EX PARTE OR LATE FILED DOCKET FILE COPY ORIGINAL

RECEIVED

AUG 16 1995

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

Building The Wireless Future™

CTIA

Cellular
Telecommunications
Industry Association
1250 Connecticut
Avenue, N.W.
Suite 200
Washington, D.C. 20036
202-785-0081 Telephone
202-785-0721 Fax
202-736-3248 Direct Dial

Michael F. Altschul
Vice President,
General Counsel

August 16, 1995

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
1919 M Street, N.W. - Room 222
Washington, D.C. 20554

RE: Ex Parte Filing - CC Docket No. 94-102

Dear Mr. Caton:

On August 16, 1995, Michael Altschul, Vice President and General Counsel, CTIA, sent Mr. John Cimko, Chief, Policy Division, Wireless Bureau, and his staff members, Ms. Nancy Boocker, Mr. Daniel Grosh, and Mr. Todd Lantor, copies of the attached letter.. The letter references the proceedings regarding the provision of "E-911" services by wireless carriers, and expressed CTIA's positions as previously filed in the above-referenced docket, as well as in the attached document.

Pursuant to Section 1.1206 of the Commission's Rules, an original and one copy of this letter and the attachment are being filed with your office.

If there are any questions in this regard, please contact the undersigned.

Sincerely,

Michael F. Altschul

Attachment

No. of Copies rec'd 0+1
List A B C D E

Building The Wireless Future™

CTIA

Cellular
Telecommunications
Industry Association
1250 Connecticut
Avenue, N.W.
Suite 200
Washington, D.C. 20036
202-785-0081 Telephone
202-785-0721 Fax
202-736-3248 Direct Dial

Michael F. Altschul
Vice President,
General Counsel

August 16, 1995

Mr. John Cimko
Chief, Policy Division
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W. - Room 5202
Washington, D.C. 20554

RE: Wireless "E-911" Service: CC Docket No. 94-102

Dear Mr. Cimko:

On August 3, 1995, I met with you and your staff to discuss CTIA's views on the issues raised in CC Docket No. 94-102, Wireless "E-911" Service. In response to my suggestion that the Wireless Bureau should be aware of other federal initiatives that may impact on this proceeding, you requested additional information on the Intelligent Transportation System ("ITS"), formerly known as the Intelligent Vehicle Highway System, and the Cellular Priority Access Services ("CPAS") project of the President's National Security Telecommunications Advisory Committee.

I have enclosed a description of the ITS projects taken from *Wireless Technologies and the National Information Infrastructure,* a report authored by the Office of Technology Assessment. As OTA notes, in 1991, Congress committed $659 million to establish the ITS Architecture Development Program. *See* U.S. Congress, Office of Technology Assessment, *Wireless Technologies and the National Information Infrastructure,* OTA-ITC-622 (Washington, DC: US Government Printing Office, July 1995) at 50-52. I also have enclosed the OTA Report's description of the privacy issues raised by ITS (and E-911) under the Communications Assistance to Law Enforcement Act, Public Law 103-414, sec. 103(a)(2), Oct. 25, 1994, 108 Stat. 4281. *Id.*, at 230-232.

With respect to the CPAS project, I have enclosed the most recent draft of the CPAS Subgroup's Report. CTIA has supported the activities of the CPAS Subgroup established by the Wireless Service Task Force of the National Security Telecommunications Advisory Committee. As the draft report indicates, the CPAS Subgroup is in the process of designing a priority access service for cellular systems, and seeks to integrate the E-911 services that are the subject of CC Docket No. 94-102 with the CPAS deployment effort.

Please feel free to contact me if you need additional information on these programs.

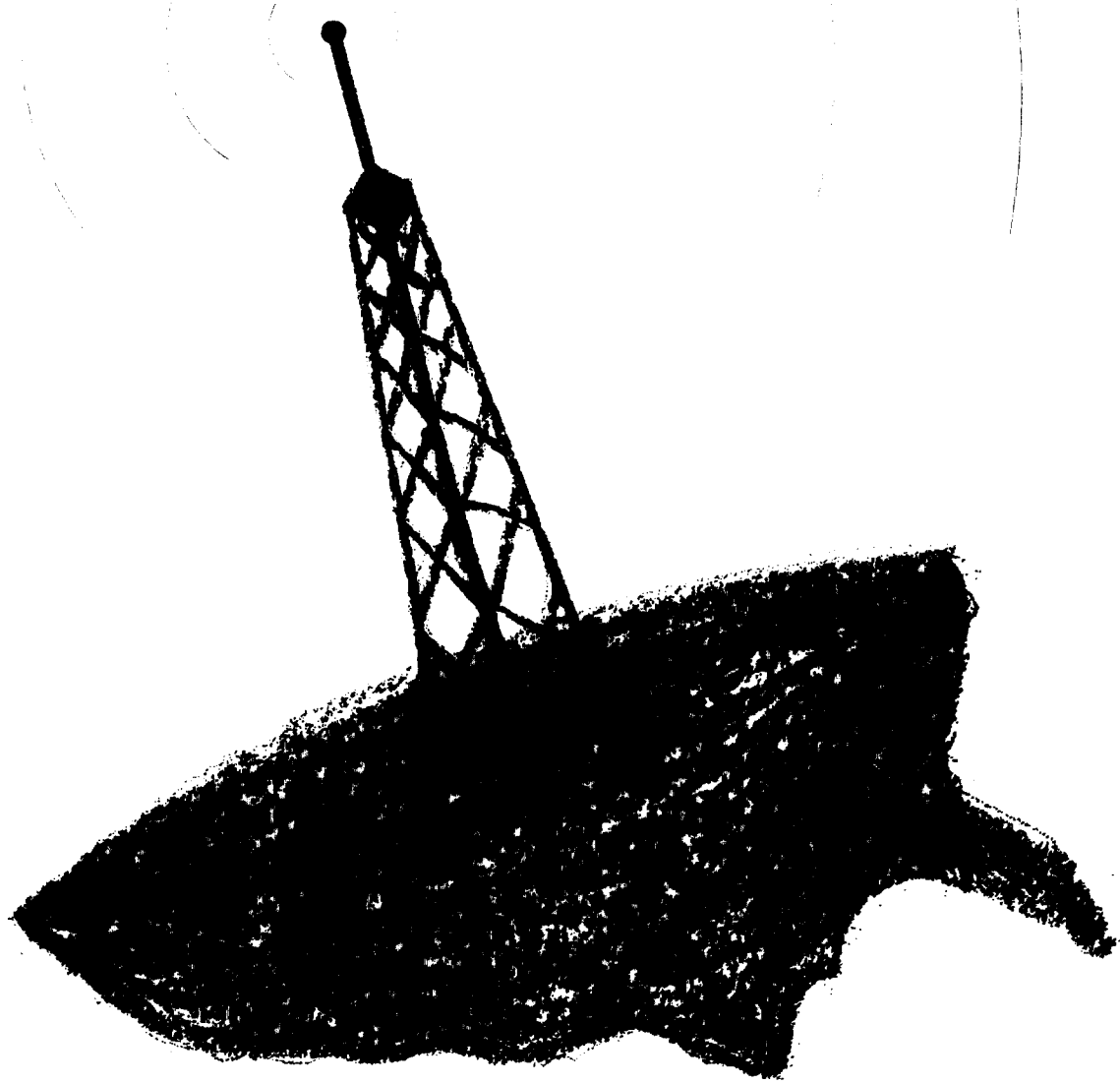
Sincerely,

Michael F. Altschul

Attachments

cc: Ms. Nancy Boocker (w/att)
Mr. Daniel Grosh (w/att)
Mr. Todd Lantor (w/att)

Wireless Technologies and the National Information Infrastructure



Office of
Technology
Assessment

Congress
of the
United States

eral wireless services have been developed. For example, a low-power FM transmitter can be placed on a property for sale which will broadcast messages that identify key characteristics of the property. An agent driving past the house can tune in to hear the details. Another system uses a personal digital assistant (PDA) and a cellular digital packet data (CDPD) radio modem to provide real estate agents access to a multimedia database of homes. The data consist of pictures of houses, maps of residential areas, and detailed statistics that can be searched by price, location, number of rooms, etc. Rather than having to return to the office to search the listings again, a revised list of appropriate offerings could be accessed from any location.

Field Service

To handle more calls, provide faster and more accurate inventory control, and reduce the time spent sending dispatch instructions, Coast Plumbing of Solana Beach, CA, implemented a data communications system that integrated dispatch, billing, and inventory functions.[4] The system connects a portable computer in each of the company's 20 trucks to a host computer in the office. The system delivers text dispatches to the plumber's portable computer, which displays the customer's name, address, and the reason for the call. The system also allows the technicians to check on part availability, access prior service history, and look up prices. Once a job is finished, the system automatically transmits billing and inventory information back to the host computer, which then updates parts lists and customer accounts. Coast also uses specialized mobile radio for voice and data communications.

After implementing the system, Coast Plumbing increased the number of calls per day handled by each plumber, dramatically reduced the amount of time spent on physical inventory, improved customer satisfaction, and streamlined administrative processes. The company estimates that the system saves it more than $10,000 per month in total costs.

Disaster Recovery and Assistance

The success of emergency relief and recovery efforts relies on the ability of workers to communicate effectively, efficiently, and securely. Wireless is uniquely suited to these applications because: 1) disasters typically do not affect wireless communications links, especially satellite links, and 2) the rapid deployment of a communications system for mobile field workers is more efficacious with a wireless system. The users of these systems include insurance companies; emergency relief workers; federal, state and municipal disaster agencies; emergency medical personnel; and other suppliers of necessary services. They will typically need communications in the field to report assessments of damage, call for reallocation of resources, predict additional consequences, and file insurance claims or pay such claims electronically. For example, one company provided Iowa's 99 counties with backup protection during the flood of 1993 with a portable 18 GHz digital microwave system. The system was engineered, manufactured, delivered, and installed in just four days.

Intelligent Transportation Systems

Intelligent Transportation Systems (ITSs)[5] apply information and communication technologies to surface transportation systems to reduce traffic

[4] Deborah Kirtland, *Wireless for the Corporate User*, vol. 3, No. 2, 1994, p. 53.

[5] ITS was formerly called Intelligent Vehicle Highway Systems (IVHS), but was changed to ITS to include public transit and other transportation modes.

congestion, improve safety, make public transit options more attractive to commuters, and decrease transportation-related environmental impacts.[6] Interest in ITS stems from the realization on the part of transportation experts that building more roads and/or expanding existing ones is often too costly and only marginally effective in reducing congestion, and does little to alleviate safety and environmental problems. ITS could make more efficient use of the current transportation infrastructure, improve safety, and allow public transportation to be more responsive to passenger demands. To transmit information to mobile units (automobiles, buses, and trains, etc.) from a fixed location, and vice versa, wireless technology of some kind is necessary.

In 1991, Congress passed the Intermodal Surface Transportation Efficiency Act (ISTEA[7]), which committed $659 million over six years for ITS projects. ISTEA also mandated the U.S. Department of Transportation (DOT) to establish the ITS Architecture Development Program. This program brings together DOT, a public/private consortium called ITS America, and various private transportation and communication companies for the purpose of forming a framework to develop an integrated, interoperable ITS in the United States.[8] More recently, the Federal Communications Commission (FCC) has allocated 26 MHz in the 902-928 MHz band for what it terms Transportation Infrastructure Radio Service, or TIRS.

Among the areas being developed are advanced traveler information systems that will inform people on the best way to get to their destinations; advanced traffic management systems that will gather and distribute data on traffic congestion and alter the timing of control signals to move traffic more efficiently; automatic toll collection; parking and security applications; and automated vehicle control. To date, most ITS efforts have focused on providing route guidance to travelers and fleet monitoring and control to transportation companies. Systems in Japan, Europe, and the United States rely on the Global Positioning System (GPS) for vehicle location, often used in conjunction with dead reckoning.[9] Some systems also employ terrestrial-based wireless data systems to relay traffic conditions to travelers in their cars. Both scenarios involve sophisticated mobile units for the users that can cost as much as $8,000.[10] One system marketed by Oldsmobile offers drivers stored information about local points of interest, such as restaurants, with the option to receive updated traffic, weather, and special event information via a wireless link.

More complex ITS proposals will require more sophisticated technology, both in-vehicle and in the public transportation infrastructure, than existing systems now offer. For example, some plans call for a radar-equipped vehicle that will sense the distance between it and the car in front and automatically apply the brakes if the gap is too small. Some plans for these Advanced Vehicle Control Systems (AVCS) may also incorporate sophisticated sensing equipment in the roadway, which would work in conjunction with systems in the ve-

[6] National Research Council, "Primer on Intelligent Vehicle Highway Systems," Transportation Research Circular 412, Washington, DC, August 1994. See also U.S. Congress, Office of Technology Assessment, *Intelligent Transportation Systems for Metropolitan America—Background Paper*, background paper for OTA's Project on the Technological Shaping of Metropolitan America (in progress).

[7] Public Law 102-240; Dec. 18, 1991.

[8] U.S. Department of Transportation and ITS America, ITS Architecture Development Program; Phase I, Summary Report, Washington, DC, November 1994.

[9] Dead reckoning is a technique by which vehicle location can be calculated and matched to on-board maps by calculating the distance traveled from a specific starting point.

[10] W. Clay Collier and Richard J. Weiland, "Smart Cars, Smart Highways," *IEEE Spectrum*, Apr. 4, 1994, pp. 27-33.

hicles to automatically track the vehicle down the road at a constant speed toward the driver's destination.

CHARACTERISTICS OF MOBILITY

At the root of interest in wireless telecommunications is its ability to accommodate the physical mobility of people and things. However, our understanding of mobility is intuitive and poorly characterized analytically.[11] Some of the broad outlines of mobility are sketched here to provide a sounder basis for analyzing mobility and its implications. Key questions are: Why are people mobile? What are the features and forces that have shaped people's mobility patterns? What are the key trends in mobility? How do wireless technologies fit with mobile activities? What are the consequences of mobility?

Mobility has a number of dimensions that give it different meanings for different people. For example, some mobility is local, as in a hospital where nurses and doctors are constantly on the move, but within well-defined boundaries. Some mobility is long-distance, as with cross-country trucking or cellular roaming to cities outside the home service area. Some people are mobile but do not communicate en route, such as executives travelling to meetings in distant cities. Others communicate en route over long distances, such as salesmen who need to get up-to-date information before meeting their next prospect. While each is mobile, the wireless telecommunications technologies each would likely use may be quite different. Using the single term "mobility" masks its multiple dimensions and deprives it of analytic precision. Data on mobility characteristics, as described below, do not exist at present.

From the examples of applications given above and data on past and projected demand, the following characteristics or drivers of mobile access can be inferred:

- **People want to be mobile because they can increase their control and reduce uncertainty** in the conduct of their business or personal affairs. People move to see and do things remotely so that they can control their activities or gather information that reduces their uncertainty.
- **People want to communicate while moving,** or while in transit. They want flexibility in deploying and redeploying assets, services, etc. In many situations, people cannot predict their communications requirements, either for type of service or its location. All of these needs are met by a variety of wireless technologies, at a low cost, depending on the application, the data rate, and security requirements.
- **People want to communicate and get information *immediately.*** When they are traveling or away from wired telecommunications links, the urge to be connected is strong. Although one can usually travel to a place that has communications resources, the time pressures of today's society and business world dictate that those who have easiest access to communications resources have a competitive advantage.

Typologies like those in table 2-1 could be used to develop research programs and data sources on mobility and communications that could assist both policymakers and business planners. In particular, this framework could help determine the potential scale of wireless communications. Decisionmakers would then know whether particular public wireless communications systems are likely to be confined to small populations of workers or users, or are likely to be applicable to large segments of society. They could also provide information on the impact these technologies may have on individuals, organizations, and society at large.

[11] One attempt is that of the Cross-Industry Working Team, Corporation for National Research Initiatives, "Nomadicity: Characteristics, Issues and Applications," March 1995.

Encryption

Additional security can be provided by a variety of separate encryption schemes. Voice encryption has been used since the 1920s for military use.[12] Commercial products have been available since the 1970s, and a few companies make such products today. Total sales of encryption products now number only a few thousand a year. Some cellular companies offer encryption services, but they are not widely used.

Encryption systems can use either analog or digital techniques. Analog systems manipulate analog wave forms by splitting and inverting the voice signals using ordinary filters. A harmonic signal is injected into the output, resulting in harmonic distortions. These encrypted signals are transmitted, and the reverse process is used to reconstruct the communication. Further encryption can be achieved by varying some of the parameters of the signal-splitting and harmonic distortion, but voice quality may suffer as more distortion is introduced. Companies manufacturing such systems claim that they cannot be decoded in real time, but they admit that they could be recorded and broken later. Nevertheless, these systems can provide a high level of security, but cost from $300 to $1,000 per unit (two units are needed—one for each end of a communication).

Digital encryption systems work by manipulating digitized voice signals. The data representing voice speech are compressed and processed to pass through only phonemes or speech elements (which are reconstructed by the receiver using special software). The digital bitstream is further manipulated using bit substitution, permutation, and other techniques. The encrypted data can be further scrambled, as noted above, with the use of digital transmission systems, which break the bitstream into packets and are coded and displaced in time. Such manipulations incur little or no cost in signal quality, because digital data can be accurately reproduced, and error-checking and correction techniques applied. Voice encryption schemes based on RSA, an encryption algorithm thought to be extremely secure, are on the horizon, and promise a level of privacy protection that is thought to be unassailable.[13] The main constraint with all encryption is the slow speed of processing and the lag that occurs if signals take too long to pass through the system. As signal-processing hardware and software improve, greater levels of security may become available, but the ability of decrypters is also likely to improve as well. To date, most voice encryption devices are bulky and inconvenient, and do not enjoy much consumer or carrier acceptance.

Privacy of Location

A new aspect of wireless networks is uncertainty about and concern for *privacy of location*, where a caller's location can be hidden to a certain extent from the network and from the recipient of the message. By the same token, location information is necessary, at least to the level of a sector within a cell, for the switching equipment to be able to successfully connect users.

This feature contrasts markedly with wireline networks where location of the parties is unambiguous, especially to the system operator, but also most likely to the correspondents. The ambiguity of wireless is likely to lead to a series of new issues for wireless users. Much of our common understanding of business, law, and social behavior is based on assumptions about the unchanging nature of place and people. With widespread deployment of wireless technologies, this is less likely to be the case. Assumptions about boundaries, jurisdictions, and proximity are challenged by mobility and ambiguous location information. People will likely develop strategies to uncover the location of users and to hide themselves from others.

[12] Material on voice encryption drawn from Dan Sweeney, "The Wages of Fear: Marketing Cellular Encryption," *Cellular Business*, vol. 9, No. 13, December 1992, pp. 58-66.

[13] Red Rock Eater listserver, op. cit., footnote 9.

Unlike wireline networks, wireless networks typically do not know the precise location of the parties to a transmission. This uncertainty varies depending on the type of system: satellite systems have the largest "granularity" of coverage because they are typically broadcasting either to whole continents or large regions. Cellular and other terrestrial networks have much smaller areas in which signals can be received and transmitted, with a maximum of about 20 miles for cellular systems. Future personal communication services (PCS) will use cells covering even smaller areas, perhaps only a few hundred yards in diameter. Location identifying techniques must confront the fact that while it is simple to identify a particular transmitter used by someone with a wireless device, the area that transmitter serves may be quite large or difficult to search, thereby making precise location difficult to determine.

A number of services already exist to address location concerns, and there will be implications associated with this inherent ability. Tracking people and things may be easier in the future with both Global Positioning Satellite (GPS) (see box 4-3) and non-GPS systems using lightweight and inexpensive receivers and radios. In trucking logistics, for example, wireless technologies have helped produce significant improvements in services for firms such as UPS and Federal Express, which now depend on such technologies to conduct their business.[14] Vehicle location services such as Lo-jack and Teletrak are already well established or are under development.

Cellular telephones are actually in operation more than most users think (if the phone is turned on, but not actually being used). To monitor the state of the network and be able to respond quickly when calls are made, the main cellular controlling switch periodically "pings" all cellular telephones. This pinging lets the switch know which users are in the area and where in the network the telephone is located. This information can be used to give a rough idea of location, down to the level of a cell, or cell sector, or even smaller areas, depending on the system used.

With the prospective launch of PCS systems, with cell areas typically smaller than those of cellular telephone systems, it may be possible to specify particular areas in which a PCS phone may operate. Parents might use this to control the movements of their children, or administrators the movement of their employees. If a user strays from the approved area, a message might be sent, "Get back home now!" Such services would be inexpensive to provide, because they are a byproduct of the normal operation of this type of technology.[15] As yet, however, there has been no demand for such services.

A wireless user's location can also be calculated by using a combination of signal strength, angle of return, time delay and synchronization, in somewhat the same way that a person can infer distance by seeing or hearing an object with two eyes or ears. Technology developments in location identification for emergency 911 services with wireless systems will undoubtedly improve the ability of wireless service providers to locate individual users. These methods can be fairly accurate, particularly when used together, and they are likely to improve in the near future (see discussion of emergency 911 services in chapter 3). Law enforcement services already can locate an emitter to within six feet, if given sufficient time and resources, possibly in as little as a half hour.[16] (This level of detail would be the result of significant effort, for example, in serious fraud or drug investigations.)

Techniques are likely to be found that enable people to hide themselves from wireless networks and other people. Mobility allows users to contact others from any location; if they move quickly

[14] Frank Erbrick, UPS Vice President for Operations, OTA Advisory Panel meeting, May 12, 1994.

[15] Scott Schelle, vice president for operations, American Personal Communications, Inc., OTA Advisory Panel meeting, May 12, 1994.

[16] Interview with U. S. Secret Service officials, Dec. 12, 1994.

enough, it will be difficult to trace them. Simply turning off the handset will serve in many cases (but will also make the phone unusable for receiving calls).

One area of growing concern is how information about personal location and behavior could be gathered and used by a range of large information systems, such as electronic payment systems, credit card and other credit reporting, telecommunications transaction records, health record systems and the like.[17] The Communications Assistance to Law Enforcement Act forbids wireless carriers from divulging location information to anyone, except to law enforcement authorities with a proper warrant.[18]

The issues of personal information-gathering and disclosure are beyond the scope of this report. They generally do not involve matters of wireless telecommunications technologies, with one exception: the Intelligent Transportation System (ITS), formerly known as the Intelligent Vehicle Highway System (IVHS). The inherently mobile nature of transportation, and the reliance of ITS designers on wireless telecommunications for some aspects of the system, raises the issue of privacy protections.[19] Some analysts have argued that:

> Many of these technologies involve surveillance of the location and behavior of identified vehicles and/or people, and the collation of such data for further use. These and other aspects of IVHS technologies raise concerns amongst the community, and have delayed adoption of some systems.[20]

> [S]ome proposed designs require the system to collect vast amounts of data on individuals' travel patterns, thus raising the potential for severe invasions of privacy. To make social choices about IVHS, it is necessary to reason about potentials for authoritarian uses of an IVHS infrastructure in the hypothetical future.[21]

The design of such systems or subsystems needs to carefully considered with privacy concerns in mind.

Location and legal jurisdiction

Many aspects of the law are predicated on geographic location. To a certain extent, wireless telecommunications confound such geography-based distinctions, because with cellular telephones, boundaries (local or state, and to a limited extent, international) can be broached. With satellite-based communications, boundaries are essential-

[17] GSM systems reportedly know the location of all phones within 10 meters, and that the three closest cell sites track the phone at all times, to enable smooth hand-offs from one cell to another. Continuous location data could easily be recorded, even for many users, without posing an undue data burden—one observer estimates that 1 million users, tracked every 10 minutes to one square meter, for one year, would generate about 510 gigbits of uncompressed data, well within the data processing capability of most business and many personal computers. See Internet post, Date: Thu, 20 Apr 1995 08:32:19 +0200, From: mobile-rg@dxm.ernet.in, To: cellular@dfv.rwth-aachen.de, Subject: Does GSM track the physical location of a phone?, Message-ID: <9504200632.AA02651@lorien.dfv>.

[18] Public Law 103-414, sec. 103 (a)(2), Oct. 25, 1994, 108 Stat. 4281.

[19] For example, see Don Phillips, "Big Brother in the Back Seat? The Advent of the 'Intelligent Highway' Spurs a Debate Over Privacy," *The Washington Post*, Feb. 23, 1995, pp. D10-D11.

[20] Marcus Wigan, "The Influence of Public Acceptance on the Reliability of the Potential Benefits of Intelligent Vehicle-Highway Systems," *Information Technology & People*, special issue on "Identification Technologies and Their Implications for People," vol. 7, No. 4, 1994, pp. 48-62.

[21] Philip E. Agre and Christine A. Harbs, "Social Choice About Privacy: Intelligent Vehicle-Highway Systems in the United States," *Information Technology & People*, special issue on "Identification Technologies and Their Implications for People," vol. 7, No. 4, 1994, pp. 63-90.

The President's National Security Telecommunications Advisory Committee (NSTAC)

Wireless Services Task Force

Cellular Priority Access Services (CPAS) Subgroup Working Document

DRAFT

June 30, 1995
Version 4.0

CELLULAR PRIORITY ACCESS SERVICES SUBGROUP WORKING DOCUMENT SECTION ONE

PROJECT OVERVIEW

1.0 Purpose. This paper presents the conclusions of the Cellular Priority Access Service (CPAS) Subgroup of the President's National Security Telecommunications Advisory Committee (NSTAC) Wireless Services Task Force regarding the implementation of a nationwide cellular priority access capability in support of national security and emergency preparedness (NS/EP) telecommunications. This working document is intended to provide ongoing guidance and assistance to the Office of the Manager, National Communications System (OMNCS) and other federal government organizations in their efforts to encourage implementation of a nationwide CPAS capability. The OMNCS, in a letter from the President in January 1995, was tasked to "develop a capability to provide NS/EP users with priority access into wireless communications systems."

1.1 Background. The CPAS Subgroup's effort to define, standardize, and encourage deployment of a nationwide cellular priority access capability was prompted by recent emergency situations in which disaster response operations were hindered by cellular network congestion caused by extraordinary demand for mobile communication services.[1] In July 1994, the Wireless Services Task Force established the CPAS Subgroup to investigate the issues associated with the deployment of a nationwide CPAS capability.[2] The subgroup provided a forum for government and industry organizations to define, scope, and address the many technical, administrative, and regulatory issues related to this topic. It also provided a platform for developing a comprehensive CPAS implementation strategy.

---

[1] Hurricane Andrew -- August 1992, Hurricane Iniki -- September 1992, the Northridge California earthquake -- January 1994, and the Pittsburgh plane crash -- September 1994.

[2] In April 1993, the Industry Executive Subcommittee (IES) of the NSTAC instructed the Wireless Services Task Force to, among other things, "explore methods for incorporating priority access into wireless systems for NS/EP use." Following a study of the issue by a subgroup, the task force reported its findings and recommendations to NSTAC XVI in March 1994. The task force concurred in the need for a nationwide CPAS mechanism for NS/EP call attempts, which ". . . should be: implemented for all authorized NS/EP users at the Federal, State, and local levels; uniform across the Nation; interoperable across service boundaries; authorized by the FCC; [and] administratively consistent with the TSP Program." The task force recommended that the Government continue to pursue implementation of a single, nationwide cellular priority access capability.

1.2 User Needs. Priority access to the public switched network (PSN) for NS/EP users has been a topic of great interest to the Federal Government for several years. As evidenced by the OMNCS' work in developing the Government Emergency Telecommunications Service (GETS) program. As cellular telephone use has expanded, the need for priority access to cellular networks has become an issue of growing importance to the NS/EP user community. The need for priority access has been demonstrated time and time again by the inability of existing cellular networks to handle the sudden influx of call attempts. The most recent significant events were the Oklahoma City bombing in April 1995, the Pittsburgh plane crash in September 1994, the Northridge earthquake in January 1994, Hurricane Iniki in September 1992, and Hurricane Andrew in August 1992. Federal, State, and local officials responding to those disaster situations encountered frequent blocking of their cellular call attempts and were forced to redial repeatedly to gain access to the cellular system. This resulted in significant delays in critical communications affecting disaster response, particularly when landline networks were damaged and cellular networks become an important means of emergency communications.

In addition to using cellular networks during regional and national disaster response activities, local emergency management teams also use cellular when responding to less drastic situations such as auto collisions and forest fires. Often, local emergency responders, faced with budgetary constraints, do not have dedicated communication resources available to them and must rely upon public cellular communication networks as their primary means for coordinating emergency response activities. During local emergencies, there are likely to be sudden and drastic increases in the demand for cellular telephone services, especially during the first few hours of an incident. Of particular concern to State and local officials is the possibility that news reporters and other noncritical users often consume a significant amount of cellular resources during emergencies, making it nearly impossible for emergency personnel to access cellular networks. Successful deployment of a nationwide CPAS would greatly improve the ability of local disaster response agencies to use cellular networks in response to a wide range of emergencies. Each State and local jurisdiction, therefore, has a stake in the development of a CPAS capability. However, rather than have each jurisdiction develop its own CPAS capability, the subgroup found it desirable for the development of a nationwide approach,

allowing the Federal Government to coordinate the deployment of a nationwide CPAS capability. This would increase the likelihood that authorized Federal, State, and local NS/EP users could gain access to cellular telephone networks during disaster situations, especially as disaster response teams moved from location to location.

1.3 Scoping Effort. The CPAS Subgroup scoping effort was composed of a series of meetings providing an opportunity for cellular stakeholders to come together in a forum to discuss CPAS issues. The objectives of the CPAS Subgroup were to reach an understanding of cellular priority access user requirements, gain consensus on a service description, identify technical alternatives and approaches, determine the necessary administrative and authentication mechanisms, identify implementation steps and government project management roles, and develop a path forward for a nationwide implementation of cellular priority access services. This paper outlines the CPAS Subgroup's activities and presents its findings and recommendations.

1.4 Participants. The CPAS initiative has been supported by equipment manufacturers and cellular service providers, representatives from standards organizations and industry associations, and Federal and State government agencies and emergency management associations. More than 70 people have been involved in the effort. The CPAS Subgroup greatly benefited from the diversity of its participants and was successful at facilitating intelligent and useful discussion among a broad range of stakeholders. As the Federal Government encourages the implementation of CPAS, it should continue to seek advice from the various stakeholders that participated in the CPAS Subgroup. (The CPAS Subgroup participants are listed in Attachment 1.)

Although it should be relatively easy to identify Federal Government and industry organizations that should be involved in the deployment of nationwide CPAS, a greater challenge is to obtain consensus from State governments and their supporting emergency management associations regarding the specifics of CPAS implementation. The CPAS Subgroup believes the best way to attain consensus from the States is to include in the planning process those state organizations that represent the needs and interests of emergency

management and disaster response personnel. The key organizations identified are listed below:

National Emergency Management Association (NEMA) -- 50 State emergency management directors and representatives from 8 territories; 10 membership regions paralleling Federal Emergency Management Agency (FEMA) regions.

National Coordinating Council on Emergency Management (NCCEM) -- 15,000 members from city and county emergency management organizations; 10 membership regions paralleling FEMA regions.

National Association of State Telecommunications Directors (NASTD) -- 50 State telecommunication directors plus the District of Columbia; coordinates with the National Governor's Association.

National Emergency Numbers Association (NENA) -- 38,000 city, county, and State personnel involved in 9-1-1 and public safety; commercial members include telcos, equipment vendors, and public safety service providers.

National Association of State Nine One One Administrators (NASNA) -- 26 State 9-1-1 managers, administrators, and State telecommunication directors.

Association of Public-Safety Communications Officials (APCO) -- 11,500 managers of emergency communications centers, engineers/technicians, information systems specialists, dispatchers, equipment vendors, and consultants.

The CPAS Subgroup concluded that it was essential for the Federal Government in its role as project manager to continue to seek input from these groups and others identified to ensure a broad base of support for a nationwide CPAS.

CELLULAR PRIORITY ACCESS SERVICES SUBGROUP WORKING DOCUMENT SECTION TWO

SERVICE DESCRIPTION

2.0 Service Description Overview. This section presents an overview of cellular technology and call flow logic, describes discussions that the CPAS Subgroup held regarding government CPAS requirements, and documents specific recommendations for further government action to ensure the successful deployment of a unified, nationwide CPAS capability.

2.1 Basic Cellular Overview. Cellular telephone service is a mobile and portable radio capability that provides two-way switched voice communications in metropolitan and rural areas across the country. The basic cellular system consists of four parts: a mobile switching center (MSC), cell sites, radio spectrum, and mobile stations. The MSC is the central coordinating element for all cell sites in a system and contains the cellular processor and switch. The cell site provides the interface between the MSC and the mobile stations. The radio frequencies allow interconnection of the cell sites to the mobile stations. The Federal Communications Commission (FCC) regulates the amount of radio frequencies allocated to different wireless services to ensure equitable distribution, which often results in cellular's radio spectrum being overtaxed during disasters by a large number of users. Priority use of that spectrum by NS/EP users during disasters is the focus of this report. The fourth and final part of the basic cellular system is the mobile station. It contains a control unit, a transceiver, and an antenna system. Cellular telephony uses full-duplex mode and each mobile telephone is assigned its own telephone number. Attachment 3 provides a basic overview of cellular communication technology to give the reader a general understanding of the key network components potentially affected by nationwide cellular priority access services.

2.2 Government Cellular Priority Access Requirements. Several recent disasters have underscored the potential vulnerabilities of both wireless and wireline PSN services. When both wireless and wireline services are interrupted, wireless services are often reestablished more quickly because they are easier to restore. The mobility and widespread deployment of cellular communication often makes it the vehicle of choice, especially during

disasters or emergencies. NS/EP users responding to an emergency also rely on these same cellular communication networks to help them respond to the crisis. To some NS/EP users, cellular networks represent an inexpensive and available alternative to overburdened very high frequency and frequency modulated emergency networks. To others, cellular networks offer the only practical communications network available to coordinate both day-to-day and emergency response activities. Often, however, demand for cellular services during disasters outpaces capacity and customers are blocked due to overburdened facilities.

CPAS is designed to mitigate the problem of NS/EP cellular call attempts being blocked during emergency situations, providing call-by-call priority handling of call attempts originating from designated cellular users. When cellular networks are congested, CPAS would provide priority access to those networks for authorized NS/EP users.

The Government's requirements for cellular priority access were first documented in the Federal Wireless Policy Committee's (FWPC) document entitled *Current and Future Requirements for Federal Wireless Services in the United States*. The OMNCS, acting as focal point for the NS/EP user community, incorporated the FWPC requirements for cellular priority access into its document entitled *OMNCS Cellular Priority Access Implementation Plan*. The CPAS Subgroup examined each of these requirements and subsequently developed a CPAS service description that supported nearly all of the Government's concerns. Industry's analysis and comments on the Government's cellular priority access requirements are addressed in Section 2.3 of this paper, though each requirement listed below was agreed to in principle by the CPAS Subgroup's Technical Working Group. The following is a list of the high-level government requirements for CPAS:

Standard Terminal. Cellular Priority Access will be provided via commercially available cellular handsets. No unique, specialized handset will be required. The handset will provide periodic status information to the user, visually and/or audibly, indicating that the call is being processed. CPAS is linked to the ESN/MIN of the cellular subscriber.

Nonpreemptive. The Cellular Priority Access mechanism should not support any form of termination or interruption of current calls.

Information Independent. CPAS should be independent of the media transmitted on the radio channel. The voice channel that is acquired through the application of cellular priority access privileges should be able to support low speed data in addition to voice.

24-Hour Availability. Cellular Priority Access will be continuously available. This will preclude any requirement to activate the capability coincident with or subsequent to the declaration of a disaster condition.

Feature Invocation. Although Cellular Priority Access is continuously available, it will be selectively invocable when required.

Hand-off And Roaming. CPAS should support handoff and roaming in a manner similar to nonpriority calls, assuming there is a channel available. Intersystem roaming will be fully supported once IS-41 (Revision C) is deployed. Until that time, CPAS will provide only partial roaming capability.

Priority Level Assignment. The CPAS Administrative Office will assign priority levels to all users nationwide in accordance with CPAS guidelines and procedures. Cellular carriers will provide priority access based on the user's priority level.

Priority Access. When invoked, CPAS will provide NS/EP subscribers with priority access to the next available voice channel when all voice channels at a cell site are busy.

Priority Egress. Priority egress will not be provided in the initial service offering.

One-Time Subscription. Authorization and subsequent activation of CPAS shall be sufficient to provide nationwide service to the user. (Subject to roaming agreements).

User Identification. The capability will ensure that only authorized subscribers are permitted to invoke cellular priority access. On receiving a bid for access that is accompanied by an attempt to invoke cellular priority access, the responding cellular system will verify that cellular priority

access has been activated for the requesting end instrument.

Uniformity. CPAS will be uniform nationwide both technically and administratively, although some service provider options will exist. This will ensure that subscribers can be afforded the capability in all systems.

Transparency. Once a subscriber has invoked the Cellular Priority Access capability, the operation of the system shall be transparent to the subscriber. There shall be no further requirement placed on the subscriber except to wait for the call to be connected.

GETS Compatibility. CPAS users should be able to access the Government Emergency Telecommunications Service (GETS) via the 710 area code. Further enhancements will require additional study.

Feature Compatibility. Cellular Priority Access feature interactions shall be the same as those as defined for Priority Access and Channel Assignment (PACA) in IS-53-A, *Cellular Features Description.*

The Government requires multiple cellular priority access levels to serve the different functions of the NS/EP user community. To address these needs, a CPAS capability will be implemented via a priority queuing technique similar to, but not identical to, the technique described in the Telephone Industry Association (TIA) Priority Access and Channel Assignment (PACA) draft standard. The major differences between PACA and CPAS are:

- The Government's requirements would not permit subscribers to change their priority level at the time of invocation.

- PACA requires one queue per cellular system; the CPAS Subgroup is considering one queue per cell site. This is still an unresolved issue.

The CPAS service description does not include sufficient technical detail for manufacturers to develop and modify equipment. Therefore, more detailed technical

requirements should be developed to enable manufacturers to move forward with equipment modifications. These requirements should serve as a guide for equipment manufacturers and service providers to upgrade specific network components in support of CPAS. The CPAS Subgroup concluded that detailed technical requirements could be developed by an existing standards group or under contract to the Government.

2.3 Industry Analysis of Government Cellular Priority Access Requirements. The CPAS Subgroup discussed all of the Government's requirements for cellular priority access and concluded that while all might be technically feasible, some might not be practical at this time due to their degree of difficulty and the resulting costs. As new standards, features, and functionalities are added to cellular systems due to marketplace demand, these additional CPAS features might be reasonable to attain.

2.3.1 CPAS Feature Characteristics. IS-53-A, an industry standard, includes a description of priority queuing, referred to as Priority Access and Channel Assignment (PACA). The PACA priority queuing technique provides for a minimum of eight and a maximum of fifteen priority levels. The feature is invoked only when requested *and* an idle voice or traffic channel required for an origination request is not available. Each valid invocation attempt is slotted into a particular priority level depending upon the subscriber's service profile. Higher priority calls are queued ahead of lower priority calls regardless of when they arrived. Call requests of the same priority level are queued in the order of arrival. New requests may displace older requests if the new request arrives when the queue is full and has higher priority than other requests.

IS-53-A describes an alternative approach for providing CPAS that is based on channel reservation rather than queuing. Although the CPAS Subgroup endorsed priority queuing as the best method for fulfilling the Government's priority access requirements, some participants stated that queuing was not a panacea for all cellular congestion scenarios. These participants contended that situations could occur in which cellular channels would be held for extended periods of time and as a result, priority queuing would have limited benefit to NS/EP users. Such a situation occurred when the news media held most of the cellular voice channels during the police pursuit of O.J. Simpson. Some subgroup participants further contended that the

Channel Reservation (Alternate PACA) feature would ensure that NS/EP users could establish cellular calls in such a situation.

During the subgroup's deliberation on this issue, members investigated service provider data from southern Florida that indicated that, despite dramatic increases in the number of cellular call attempts, the average call holding time during Hurricane Andrew remained at predisaster levels. The CPAS Subgroup concluded that the issue was implementation specific and that PACA and Alternate PACA were complementary approaches to providing CPAS.[3]

Noted previously in this report were the recent incidents that have contributed to establishing the need for CPAS. Some members expressed concern early in CPAS Subgroup meetings, however, about the potential impact that CPAS might have on other users of the cellular system. To estimate CPAS' potential effects, the OMNCS sponsored several computer simulation studies that modeled cellular congestion during disaster situations. Results of those computer simulations have shown that cellular priority queuing would have minimal incremental impact on the blocking of nonpriority calls. The results also indicate that priority queuing could achieve significant reductions in call blocking for NS/EP users. The Government's simulation efforts are ongoing and current results are summarized in each successive version of the *OMNCS Cellular Priority Access Implementation Plan.*

The CPAS Subgroup discussed the possibility of using individual cell-site queues rather than a systemwide queue to simplify the technical implementation of CPAS. The subgroup endorsed systemwide queuing because it offered more effective service and was already supported by the queuing standard. Evidence was presented that indicated that handheld terminals could contact different cell sites from the same location, and did so frequently when they were used at the edges of cell coverage. Only systemwide queuing handled this situation effectively. In addition, the PACA feature description contained in IS-53-A provides for the assignment of priority calls to a queue on a systemwide basis. This capability supports intrasystem hand-off of a user's queue request as the user moves from one

[3] It should be noted that CPAS would not cause the termination or interruption of ongoing calls. Preemption of other calls was considered, but deemed unsuitable for inclusion as a feature in a public network.

cell to another. The system would maintain the user's queue position based on the user's priority level and time of priority request.

2.3.2 CPAS Deployment. The CPAS Subgroup also debated how the CPAS capability could be deployed cost effectively from a technical standpoint. The subgroup concluded that the OMNCS should disseminate its high-level technical requirements to State governments and emergency management organizations to specify service capabilities and operational scenarios. The OMNCS has since included its technical requirements in an outreach briefing being prepared for those audiences.

The CPAS Subgroup suggested that CPAS be phased in across the Nation, with priority deployment in high-risk areas. The OMNCS has identified high-risk service areas to help allocate resources effectively by implementing CPAS in areas where it is needed most. The OMNCS has included the high risk areas in a list of metropolitan statistical areas requiring CPAS within 1 year of the award of the federal wireless services procurement contract.

The CPAS Subgroup also debated providing a priority access arrangement to commercial customers and concluded that would be acceptable as long as the priority level assigned to such subscribers was below authorized NS/EP users. Commercial service offerings would provide a cost recovery benefit to cellular carriers, potentially reducing the costs to NS/EP users by utilizing the additional priority levels supported by PACA.

2.3.3 Terminals. The CPAS Subgroup discussed the Government's requirement for a standard mobile terminal and debated the likelihood that digital technology would eventually triple the capacity of existing analog cellular networks. As a result, the CPAS Subgroup agreed that potential CPAS users should be encouraged to purchase dual mode mobile terminals to take advantage of new digital technologies. The subgroup also speculated that when air interface standards were modified, all newly manufactured cellular mobile terminals would soon be compatible with CPAS technical requirements. In the meantime, CPAS stakeholders should work together to address the issue of CPAS compatibility with existing analog mobile terminals.

2.3.4 Performance Metrics. The CPAS Subgroup addressed the topic of CPAS feature performance metrics. The subgroup developed a high-level position on the measurements that needed to be collected to assist manufacturers in planning for data collection capabilities in their equipment. The subgroup concluded that it would be beneficial if the following data on the operation of the CPAS feature were collected by cellular equipment on a cell site-by-cell site basis, provided the development costs for such metrics are reasonable:

- Number of feature invocation attempts
- Number of successful attempts
  - By priority level
  - Per hour
- Number of unsuccessful attempts
  - Callers not queued or bumped from the queue
  - Calls deliberately abandoned or attempted another call while waiting
  - Callers lost while in queue because they did not answer the page and/or moved out of the service area
- Delay (time in queue)
- Blocking of plain old telephone system calls
- Percentage of channels occupied by NS/EP calls.

2.3.5 Standards Development and Industry Implementation. The CPAS Subgroup worked with industry standards representatives from the Alliance for Telecommunications Industry Solutions, the Telecommunications Industry Association, and the Cellular Telecommunications Industry Association to determine the best solution for implementing technical standards that would support CPAS implementation. Specifically, several subgroup participants submitted contributions to TR45.2 regarding the number of priority levels and other issues that should be supported by the PACA standard, which was formally approved by TR45.2 on December 13, 1994. The CPAS Subgroup recommended that PACA support a minimum of 7 and a maximum of 15 priority levels. With regard to the use of PACA to provide CPAS, the subgroup recommended to the Government that CPAS users not be able to change their priority levels dynamically, a PACA feature.

Additionally, the CPAS Subgroup received input from several industry experts indicating that three air interface standards need to be modified to fully support PACA. These standards are EIA/TIA553, IS95, and IS136/IS54. Each of these standards would require modification to provide notification that the user was in the queue, to advise the user of queue status, and to alert the user when a channel became available.[4] The CPAS Subgroup recommends that the OMNCS work with industry groups and the NSTAC to expedite the modification of air interface standards in support of CPAS

2.3.6 Future CPAS Feature Characteristics. Several government requirements were tabled because the subgroup considered them too costly or difficult to implement or ahead of the technological curve. An example of such a requirement is priority egress, which is not included as an initial feature in the CPAS Subgroup's service description due to the complexity anticipated in implementing such a capability. Priority egress would have to address how to handle competing access and egress calls of similar or different priority levels. Priority egress may be added later as the initial CPAS capability is expanded. The biggest obstacle to priority egress is associated with billing for long distance assets while an incoming long distance call originating in the wireline PSN is queued awaiting a voice channel. During that period the PSN has not yet connected the two callers. Since billing for the caller placing the call does not commence until the call is connected nobody is billed for the use of long distance wireline circuits until a voice channel is made available. This is an unacceptable situation which may be rectified in the future, but will prevent the inclusion of the priority egress characteristic in the initial rollout of the CPAS feature.

The CPAS Subgroup also debated the issue of GETS compatibility as a requirement and concluded that the Federal Government had not developed a document to describe CPAS/GETS compatibility. The CPAS Subgroup agreed that most GETS users should be eligible for CPAS service based on their mission. In response to the subgroup's concerns, the OMNCS prepared a CPAS/GETS interoperability issue paper in April 1995. The issue paper described GETS and the OMNCS' Cellular Priority Services (CPS) Program in an effort to determine the issues surrounding the eventual interoperation between the two services. The

[4]The following companies have agreed to champion the standards modification process: Motorola -- TR45.1 (EIA/TIA553), McCaw Cellular -- TR45.3 (IS136/IS54), and Airtouch Communications -- TR45.5 (IS95).

effort concluded that interfacing GETS and CPAS so that users could take advantage of their benefits would require that both the Government and industry evaluate and address several issues. Those issues would require consideration by the GETS and CPS programs individually, together, and in concert with industry.

The paper identified the following issues for the CPS and GETS program offices to address to provide interoperability and, ultimately, seamless interface between GETS and CPAS:

- Ensure opening of 710 area code within cellular switches
- Work with cellular carriers to develop an MSC capability to recognize the NS/EP code point within the High Probability of Call Completion protocol for roaming call forwarding
- Resolve CPAS call egress and work with cellular carriers to develop the ability of MSCs to recognize the NS/EP code point for cellular egress priority
- Influence the deployment of GETS access control functionality in cellular and/or local exchange carrier (LEC) networks
- Develop equal access provisions within cellular carriers
- Implement the ability to support GETS access for roaming cellular users
- Develop a list of cellular system location codes and dialing procedures for GETS users
- Provide cellular users with GETS capabilities as an extension to CPAS.

The Government recognized that, prior to addressing these issues, it should evaluate the complete effort required for CPAS/GETS interface development. For example, an initial study into the feasibility and cost required from all relevant parties may be required. Also, the eventual interoperability of GETS and CPAS may require software and/or hardware changes within cellular, LEC, and interexchange carrier networks. Finally, users may need to be