996.

adopt rigid rules that would remove the flexibility carriers need in order to develop innovative new services, to gauge customer acceptance of those services, and to determine the level of privacy protections customers want with their services. It is important to remember that the CMRS market is robustly competitive and that the cost to acquire new customers is high. CMRS carriers, therefore, have powerful incentives to match their privacy protections to meet the needs and demands of their customers.

Second, the Commission must recognize that it lacks authority to regulate most entities that will generate or gain access to wireless location information. The Commission's jurisdiction over CPNI is limited to "telecommunications carriers," but most of the entities that will have access to wireless location information will be non-carrier third parties. Consumers are entitled to expect that *all* persons or firms with access to their sensitive wireless location information be subject to a core, uniform set of privacy protections — regardless of whether the person is classified for regulatory purposes as a carrier or a non-carrier.

Recommendations. Sprint PCS recommends that the Commission take four steps at this time:

1. Adopt the Fair Information Practices policies, whether as rule guidelines or by a policy statement, but resist the temptation to adopt detailed rules;

2. Preempt all state laws addressing wireless location information;

3. Include development of location-based services and associated privacy practices in the annual CMRS reports as a way to monitor the development of this nascent industry; and

4. Host a wireless location workshop, perhaps jointly with the Federal Trade Commission ("FTC"), both to take advantage of the work that the industry has already undertaken on this subject and to investigate ways for uniform standards to apply to all information handlers.

DISCUSSION

Sprint PCS is committed to protecting the privacy interests of its customers, and it has devoted considerable resources to learn more about this important subject in the context of location-based services.[5] Three points have become clear from Sprint PCS' investigation. First, the subject is extraordinarily complex. Location privacy, of course, impacts consumers directly. But location privacy also impacts service providers, manufacturers, applications developers, merchants, standards bodies, privacy groups, and government regulators/legislators. Location privacy has relevance for both the voice and data services. The market may develop in unforeseen ways. For example, Sprint PCS initially assumed that it would be able to control the release of its customers' location information to third parties and that in performing a "gateway" function, it would be able to provide an additional level of privacy protections to its customers. However, recent developments suggest that wireless location information may be generated by third parties entirely outside the network of a customer's serving carrier — and that non-carrier firms may control the "gateway."

Second, it is already clear that states should have no role in the adoption of rules governing the privacy afforded to wireless location information. State laws are not workable, either for carriers (which have built networks based on multi-state regional

[5] For example, Sprint PCS employees participated on panels at the recent FTC workshop. *See* FTC, "The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues" (Dec. 11-12, 2000), www.ftc.gov/bcp/workshops/wireless/index.html. They have also been active in international fora, such as the WAP Forum, and it was Sprint PCS that recently recommended formation of a Privacy Expert Group within the WAP Forum. Sprint PCS envisions that the PEG would address the issues that privacy concerns raise and act as a liaison to disseminate privacy-related information and requirements within the WAP Forum and other industry groups. The PEG could not engage in developing or implementing privacy standards, but it would rather research existing privacy frameworks and protocols and their associated regulatory impacts (*e.g.*, FCC and FTC in the U.S., ED Data Directives).

markets), or for consumers (who expect to receive, regardless of where they may travel, a uniform set of privacy protections and a uniform set of services). The Commission could adopt national rules, but they would extend only to wireless carriers and not to the hundreds of entities that will have access to location information. Even if there was a super federal agency with the requisite authority to adopt national rules applicable to all location handlers in the U.S., there remains the issue over the rules governing servers located in foreign countries that may access location information of U.S. citizens.

Third, and finally, the premature adoption of government rules could easily have the unintended effect of stifling and distorting the natural development of a market that is in only its embryonic stage. Adoption of a disparate set of rules — one set applicable to carriers and another set (or worse, no rules) applicable to non-carriers — could also destroy consumer confidence in a technology that has considerable promise. Detailed government rules are not needed at this time because CMRS carriers have strong incentives to implement privacy policies that meet customer needs (because they will not subscribe to location-based or other 3G services unless they are confident that their transactions are secure and that their privacy is not infringed upon).

The subject of wireless location information certainly deserves the Commission's attention. But, the Commission must proceed cautiously and act judiciously. And, it must recognize that it does not, today, have the tools to address the subject comprehensively.

I. Rigid, Detailed Privacy Rules Are Inappropriate at This Time, As They Could Needlessly Stifle Development of Robust New Services

The challenge Sprint PCS (and other service providers) face with the subject of location privacy is that location-based services are so new that no one knows what

services will succeed in the market, much less what privacy protections customers will want with such services. Consumers may also determine that they want different levels of privacy protection for the different levels of location information. Service providers will need time to test and explore new arrangements with customers — and an important component of this evaluation will be a determination of the level of privacy protections customers want attached to particular services.

Sprint PCS has decided that the best practice for it and its customers to use initially is a confirmed "opt-in" consent procedure — namely, Sprint PCS will require customers to provide a proactive authorization before it will provide to any third-party any information identifying a customer's location. Sprint PCS will use this opt-in procedure for all three levels of location information: (1) "precise" location (GPS-aided handsets); (2) "area" location (cell site/sector information); and (3) "presence" information (whether phone is turned on).[6]

Congress amended the Communications Act in 1999 by expanding the CPNI definition to include wireless location information and to preclude disclosure of, or access to, wireless location information "without the express prior authorization of the customer" — but this statutory obligation extends only to telecommunications carriers.[7] Customer authorization can be obtained using a variety of means, including written, oral,

[6] "Presence" information is useful for such services as instant messaging. Technically, presence information does not constitute location information because the information does not divulge one's location, but only whether one is "on" the network at a particular point in time. However, presence information is sufficiently similar to location information that Sprint PCS finds it useful to consider the subjects together.

[7] *See* 47 U.S.C. § 222(f) and (h)(1)(A). There are several exceptions to the requirement of express authorization, such as the provision of location information to emergency personnel in a time of an emergency. *See id.* at ¶ 222(d)(4).

or electronic (*e.g.*, email, Internet). Customer consent can also be obtained using either notice/opt-in or notice/opt-out procedures.

In choosing to use an opt-in procedure for itself, Sprint PCS does not mean to suggest that an opt-out procedure inadequately protects consumer privacy interests.[8] To the contrary, Congress recently determined that a notice/opt-out procedure is an acceptable way to protect consumer privacy interests in their sensitive financial records.[9] Ensuing market experience may reveal that consumers find opt-in procedures unreasonably interfere with their ability to timely obtain and use certain desired services.

Choosing one consent procedure over another is not a decision this Commission (or any other regulator) needs to, or should, make — at least at this point in time. The CMRS market is robustly competitive, with 70% of all Americans having a choice of five or more service providers.[10] Mobile customers can, and do, switch serving carriers easily.[11] The high cost of acquiring new customers gives carriers ample incentive to listen to their customers' needs and preferences.[12] A carrier will not succeed in a

---

[8] Indeed, subsequent, real-world market experience may reveal that consumers find that opt-in procedures for all of their location information may not meet their needs.

[9] For example, in the 1999 Gramm-Leach-Bliley Act, Congress chose to use an opt-out procedure for sensitive financial and other nonpublic personal information. *See* 15 U.S.C. § 6802. Similarly the FCC, historically, used opt-out procedures for residential and small business CPNI, but it then reversed course in 1998 by imposing an opt-in requirement. *See CPNI Order,* 13 FCC Rcd 8061 (1998). However, the next year the 10th Circuit vacated the FCC new opt-in procedures because they impermissibly infringed upon the First Amendment. *See U S WEST* v. *FCC,* 192 F.3d 1224 (10th Cir. 1999), *cert. denied,* 120 S. Ct. 2215 (2000).

[10] *See Fifth Annual CMRS Report,* 15 FCC Rcd 17660, 17664-66 (2000).

[11] *See CTIA LNP Forbearance Order,* 14 FCC Rcd 3092 at ¶ 22 (1999)("[T]he high incidence of switching between wireless carriers (popularly referred to as 'churn') indicates that many wireless customers easily and routinely switch from one carrier to another.").

[12] *See telel.com,* "Verizon Looks Beyond the Horizon – New Incentives Aim at Holding onto Subscribers" (Oct. 2, 2000)(Cahners In-State Group estimates CMRS customer acquisition costs of "around $250"); *Radio Communications Report,* "Wireless Carriers Take New Approaches to Reducing Churn," at 18 (Aug. 28, 2000)(Strategy Analytics estimates CMRS customer

competitive market (*i.e.*, retain current customers and acquire new ones) if its customer care practices generally, or its privacy protection policies in particular, do not match the needs of its customers.

Given the nascent stage of this new market, it would be foolhardy for anyone (carrier or regulator) to predict today, with confidence, what privacy protections the public will demand with location-based services that have not even been developed and introduced in the market. Real world experience may reveal that Sprint PCS' initial privacy policies are too conservative; on the other hand, a service provider utilizing a different approach at service commencement may discover that its customers do not deem the procedures sufficiently comprehensive.

Carriers have every incentive to listen carefully to what their customers want. The premature adoption of rigid, detailed government rules could easily stifle and distort the development of an entirely new market, either by precluding the introduction of new services altogether or by preventing the consuming public from receiving desired services in the manner they deem most appropriate.

II. Sprint PCS Supports the Fair Information Practices Policies

Consensus around a set of "fair information practices" principles has developed over the years among service providers, privacy organizations, and regulators.[13] Sprint PCS supports these principles, and believes, that they should form the basis for a minimal set of privacy protections available to *all* mobile consumers and should be applicable to

---

acquisition of $350); *Miami Herald*, "BellSouth's New Wireless Plan Allows Customers to Roll Over Unused Minutes" (May 20, 2000)(Current Analysis estimates customer acquisition costs of $300).

[13] The Federal Trade Commission recently set down these principles. *See* FTC, "Privacy Online: A Report to Congress" (June 1998).

all entities that generate, access, or use wireless location information — carriers and non-carriers alike. Sprint PCS also supports Commission adoption of these principles — so long as the Commission understands that any guidelines it adopts would not cover non-carrier location information users and that, as a result, new guidelines would not meet the public need for uniform requirements applicable to all service providers.

A. *Notice/Awareness*. Data users and collectors must disclose their information practices *before* they use or collect personal information from consumers. Notice is the most fundamental of all principles because, without notice, a consumer cannot make an informed decision as to whether (and to what extent) to disclose personal information. In addition, the other principles discussed below are meaningful only when a consumer has notice of a firm's policies, and his or her rights with respect thereto.

As CTIA notes, notice can take many forms, including service contracts, web sites, bill inserts, or firm/consumer correspondence (*e.g.,* letters, email). It is inappropriate for the government to micromanage details of the notice so long as the notice is (1) clear and conspicuous, (2) easily accessible (*e.g.,* available on a web site's home page), and (3) reasonably and accurately describes how the person's information (*e.g.,* location information) would be used with consent.

B. *Choice/Consent*. Congress has determined that telecommunications carriers may share wireless location information only with a customer's "express authorization." (Currently, there are no statutory requirements on non-carrier firms accessing location information.) As CTIA notes, this authorization may be written, oral, or electronic, and may even be implicit in certain transactions (*e.g.,* concierge services). Choice means giving consumers options as to how any personal information collected may be shared —

specifically regarding secondary uses of the information beyond those necessary to complete the contemplated transaction (*e.g.*, sale of information to third-parties).

As noted above, two types of choice/consent procedures are available: (1) opt-in (requiring a consumer to take affirmative steps to allow the use and/or collection of the information); and (2) opt-out (requiring affirmative steps to prevent the use and/or collection of the information). It is inappropriate for the government to select one procedure over another, given that the CMRS market is robustly competitive and that carriers have every incentive to listen to the preferences of their customers. Just as important – basic privacy protections must be extended to non-carrier entities that access sensitive location information.

C. *Access/Participation*. Access ordinarily refers to a person's ability both to access data about him or herself (*e.g.*, view the data in a firm's files), and to contest that data. As CTIA notes in its petition, in the context of wireless location information, the access/participation principle does not mean that CMRS carriers must record and store information about a person's location over a period of time. Rather, in this context, the access/participation principle ordinarily means only that a customer can access his or her location preferences (*e.g.*, default settings) currently utilized by the data collector and change those decisions to reflect the person's current requirements. The role of government under the access/participation principle is to ensure that consumers have a right to access their data and that a customer can change his or her preferences easily and timely.

D. *Integrity/Security*. This principle means that the data user/collector must take reasonable steps to protect the sensitive data — both from unauthorized access by third parties and unauthorized disclosure to third parties. The government need not legislate in this area so long as consumers have an effective means of redress if a data user/collector breaches its obligation to maintain the integrity and security of personal information.

E. *Enforcement/Redress*. The privacy principles discussed above can be effective only if there is a mechanism to enforce them. The Commission could adopt rules incorporating the principles discussed above, in which case, consumers could file complaints under Section 208 of the Communications Act. But as discussed herein, FCC rules would apply only to telecommunications carriers, leaving consumers without redress with the thousands of non-carrier firms that may generate, access and/or collect location information. It is for this reason that Sprint PCS favors a national/global solution whereby uniform requirements would be imposed on all information users or collectors, and consumers would have one set of enforcement remedies that they could invoke, regardless of how the data user/collector is classified for regulatory purposes and regardless of where the data user/collector happens to be located.

As noted above, Sprint PCS is not opposed *per se* to the Commission's incorporation of the fair information practices policies into its rules — so long as the Commission does not attempt to micromanage this one small subset of the new location industry. Sprint PCS submits that the Commission's near term resources are better spent gaining an understanding of the complexities of this subject and finding a solution that will meet the need of the American public — a uniform set of privacy principles applicable to all persons or entities that may gain access to sensitive location information.

III. A Comprehensive Federal/Global Framework Is Needed for Wireless Location Information

A patchwork of disparate laws will not benefit applications developers, network operators, or consumers. Besides, the geography of a customer or an applications server or the regulatory classification of the service provider have little relevance to the level of privacy protections that should be available. There is a real need for a set of simple, easily understood uniform rules, and this need will be met only if (a) states are prevented from adopting an inconsistent set of rules and (b) a comprehensive federal (preferably, global) privacy framework is established that applies to all entities generating or gaining access to wireless location information.

A. State Laws Are Not Workable and Must Be Preempted

The most important step the Commission can take at this point in time is to preempt states from regulating wireless location information practices. A patchwork of state laws will preclude industry from determining through trial and error the right mix of services and privacy protections, and disparate state laws will undermine the consumer expectation of a uniform set of services and set of privacy protections regardless of where they may travel. The Commission has the authority to preempt state law,[14] and it must exercise this authority with respect to the privacy rights available to mobile customers — including the use or disclosure of wireless location information.

Some states are considering legislation that would prohibit carriers from even offering location-based services to their customers. For example, H.B. 3345, introduced in the Oregon Legislature last month, would prohibit CMRS carriers from disclosing

location information except to 911 and law enforcement authorities.[15] Such state laws constitute entry regulation that the Communications Act expressly prohibits.[16] Just as important – such laws would undermine the strong federal policy of promoting new technologies so carriers can offer new services to consumers that will improve their lives and enhance our nation's productivity and economy.[17] And, such bills completely ignore the practical reality that, in most instances, CMRS carriers could not possibly comply with state-specific laws.

The Commission must preempt state laws that are not only inconsistent with federal law, but also those that attempt to impose different (*e.g.,* more limiting) requirements on CMRS carriers or consumers. State laws addressing the privacy of mobile customers are not workable given that mobile services, "by their nature, operate without regard to state lines as an integral part of the national telecommunications infrastructure."[18] CMRS carriers build networks to markets, not to geopolitical boundaries, and there are numerous instances where network equipment (*e.g.,* switches, base stations) serve customers in multiple states. National carriers have developed national billing and customer care systems and it is not practical to train thousands of

---

[14] *See, e.g., California* v. *FCC,* 39 F.3d 919, 932 (9th Cir. 1994, *cert. denied,* 115 S. Ct. 1427 (1995) (affirming FCC's preemption authority over CPNI rules); *Southwestern Bell* v. *Texas PUC,* 812 F. Supp. 706 (W.D. Tex. 1993)(same).

[15] Section 2(1) of H.B. 3345 provides, in pertinent part, that "a person providing cellular telephone service may not disclose the location of a cellular telephone to any other person."

[16] *See* 47 U.S.C. § 332(c)(3)(A)("[N]o State or local government shall have any authority to regulate the entry of . . . any commercial mobile service.").

[17] *See, e.g.,* 47 U.S.C. § 157; Section 706 of the Telecommunications Act of 1996; The White House, Memorandum for the Heads of Executive Departments and Agencies, "Advanced Mobile Communications/Third Generation Wireless Systems" (Oct. 13, 2000).

[18] H.R. Rep. No.103-11, 103d Cong., 1st Sess. 260 (1993). *See also Universal Service Reconsideration Order,* 13 FCC Rcd 21252, 21270 ¶ 32 ("[M]any wireless telecommunications providers operate without regard to state boundaries.").

employees to use up to 50 different "scripts" or notice/consent requirements based upon "applicable" state law. Indeed, defining "applicable" state law is itself a major challenge. Is the "applicable" state law the law where the mobile telephone number is rated, the law of the customer's billing address, the law where the customer is located at the time of the call (assuming this information can even be discerned), or the law where the particular server is located?

The traveling public expects that their mobile service will work the same regardless of where they may travel. Customers will be confused if they encounter different notice or consent screens as they travel from one jurisdiction to another, and they will be, understandably, upset if they cannot obtain desired services in certain areas because of peculiar requirements adopted by certain states.[19] In the end, the interests of mobile consumers will be met only if there is one set of rules nationwide, and only if that set of rules applies to all persons or entities that may have access to their wireless location information.

The Commission must understand that its failure to preempt will effectively empower one state (or a handful of states) to establish the *de facto* national privacy policy applicable to all wireless location information. Given the way CMRS networks are built and operated (multistate regions), the administrative burdens and jurisdictional questions, CMRS carriers may, as a practical matter, have no choice but to adopt, nationwide, the requirements of the state adopting the most stringent standards. No one state should have the right or authority to establish national policy — especially where, as here, Congress

[19] For example, assume a state imposes a requirement that consent is only valid if the customer receives prior notice in writing (as is being currently proposed in Minnesota S.F. No. 565). Will a customer from another state be able to receive his desired location-based services while traveling in Minnesota if a customer's original consent was not based on written notice?

established the Commission precisely to establish a nationwide telecommunications policy.

B. The Commission's Privacy Authority Appears to be Limited

The FCC has authority to adopt rules governing the use and disclosure of wireless location information, but its rules would be limited to telecommunications carriers,[20] while most location-based services will be provided by third-party service providers. The Commission could presumably require carriers to include certain privacy protections in their contracts with third-party providers, but what enforcement mechanism will consumers have if a non-carrier breaches its contract obligations and impermissibly uses or discloses the location information? And what about third parties with which a carrier has no contractual arrangement that nevertheless come into possession of certain location information?

There are market developments that, if implemented, may inhibit the ability of carriers to assist their customers in protecting the privacy of their sensitive information. For example, several major handset vendors have suggested that handsets be capable of retrieving location information from the carrier's network and then forwarding this information to third party application providers while bypassing the carrier's privacy gateway.[21] Other firms are proposing to generate location information completely outside the network of the customer's serving CMRS carrier.[22]

---

[20] The FCC's authority would be based on the CPNI statute, 47 U.S.C. § 222, but this statute applies only to "telecommunications carriers."

[21] *See* Location Inter-operability Forum, www.locationforum.org.

[22] *See, e.g.,* www.timesthree.com.

The Commission must exercise care in adopting privacy rules for telecommunications carriers when those rules will not apply to non-carriers engaging in identical conduct. Adoption of rules with disparate application will not serve the public's need, and may, in fact, give the public the erroneous impression that privacy rules applicable to carriers also apply to non-carrier handlers of the same information. Adoption of rules with disparate application could also distort competition, if carriers are precluded from engaging in the same experimentation that other non-carrier firms will undoubtedly engage in.

IV. A Recommended Course of Action

Sprint PCS recommends that the Commission take four steps at this time:

A. Step No. 1: Adopt the Fair Information Practices Policies

Sprint PCS supports Commission confirmation of the Fair Information Practices policies, although it should consider using the medium of a more flexible policy statement rather than rigid rules. While the Commission's jurisdiction is severely limited, there is general consensus that the Fair Information Practices constitute a core set of privacy protections that should be available to all consumers and applicable to all service providers. Commission adoption of the Fair Information Practices policies may help spur adoption of similar policies applicable to non-carrier firms that will generate or gain access to wireless location information.

Nevertheless, the Commission must proceed judiciously, lest it give the American public the false impression that new privacy policies or rules applicable to CMRS carriers only will protect, fully, their privacy interests. And, at this time, the Commission should not adopt detailed rules because such rules are unnecessary (given market incentives) and

because premature adoption of government rules could distort the development of new markets.

B. Step No. 2: Preempt State Laws Addressing Wireless Location Information

Sprint PCS next recommends that the Commission preempt all state laws addressing wireless location information. CMRS carriers have built their networks not around state boundaries, but around markets to match mobile customer use of these networks, and it is doubtful that CMRS carriers could even implement disparate state laws. As importantly (and assuming CMRS carriers could implement inconsistent state laws), disparate state laws will undermine the consumer expectation of a uniform set of services and associated set of privacy protections regardless of where they may travel. Customers will be confused if they encounter different notice and consent screens as they travel from one jurisdiction to another, and they will be, understandably, upset if they cannot obtain desired services in certain areas because of peculiar requirements adopted in certain states.

In the end, the interests of mobile customers will be met only if there is one set of privacy rules nationwide and only if that set of rules encompasses all persons or entities that may generate or gain access to their wireless location information. Indeed, there is a substantial question whether even national rules are sufficient, since location information may be easily stored or processed in servers located in other countries.

C. Step No. 3: Expand the Scope of the CMRS Annual Reports to Include Developments with Wireless Location Information

Congress has required the Commission to prepare annual reports reviewing market conditions in the CMRS market. The Commission should expand the scope of these reports to include developments with located-based services and the privacy practices used with such services. Including this information will not only educate the Commission and the public on an important subject, but these reports will also help identify whether a problem is arising and whether that problem could be addressed by additional government intervention.

D. Step No. 4: Jointly Host with the FTC a Wireless Location Information Workshop

International industry groups such as the WAP Forum and the World Wide Web Consortium ("W3C") have already spent considerable time and attention on the subjects of wireless location and associated privacy protections. The Commission should take advantage of this work product, especially since we live in a global economy and since information can flow so easily from one country to another. A workshop, hosted jointly by the FCC and FTC, would enable federal regulators and other interested parties (*e.g.*, privacy organizations, state attorneys general offices) to better understand the issues and, with industry, to determine whether global developments will meet the needs of the American consumer.

CONCLUSION

For the foregoing reasons, Sprint PCS respectfully requests that the Commission take actions consistent with the proposals discussed above.

Respectfully submitted,

SPRINT SPECTRUM, L.P., d/b/a Sprint PCS

/s/Luisa L. Lancetti
Luisa L. Lancetti
Vice President, PCS Regulatory Affairs
401 9th Street, N.W., Suite 400
Washington, D.C. 20004
202-585-1923

Joseph Assenzo
General Attorney, Sprint PCS
Mailstop: KSOPHI0414-4A426
6160 Sprint Parkway, Building 9
Overland Park, KS 66251
913-762-7728

Its Attorneys

April 6, 2001

CERTIFICATE OF SERVICE

I, Anthony Traini, hereby certify on that on this **6TH DAY OF APRIL 2001**, I served a copy of the foregoing **SPRINT PCS COMMENTS** by U.S. first-class mail, or by hand delivery as indicated with an *, to the following persons:

*ITS
1231 20th Street, N.W.
Washington, DC 20036

CTIA
1250 Connecticut Ave, NW
Suite 800
Washington, DC 20036

*Peter Tenhula, Legal Advisor
Office of Chairman Powell
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

*Mark Schneider, Senior Legal Advisor
Office of Commissioner Ness
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

*Adam Krinsky, Legal Advisor
Office of Commissioner Tristani
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

*Bryan Tramont, Legal Advisor
Office of Commissioner Furchtgott-Roth
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

*James J. Sugrue, Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th Street, S.W., Room 3C-207
Washington, DC 20554

*James D. Schlichting, Deputy Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

National Association of Attorneys General
Lynne Ross, Directory
Carla J. Stovall, President
750 First Street, NE, Suite 1100
Washington, DC 20002

Paula Bruening
Staff Counsel
Center for Democracy and Technology
1634 Eye Street NW, Suite 1100
Washington, DC 20006

Evan Hendricks
Editor & Publisher
Privacy Times
P.O. Box 21501
Washington, D.C. 20009

Ari Schwartz
Policy Analyst
Center for Democracy and Technology
1634 Eye Street NW, Suite 1100
Washington, DC 20006

Richard M. Smith
Chief Technology Officer
Privacy Foundation
Mary Reed Building
2199 S. University Blvd.
Denver, CO 80208

Marc LeMaitre
Director of Technology Strategy
Nextel Communications
Corporate Headquarters
2001 Edmund Halley Dr.
Reston, Virginia 20191

Daniel J. Weitzner
Director of Technology and Society Activities
World Wide Web Consortium (W3C)
MIT Laboratory for Computer Science
200 Technology Square
Room NE43-358
Cambridge, MA 02139

National Association of Reg. Utility Comsrs.
1101 Vermont Avenue NW
Suite 200
Washington, DC 20005

Stacy A. Feuer
Bureau of Consumer Protection
Federal Trade Commission
601 Pennsylvania Avenue NW
Room S-4112
Washington DC 20580

/s/ Anthony Traini
Anthony Traini