

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

In the Matter of	)	
	)	
Petition of the Cellular Telecommunications	)	WT Docket No. 01-72
Industry Association for a Rulemaking to Establish	)	DA-01-696
Fair Location Information Practices	)	
	)	

**REPLY COMMENTS OF THE**  
**CENTER FOR DEMOCRACY AND**  
**TECHNOLOGY**

James X. Dempsey  
Center for Democracy & Technology  
1634 Eye Street NW, Suite 1100  
Washington, DC 20006  
(202) 637-9800  
[www.cdt.org](http://www.cdt.org)

Deirdre Mulligan  
Christopher K. Ridder  
Eddan Katz  
Samuelson Law, Technology and Public Policy  
Clinic  
University of California, Berkeley  
School of Law (Boalt Hall)  
392 Simon Hall  
Berkeley, CA 94720  
(510) 848-1501

April 24, 2001

## Table of Contents

I.	INTRODUCTION AND SUMMARY	1
II.	THERE IS OVERWHELMING SUPPORT FOR A SEPARATE RULEMAKING TO DEVELOP TECHNOLOGY NEUTRAL PRIVACY RULES FOR LOCATION INFORMATION	3
	A. The majority of industry and public interest commenters believe that a separate rulemaking is appropriate at this time.	4
	B. The majority of industry and the public interest commenters emphasized that the regulations should be technology neutral.	5
	C. The majority of commenters believe that the rule should implement the fair information practices	6
III.	THERE IS SUBSTANTIAL GOVERNMENT INTEREST IN THE PROTECTION OF PRIVACY	7
	A. Self-regulation is not sufficient in the absence of FCC clarification of Section 222	7
	B. Protecting the Privacy of Users of Location Information Products and Services is a Compelling Government Interest	7
IV	THE COMMISSION SHOULD MOVE FORWARD WITH A RULEMAKING TO INTERPRET THE FAIR INFORMATION PRINCIPLES OF 222 AND GIVE GUIDANCE TO INDUSTRY SAFE-HARBOR EFFORTS	10
	A. The Commission Should Clarify How fair information practices apply to section 222	
	B. A safe harbor program may be appropriate, provided applications for safe harbor meet statutory and regulatory mandates and are subject to notice and comment review.	11
	C. If federal regulations are strong, preemption of state regulation of wireless location information may be appropriate	12

D. The Commission need to assess it jurisdiction over non-carriers	13
V. Conclusion	14

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

In the Matter of	)	
	)	
Petition of the Cellular Telecommunications	)	WT Docket No. 01-72
Industry Association for a Rulemaking to Establish	)	DA-01-696
Fair Location Information Practices	)	
	)	

**REPLY COMMENTS OF THE**  
**CENTER FOR DEMOCRACY AND**  
**TECHNOLOGY**

**I. INTRODUCTION AND SUMMARY**

The Center for Democracy and Technology (“CDT”) offers these reply comments to (i) highlight the overwhelming support among commenters for a separate rulemaking at this time to develop technology neutral privacy rules for wireless location information under section 222(f) and (h) of the Communications Act; (ii) respond to comments that the Commission could fulfill its responsibility by endorsing self-regulatory industry guidelines; and (iii) respectfully suggest a procedural and substantive outline for moving forward.

CDT and the majority of commenters agree on the following:

- Privacy rules for wireless location information should be set separately from the rest of the CPNI docket. Industry and public interest commenters agree that location information raises unique privacy concerns, that Congress specifically singled out wireless location

information for special treatment, and that the parties interested in location privacy issues will be significantly distinct from those in the CPNI proceedings.

- Privacy concerns over location-based services need to be addressed now. Ongoing changes in business models and technology are not a bar to the development of clear baseline privacy rules; to the contrary, acting now will promote consumer confidence in a consistent privacy regime, which is more likely to foster industry growth and innovation than the current situation of privacy anxiety and design uncertainty.
- Privacy rules should implement the principles of fair information practices, giving consumers control over the uses of their location information through an opt-in and mechanisms reasonably likely to ensure adherence to the consumer's decision.
- Technology neutrality is desirable for the protection of privacy and the promotion of competition through the maintenance of a level-playing field.

Despite this philosophical and procedural agreement, there are two points of uncertainty that confirm the need for Commission action:

- There is uncertainty on how to implement section 222, as illustrated by the fact that commenters pointed to no less than four different self-regulatory codes for location information.<sup>1</sup> Until the Commission offers clear guidance as to the interpretation of section 222 and sets baseline requirements, it would be premature to endorse any of these as sufficient safe harbors.

---

<sup>1</sup> See the Guidelines on Privacy and Spam submitted by the Wireless Advertising Association ("WAA"), the Draft Privacy Standards of the Wireless Location Industry Association ("WLIA"), the Privacy Promise of the Direct Marketing Association ("DMA") and the Code of Business Conduct submitted by Verizon.

- It is unclear who is covered by section 222 and who is not. In the interests of achieving technology neutrality and creating a level playing field, the Commission should exercise its jurisdiction as broadly as possible and should use its authority over telecommunications carriers to ensure that they do not disclose location information to other entities that do not respect the customer's choice as to reuse. But there may likely be entities that the Commission finds are not covered by its location privacy rules. The need to draw that line is not a reason to refrain from regulation. To the contrary, drawing that line will both fulfill the Commission's responsibility and help Congress decide if additional legislation is necessary to cover entities left out of 222.

Going forward, CDT believes that the Commission should promptly commence a separate rulemaking to define the scope of its jurisdiction in this area and to lay down baseline rules for the implementation of section 222(f) and (h) with respect to wireless location information. Thereafter, the Commission may conduct separate notice and comment proceedings to determine whether any industry code suffices as a safe harbor.

## **II. THERE IS OVERWHELMING SUPPORT FOR A SEPARATE RULEMAKING TO DEVELOP TECHNOLOGY NEUTRAL PRIVACY RULES FOR LOCATION INFORMATION**

The Wireless Communications and Public Safety Act of 1999, Pub. L. 106-81, amended section 222 of the Communications Act to set a special rule for the use and disclosure of and access to wireless location information, requiring telecommunications carriers to obtain the "express prior authorization" of their customers before any use, disclosure or access.

**A. The majority of industry and public interest commenters believe that a separate rulemaking is appropriate at this time**

Most commenters believe that the most appropriate time to craft privacy regulations clarifying the meaning of the location provisions of section 222 is now.<sup>2</sup> The establishment of consistent privacy rules will give carriers and other location service providers stable privacy standards upon which they can build business models and network infrastructures.<sup>3</sup> Hardware manufacturers will be able to incorporate into their designs features that facilitate consumer control over location information, without running the risk of having to engage in expensive retrofitting at a later date.<sup>4</sup> The comments submitted by a number of hardware manufacturers and service providers demonstrate how products can be engineered to implement privacy principles.<sup>5</sup> New products and services will benefit from the level-playing field of uniform privacy practices in the various segments of the industry.<sup>6</sup> Finally, consumers will be more

---

<sup>2</sup> See Nokia Comments (p.5), EPIC Comments (p.1), Cingular Comments (p.1), SCC Comments (p.5), Dobson Comments (p.6), Ericsson Comments (p.2), Texas 911 Comments (p.4), Location Privacy Association Comments (p.3), and SiRF Technologies Comments (p.11).

<sup>3</sup> See TruePosition Comments (p.5-7), Grayson Wireless Comments (p.2-3).

<sup>4</sup> See Location Privacy Association Comments (p.4-5, Exhibits A & B), XNS Public Trust Organization Comments (p.3-4), Cingular Comments (p.1-2), SiRF Technologies Comments (p.1).

<sup>5</sup> Grayson submitted comments noting that its Geometrix network-based wireless system remains under the control of the host carrier. (Grayson Comments, p.2) Airbiquity and Qualcomm also mention that the products that they are now developing incorporate "opt-in" features. (Location Privacy Association Comments, p.4-5; Exhibits A,B) TruePosition also submitted comments noting that it has developed products that ensure that location-based information is used only with subscriber consent. (TruePosition Comments, p.2)

<sup>6</sup> See Ericsson Comments (p.1), AT&T Comments (p.6).

willing to adopt wireless products and services if they trust that the companies providing those services adhere to consistent privacy rules.<sup>7</sup>

The majority of commenters also agree that wireless location issues should be treated separately from the rest of the CPNI docket.<sup>8</sup> Congress specifically amended section 222 to provide for a separate privacy standard for the use and disclosure of location information.<sup>9</sup> The technology of location information and the accompanying privacy concerns are unique and require particular attention.<sup>10</sup> The proceeding should also be separated from the CPNI docket because the industry participants who will comment on wireless privacy are significantly distinct from those interested in the general CPNI proceeding.<sup>11</sup>

**B. The majority of industry and public interest commenters emphasized that the regulations should be technology neutral**

Most commenters, even those that argued that section 222 applies only to CMRS, favor technology neutrality, believing it will help ensure uniformity of privacy protection across

---

<sup>7</sup> See Nokia Comments (p.5-6) AT&T Comments (p.1-2), Ericsson Comments (p.2), WLIA Comments (p.3).

<sup>8</sup> See Nokia Comments (p.3), EPIC Comments (p.2), AT&T Comments (p.4-5), Cingular Comments (p.2), SCC Comments (p.3-4), Dobson Comments (p.3), Ericsson Comments (p.1-2), Texas 911 Comments (p.2), TruePosition Comments (p.12), Location Privacy Association Comments (p.2), RTG Comments (p.1).

<sup>9</sup> See AT&T Comments (p.4-5), SCC Comments (p.3), Verizon Comments (p.2-3)

<sup>10</sup> See Cingular Comments (p.1), Dobson Comments (p.2-3), EPIC Comments (p.2), Verizon Comments (p.3-4), Location Privacy Association Comments (p.2), SiRF Technologies Comments (p.8-9), XNS Public Trust Organization (p.3).

<sup>11</sup> See EPIC Comments (p.2).



location information services.<sup>12</sup> Since consumers will not be able to distinguish between the different technologies that offer similar location services, their confidence in wireless services depends on conformity to unified privacy practices.<sup>13</sup> Technology-neutral regulations will create a level playing field so that some companies will not be artificially advantaged in the market due to lower regulatory obligations.<sup>14</sup>

**C. The majority of commenters believe that the rule should implement the fair information practices**

The comments almost unanimously agree that the principles of fair information practices should govern the privacy rules for location-based services.<sup>15</sup> A number of commenters have submitted detailed proposed fair information practice guidelines.<sup>16</sup> These proposals will provide useful information to the Commission in the context of a rulemaking on the requirements of Section 222. CDT agrees with the majority of commenters that the statutory language requires

---

<sup>12</sup> See Verizon Comments (p.6), Sprint Comments (p.14), Nokia Comments (p.5), AT&T Comments (p.6), EPIC Comments (p.3), Ericsson Comments (p.3), Dobson Comments (p.5), SCC Comments (p.4), Cingular Comments (p.5), RTG Comments (p.4), LPA Comments (p.3).

<sup>13</sup> See Verizon Comments (p.6), EPIC Comments (p.3), Ericsson Comments (p.3), Dobson Comments (p.5)

<sup>14</sup> See AT&T Comments (p.6).

<sup>15</sup> See Nokia Comments (p.2-3), AT&T Comments (p.4), TruePosition Comments (p.7-8), WLIA Draft Privacy Standards (p.3-5), XNS Public Trust Organization Comments (p.1), WCA Comments (p.2-3), Leap Wireless (p.3-6), WAA Guidelines on Privacy and Spam (p.3-5), Ericsson Comments (p.1-2), DMA Comments (p.2), RTG Comments (p.3-4), Cingular Comments (p.2-5), SCC Comments (p.4), LPA Comments (p.3-4), SiRF Technologies Comments (p.1), Verizon Comments (p.5-6), Dobson Comments (p.3-4), Sprint Comments (p.18).

<sup>16</sup> See *supra*, note 1.

an “opt-in” approach to obtaining consent,<sup>17</sup> in addition to core fair information practice principles such as notice, access, and security. Most significantly, CDT agrees with many commenters that privacy rules should follow the underlying intent of Congress to give consumers control of the personal information collected about them.<sup>18</sup>

### **III. THERE IS A SUBSTANTIAL GOVERNMENT INTEREST IN THE PROTECTION OF PRIVACY**

#### **A. Self-regulation is not sufficient in the absence of FCC clarification of section 222**

While a safe harbor provision for conforming industry guidelines may be appropriate, Congress has already decided, by adopting section 222(f) and (h) that self-regulation on its own is incapable of protecting privacy in this context. Furthermore, the disagreement amongst the different segments of the industry over particular rules confirms that there is uncertainty about the proper way to implement Section 222. Additional self-regulatory solutions might continue to appear, with more inconsistent rules. Regulatory guidance in this complex area will create a consistent privacy regime, thereby ensuring both existing companies and new entrants into the various segments of the industry will compete on a level playing field.

#### **B. Protecting the Privacy of Users of Location Information Products and Services is a Compelling Government Interest**

---

<sup>17</sup> See Location Privacy Association Comments (p.3-4), Cingular Comments (p.3-4), SCC Comments (p.3), RTG Comments (p.3), WAA Privacy Guidelines (p.4), WCA Comments (p.2-3), Nokia Comments (p.3), WLIA Draft Privacy Standards (p.4), and TruePosition Comments (p.7).

<sup>18</sup> See Location privacy Association Comments (p.3-4), SiRF Technologies Comments (p.8), EPIC Comments (p.2), RTG Comments (p.1), WCA Comments (p.3).

The government has a substantial interest in protecting consumer privacy. As the DC Circuit recently concluded in *Trans Union Corporation v. Federal Trade Commission*, there is "no doubt that this interest -- protecting the privacy of consumer credit information -- is substantial."<sup>19</sup> Equally if not more significant than the protection of credit information is the protection of location information pinpointing an individual's whereabouts. The fact that location-based services are likely to pervade individuals' everyday activities only serves to heighten these risks. Congress recognized this governmental interest when it amended the CPNI law with a special rule for location information.

The pervasive national media attention surrounding the privacy implications of new technologies and the conclusions of numerous consumer surveys clearly demonstrate that consumers are seeking laws and regulations that will help them protect their privacy.<sup>20</sup> Consumers have grown weary of practices such as the profiling of consumer preferences.<sup>21</sup> The overwhelming majority of consumers are uncomfortable with sharing personal information about themselves with companies who use that information without their express knowledge or

---

<sup>19</sup> 2001 WL 363964, 8 (D.C. Cir.) (April 13, 2001).

<sup>20</sup> See, e.g., Lorrie Faith Cranor, et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* at 5 (1999) (hereinafter "AT&T Study") <<http://www.research.att.com/projects/privacystudy>> (reporting that 87% of surveyed experienced U.S. Internet users stated that they were somewhat or very concerned about threats to their privacy online). See also Louis Harris & Assoc., Inc., Nat'l Consumers League: *Consumers and the 21<sup>st</sup> Century* at 4 (1999) (reporting that 70% of U.S. respondents were uncomfortable providing personal information to businesses online).

<sup>21</sup> The FTC's 2000 Online Profiling Report cited a Business Week/Harris Poll, indicating that "89% of consumers are not comfortable having their browsing habits and shopping patterns merged into a profile that is linked to their real name and identity," a common practice on the Internet. See OP Rept at 15.

consent.<sup>22</sup> Privacy policies influence consumers' willingness to use products and services.<sup>23</sup> In addition to escalating the potential invasiveness of the commercial profiling of individual's lives, location information also exposes users to substantial physical harm for if abused it could facilitate surveillance and stalking of individuals.

Consumers believe the government should play an important role in protecting their privacy interests.<sup>24</sup>

Protecting privacy would serve other important government interests. The implementation of coherent privacy regulations will help ensure innovation and the growth of

---

<sup>22</sup> Although 24% of users who had never engaged in an online transaction cited privacy as the reason, 93% believed that any information divulged during a business transaction should not be shared without permission. See AARP, *Many Americans Face E-Commerce Skills Gap* (Mar. 2000), available at <http://www.aarp.org/press/2000/nr033000.html>. 84% of Americans would either be "not very willing" (22%) or "not willing at all" (62%) to share personal information about themselves so online ads could be targeted to their tastes. See Business Week/Harris Poll: Online Insecurity, BUSINESS WEEK (last modified Mar. 5, 1998) <<http://www.businessweek.com/1998/11/b3569107.htm>>. 59% never register for free web sites, where personal information is required. See Id. 40% provide false information on such forms at least some of the time. See Id.

<sup>23</sup> A number of studies have indicated that privacy concerns are indeed contributing to a significant decrease in online sales. See, e.g., Forrester Privacy Best Practice Report (cited in FTC 2000 Report, citing Microsoft Advertisement, N.Y. TIMES, Mar. 23, 2000, at A12). (estimating that privacy concerns led to \$2.8 billion in lost sales in 1999); Sandeep Junnarkar, *Report: Half of Net Users Mistrust Sites*, CNET News.com (Aug. 17, 1999), available at <<http://home.cnet.com/category/0-1007-200-346152.html>> (citing results of study by Jupiter Communications, Inc., estimating that this figure will reach \$18 billion in 2002 if nothing is done to allay privacy concerns). A TRUSTe survey found that privacy statements make it two to three times more likely that a consumer will provide personal information to a website. See TRUSTe/Boston Consulting Group Consumer Survey <[http://www.truste.org/webpublishers/pub\\_bottom.html](http://www.truste.org/webpublishers/pub_bottom.html)> (also citing numerous other surveys). Finally, users tend to form unfavorable impressions of privacy practices if no privacy statement is posted on a web site. See Beyond Concern <<http://www.research.att.com/library/trs/TRs/99/99.4/99.41/Survey-TR-19990325.htm>>.

<sup>24</sup> Over 70% of Americans believe that some form of legislation is required to protect privacy. See Georgia Institute of Technology, *10<sup>th</sup> GVU WWW User Survey* (December, 1998). When asked if existing laws protecting the privacy of telephone conversations are enough to protect email and online activities, 62% of all Americans say that new laws need to be written to protect online privacy. (Pew Internet Tracking Report, April 2, 2001, <http://www.pewinternet.org/>).

location-based products and services. Many commenters pointed out that the strengthening of consumer confidence is a prerequisite for the success of these services..

Privacy regulations will promote a healthy competitive environment within the location-based services industry.

**IV. THE COMMISSION SHOULD MOVE FORWARD WITH A RULEMAKING TO INTERPRET THE FAIR INFORMATION PRINCIPLES OF 222 AND GIVE GUIDANCE TO INDUSTRY SAFE-HARBOR EFFORTS**

**A. The Commission should clarify how fair information practices apply to section 222**

A rule applying fair information practices to 222 would have the following elements:

**Notice:** The Commission's rules should require service providers to inform customers about the collection, use and disclosure of and access to wireless location information. While the specific format of the company's notice may be dependent on the device used, the notice must be easy to find and understand. The customer should also be notified of a company's policies regarding the storage of information, retention of data, and security practices.

**Express prior authorization:** The rules should require service providers to obtain a customer's express prior authorization before using, disclosing, or permitting access to that customer's wireless location information, except where the use or disclosure of the data is necessary to complete or bill for the transaction that initially generated the information. (Privacy rules need not impede customers from readily utilizing the location-based services they request.) The customer's knowing grant of permission must be explicit and may be evidenced through contemporaneous verbal communication, user signaling from a wireless device that authorizes

the particular use, disclosure or access, or by a written or electronically signed agreement, web site subscription, or other contractual instrument in which the proposed use, disclosure or access is fully, clearly and conspicuously described and separately consented to. The rules should also make clear that consent to uses and disclosures of data other than those necessary to provide the requested service must not be a condition of service.

In order to ensure that the consumers' choice is respected, the rules should require providers of location services as well as their contractors and partners to restrict any use, disclosure or access to wireless location information to the specific commercial purpose to which the customer gave their express authorization. In addition, no wireless information should be retained or subsequently released for any other purpose beyond the scope of a customer's express authorization without gaining express authorization explicitly for that purpose from the customer. Any party that collects or uses wireless location information should delete data linked to a customer after it is no longer needed for billing or billing dispute purposes. The rules should ensure the security and integrity of wireless location data and give customers access to such data.

**B. A safe harbor program may be appropriate, provided applications for safe harbor meet statutory and regulatory mandates and are subject to notice and comment review.**

A number of commenters called for a "safe harbor" approach. CDT is not opposed to a safe harbor approach, provided its parameters are properly defined and administered. A properly drawn safe harbor system could provide industry with an appropriate level of flexibility, while at the same time balancing the need to make effective rules implementing Section 222.

A safe harbor program is only acceptable if FCC regulations are already in place, clarifying the meaning of section 222 and setting forth baseline privacy rules for those who choose not to participate in a safe harbor program and if there is an appropriate public notice and comment period for specific safe harbor proposals in accordance with the standard NPRM process. Finally, any safe harbor should include oversight and enforcement, in addition to any provided by the Commission's rule. Such a safe harbor program, against the background of default Commission rules, would give industry the flexibility it desires while ensuring that consumers will be able to continue to rely on privacy standards defined by the Commission.

The Federal Trade Commission's COPPA safe harbor program, put in place through the Children's Online Privacy Protection Rule (COPPR), provides an example of a successful safe harbor program similar to the one described above. To receive safe harbor approval under the COPPR, an applicant must show that its safe harbor has "substantially similar requirements that provide the same or greater protections . . . as those contained" in the rule.<sup>25</sup> Prior to being approved, the proposed safe harbor guidelines must go through a public notice and comment period. Those organizations complying with the safe harbor gain a presumption that they are in compliance with the COPPR itself. Industry safe harbors under COPPR also provide their own layer of oversight and enforcement.

**C. If federal regulations are strong, preemption of state regulation of wireless location information may be appropriate**

---

<sup>25</sup> COPPR, 64 FR 212 at 59907.

Normally, the states have a significant interest in protecting the privacy of their residents. However, with regard to wireless location information, federal preemption of inconsistent state rules may be appropriate if the federal rule is sufficiently protective of privacy. Preemption could thus serve the need to achieve a consistent and predictable privacy standard that consumers can rely on.

**D. The Commission needs to assess its jurisdiction over non-carriers**

The comments unanimously support technology neutral rules, and CDT agrees that this is a critical component of any wireless privacy regime. Unfortunately, in an era of convergence and rapidly developing technologies, it is not completely clear which technologies are covered by Section 222(f). Yet this is an issue that will surely arise, in applying Sections 222 (f) and (h), so the Commission should address it in the rulemaking.

The Commission may find that some location services, at least to the extent they collect or use wireless location information via radio communication, are either CMRS or functional equivalents thereof. Alternatively, the Commission may find that an extension of ancillary jurisdiction over some services is necessary to effectuate Congress' intent – that consumers be assured of privacy protection for their location information. It is also possible that technological developments since Section 222 was drafted have changed the r landscape so much that certain entities providing location services fall outside the statute's limitation to “telecommunications carriers.” But CDT believes that the Commission has sufficient authority to cover a large portion of the emerging wireless location industry.



To the extent a third party obtains location information relayed through a traditional CMRS carrier's facilities, such information would clearly be covered by the statute. Section 222 does not merely prescribe certain privacy rules that telecommunications carriers are bound to follow. It also generally charges them with "a duty to protect the confidentiality" of customer information.<sup>26</sup>

This duty extends to a carrier's relationship with other service providers, to the extent they obtain information by virtue of the carrier's network. The duty would obligate CMRS providers to, at a minimum, contractually require third parties to whom they provide information to abide by the same customer decisions that the carriers themselves are subject to.

## **V. CONCLUSION**

There is overwhelming support among the comments received for a separate rulemaking at this time implementing Sections 222 as to location information. The comments unanimously support rules that are technology neutral, and that implement the core principles of fair information practices.

Congress has already said that wireless privacy location must be subject to special privacy protection, but the details of that rule and the scope of coverage are unclear. A rulemaking is appropriate now precisely because location-based services are in their infancy and in need of regulatory certainty prior to a large-scale rollout. A separate rulemaking is appropriate because wireless location information is different from other CPNI, because it

---

<sup>26</sup> Section 222(a).

implicates unique privacy concerns and involves a different group of industry participants than in the CPNI proceedings generally.

The need for FCC guidance (as opposed to unlimited deference to safe harbors) is evidenced by the fact that at least four different codes of fair information practices have been suggested. Although similar in nature, there are enough differences among them to suggest that the industry is uncertain about how Section 222 should be implemented. Although there should be some room for different industry approaches, such flexibility should still be guided by baseline rules established by the Commission. A safe harbor program could provide the flexibility industry seeks, while at the same time providing the guidance necessary for proper implementation of Section 222.

Finally, there is also uncertainty over which participants these provisions apply to. It is essential that the Commission provide guidance to industry and the public about the scope of the wireless privacy rules envisioned by Congress.

Respectfully submitted,

James X. Dempsey  
The Center For Democracy & Technology  
1634 Eye Street NW, Suite 1100  
Washington, DC 20006  
(202) 637-9800  
[www.cdt.org](http://www.cdt.org)

Deirdre Mulligan  
Christopher K. Ridder  
Eddan Katz  
Samuelson Law, Technology and Public Policy  
Clinic  
University of California, Berkeley  
School of Law (Boalt Hall)  
392 Simon Hall  
Berkeley, CA 94720  
(510) 848-1501

April 24, 2001

## CERTIFICATE OF SERVICE

I, James X. Dempsey, hereby certify that on this 24<sup>th</sup> day of April 2001, I caused copies of the foregoing "Reply Comments of the Center for Democracy and Technology" to be sent first class, postage prepaid to the following:

John T. Scott III, Charon J. Harris,  
Stephen J. Berman  
Verizon Wireless  
1300 I Street, NW Suite 400 West  
Washington DC 20005

John W. Jimison  
Attorney for Wireless Location Industry Assn.  
1225 19th Street, NW  
Washington, DC 20036

Philip L. Verveer, David Don,  
Kelly N. McCollian  
Willkie Farr & Gallagher  
Attorneys for Trueposition Inc.  
Three Lafayette Center  
1155 21st Street, NW Suite 600  
Washington DC 20036

James Green  
Tongour Simpson Holsclaw Green, LLP  
Attorney for Location Privacy Association  
227 Mass. Avenue NE Suite #1  
Washington, DC 20002

James H. Barker, William S. Carnell,  
Matthew R. Vandergoot  
Latham & Watkins  
Attyns for Leap Wireless International Inc.  
555 Eleventh Street, NW Suite 1000  
Washington, DC 20004-1302

Ian D. Volner, Heather L. McDowell  
Venable, Baetjer, Howard & Civiletti, LLP  
Attorneys for Direct Marketing Association  
1201 New York Avenue, NW Suite 1000  
Washington DC 20005

Amy L. Bushyeager  
Mintz, Levin, Cohn, Ferris, Glovsky  
& Popeo, PC  
Attorney for AT&T Wireless Services  
701 Pennsylvania Avenue, NW  
Washington, DC 20004

Scott J. Rafferty  
SiRF Technology Inc.  
148 East Brokaw Road  
San Jose, CA 95112

Eliot J. Greenwald  
Swidler Berlin Shereff Friedman, LLP  
Attorney for Grayson Wireless  
3000 K Street, NW Suite 300  
Washington, DC 20007

Caressa Bennet , Brent Weingardt,  
Rebecca Murphy  
Bennet & Bennet, PLLC  
Attorneys for Rural Telecommunications Grp  
1000 Vermont Avenue, NW Tenth Floor  
Washington, DC 20005

Robert L. Hoggarth, Leslie Kaplan, Richard  
Grant  
Personal Communications Industry Association  
500 Montgomery Street Suite 700  
Alexandria, VA 22314

J.R. Carbonell  
Cingular Wireless  
5565 Glenridge Connector Suite 1700  
Atlanta, GA 30342

Martha Jenkins, Craig Donaldson  
 SCC Communications Corporation  
 1225 I Street, NW Suite 500  
 Washington, DC 20005

Carl Hillard  
 Wireless Consumer Alliance Inc.  
 1246 Stratford Court  
 Del Mar, CA 92014

Elisabeth H. Ross, Allison M. Ellis  
 Attorneys for Ericsson  
 Birch Horton Bittner & Cherot  
 1155 Connecticut Avenue, NW Suite 1200  
 Washington, DC 20036

Wireless Advertising Association  
 Wiley, Rein & Fielding  
 1776 K Street NW 9<sup>th</sup> Floor  
 Washington, DC 20006

Cheryl A. Leanza, Andrew Jay Schwartzman,  
 Harold J. Feld  
 Media Access Project  
 750 18th Street, NW Suite 220  
 Washington, DC 20006

Ronald L. Ripley  
 Senior Corporate Counsel  
 Dobson Communications  
 13439 N. Broadway Ext. Suite 200  
 Oklahoma City, OK 73114

Michael Altschul  
 Randall S. Coleman  
 Cellular Telecommunication Industry Assoc.  
 1250 Connecticut Avenue, NW Suite 800  
 Washington, DC 20036

Luisa L. Lancetti  
 Sprint PCS  
 401 19th Street, NW Suite 400  
 Washington, DC 20004

Leo R. Fitzsimon  
 Director of Regulatory & Industry Affairs  
 Nokia Inc.  
 1101 Connecticut Avenue, NW Suite 910  
 Washington, DC 20036

Barbara Baffer  
 Ericsson Inc.  
 1634 I Street, NW Suite 600  
 Washington, DC 20006

David Sobel  
 Electronic Privacy Information Center  
 1718 Connecticut Avenue, NW Suite 200  
 Washington, DC 20009

Rupaco T. Gonzalez, Jr., Richard A. Muscat  
 Attorney for Texas 9-1-1 Agencies  
 The Gonzalez Law Firm, PC  
 One Westlake Plaza Suite 100  
 1705 South Capitol of Texas Highway  
 Austin, TX 78746

Albert Gidari  
 Attorney for Cellular Telecommunications  
 Industry Assoc.  
 Perkins Coie, LLP  
 1201 Third Avenue, 48th Floor  
 Seattle, WA 98101

Barbara Reideler  
 Policy Division  
 Wireless Telecommunications Bureau  
 Federal Communications Commission  
 445 12<sup>th</sup> Street SW Room 3-B101  
 Washington, DC 20554

Bryan Tramont  
Legal Advisor  
Office of Commissioner Furchtgott-Roth  
Federal Communications Commission  
445 12<sup>th</sup> Street SW Room 8-A302  
Washington, DC 20554

Thomas Sugrue  
Chief  
Wireless Telecommunications Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street SW Room C252  
Washington, DC 20554

Peter A. Tenhula  
Legal Advisor  
Office of Chairman Powell  
Federal Communications Commission  
445 12<sup>th</sup> Street SW Room 8-A204F  
Washington, DC 20554

Kris Monteith  
Chief, Policy Division  
Wireless Telecommunications Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street SW Room 3-B101  
Washington, DC 20554

Mark Schneider  
Senior Legal Advisor  
Office of Commissioner Ness  
Federal Communications Commission  
445 12<sup>th</sup> Street SW Room 8-B115  
Washington, DC 20554

James D. Schlichting  
Deputy Bureau Chief  
Wireless Telecommunications Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street SW Room 3-C254  
Washington, DC 20554

Adam Krinsky  
Legal Advisor  
Office of Commissioner Tristani  
Federal Communications Commission  
445 12<sup>th</sup> Street SW Room 8-C302  
Washington, DC 20554

---

James X. Dempsey