

Subcommittee on Civil and Constitutional Rights
Committee on the Judiciary
U.S. House of Representatives
(202) 226-7680 voice
(202) 225-3746 FAX

93 FEB 22 P7:06

FAX Cover Sheet

TO: Name: T. R. Stern
Office of Cabinet Secretary
Fax Phone: 456-2215
Voice Phone: _____

FROM: _____ Melody Barnes _____ Jan Pegues
_____ Ivy Davis-Fox _____ Ginny Sloan
X _____ Jim Dempsey _____ Deborah Ward
_____ Catherine LeRoy _____

Number of pages, including this cover 13
We are transmitting to your office on a Xerox 7020
PROBLEMS? Please call (202) 226-7680

SPECIAL INSTRUCTIONS:

Washington Telecom Week

 INSIDE
Washington
Publication

the Inside Washington look at federal telecommunications policymaking

(7.3) 892-8500

Vol. 2 No. 6 - February 12, 1993

STATE DEPT. MOVING TO STRIP AMBASSADOR RANK FROM TELECOMMUNICATIONS BUREAU

The State Department is quietly moving to strip its international telecommunications bureau of the rank of ambassador as part of a massive reorganization being spearheaded by the Clinton Administration, and sources say the move may be strongly resisted by Congress and the telecommunications industry. The department's Bureau of International Communications and Information Policy (CIP) would be folded into the Bureau of Economic and Business Affairs (EBA), and the rank of ambassador for the head of the CIP would be seriously downgraded. But State cannot make these changes without the approval of Congress, and the reorganization effort may fly in the face of earlier legislation to create the CIP.

continued on page 17

In an apparent reversal...

CLINTON REPORTEDLY READY TO PUSH CONGRESS FOR NEW WIRETAP LEGISLATION

In what would be a turnabout from a position taken several weeks ago, the Clinton White House is considering asking the 103rd Congress for passage of new federal wiretap legislation that could cost telecommunications and computer equipment manufacturers billions of dollars to implement, key congressional sources said this week. This development comes in contrast to President Clinton's decision last month to distance the Administration from the controversial wiretap issue, a position the President's advisers urged him to take shortly before Clinton assumed office.

continued on page 19

Responding to local exchange competition

USTA PROPOSES SWEEPING CHANGE IN ACCESS CHARGE POLICY, RECASTED PRICE CAPS

The U.S. Telephony Association (USTA) has proposed a sweeping change in federal policy governing access charges and price caps in response to the advent of local exchange competition, according to a copy of the proposal obtained by Washington Telecom Week. The USTA effort is the second iteration of an access policy restructure plan that was proposed last year and launched a broad effort at the state level to review access policy. The newest version is geared to influence an internal staff project at the Federal Communications Commission on access restructure that is expected to be one of the first issues to

continued on page 20

ITO SAYS NAFTA WILL LEAD TO MAJOR NEW MARKET IN MEXICO FOR ENHANCED SERVICES

A new analysis by the International Trade Commission (ITC) concludes that the North American Free Trade Agreement (NAFTA) will create a significant new market opportunity in Mexico for U.S. firms in the area of enhanced telecommunications services. The Mexican enhanced telecommunications services industry is currently less than 1% the size of the U.S. industry. Although the Mexican market for enhanced telecom services is relatively undeveloped, it displays substantial growth potential, the report says.

The development of this market is important not only to telecommunications service providers who believe that these sectors will account for an increasing share of total revenues, but also for most.

INSIDE THIS ISSUE

Collocation: States' revolt appears to be linked to RBOC serving areas	3
FCC Eyewash: Disposition of 224 complaints seen as show for Clinton White House	4
White Paper: Telecator urges FCC to halt common-private carrier distinction	6
House Spectrum Bill: Legislative effort gains speed; auctioning issue to be addressed	10
Interim Chairman: Choice of Qualls seen as setback for Hollywood	11

Senior positions may be eliminated under the reorganization of the CIP. For example, the CIP used to be headed by Bradley Holmes, who was assisted by two deputies. "It may be that not all of those positions will remain," one source said. "There may be fewer high-level people and not with the same titles."

The source said there is no intention to reduce the ability of the CIP Bureau to carry out its international functions but to more closely integrate the bureau with other functions of State. The EBA contains divisions of international finance that track developments at the International Monetary Fund and other agencies. It also has an office of trade policy and focuses on issues such as transportation, aviation, energy issues and other areas that require international agreements.

The CIP Bureau handles a whole host of telecommunications issues, including the oversight of possible telecommunications joint ventures with many of the former Soviet republics and the provision of liaison functions for the ITU and the World Administrative Radio Conference. — Joe Burey

CLINTON EYES POSSIBLE SUPPORT OF FBI WIRETAP BILL... begins page one

Clinton's reported willingness to reverse himself and now embrace the thorny issue of new wiretap legislation — an idea first proffered by Justice Department and Federal Bureau of Investigation officials under the former Bush Administration — comes as a shock to many industry observers. Others say it may be that Clinton is searching for "some middle ground" on which he can stand in an effort to placate certain conservative elements within the Congress.

One source suggested the President may be willing to agree to "most if not all" of the plan favored by Justice and the FBI in exchange for support from key conservatives in Congress for Clinton's proposal to lift the ban on homosexuals serving in the military.

"I don't think the President will go along with everything the Bureau is asking for," the source said. "But chances are [the President] will be willing to give them much of what they want — that is, assurances backed up by federal law that industry will provide law enforcement with the ability [it needs] to access these new technologies."

Prior to Inauguration Day, William Sessions, the currently embattled director of the FBI, met with top-level members of the Clinton transition team in what was subsequently described as an unsuccessful effort to sell the new Administration on the merits of the Bureau's proposed digital telephony legislative package.

Sessions had asked the new President to include the Bureau's wiretap proposal in a comprehensive crime bill package Clinton wants to present to Congress during the first 100 days of his Administration. The proposal was virtually the same plan the House telecommunications & finance subcommittee rejected late last year.

The President's advisors, consequently, told Clinton to avoid endorsing the FBI's plan for fear that the controversy surrounding it would stall congressional action on a Clinton-backed crime bill.

Now, Clinton reportedly is having second thoughts, sources say, and a new, slightly different FBI wiretap proposal could garner the President's endorsement during this first session of the 103rd Congress.

Such a possibility is so real that key congressional staffers on Tuesday (Feb. 9) warned telecommunications and computer industry representatives gathered in Washington, D.C., for a meeting of the Electronic Frontier Foundation's so-called Digital Privacy Coalition to be on the lookout for renewed wiretap legislative efforts during this session of Congress, sources close to the group said.

The Administration apparently now seems markedly less inhibited about accepting the Justice Department's position, one source said. The President reportedly is concerned that failure to address the wiretap issue will result in "the loss or impairment of the [FBI's] ability to conduct court-ordered electronic surveillance" and could "catastrophically inhibit the investigation of organized criminal groups."

The FBI is concerned about law enforcement's ability to tap into newly developed digital telecommunication technologies as well as a host of new telephone services, such as call forwarding and last number re-dial. Also, the Bureau is concerned that emerging computer technology could hamper court-authorized wiretap operations.

EFF and the coalition, on the other hand, contend the Bureau's concerns are without much basis. They maintain that the telecommunications industry has always had a good working relationship with law enforcement and that no changes in current federal wiretap and privacy laws are needed to ensure the continuation of that relationship.

Last year, the coalition "reacted to events rather than trying to affect events before they happened," one source close to the group said. But, in light of these recent concerns about which way Clinton will move on the wiretap issue, a decision was made at Tuesday's coalition meeting to "change the strategy, to become proactive rather than reactive," the source said. — Jim Rogers

February 23, 1993

FROM: Don Edwards
Chairman
Subcommittee on Civil and
Constitutional Rights
House Judiciary Committee

Patrick J. Leahy
Chairman
Subcommittee on Technology
and the Law
Senate Judiciary Committee

RE: Digital Telephony -- The Bush Administration's
legislative proposal mandating interception features
for telecommunications equipment

Summary

Last year, the Bush Justice Department and the FBI proposed sweeping legislation that would require the wiretap friendly design of all telecommunications equipment, including all computer networks and all interoffice phone systems.

The Bush Administration, on the advice of the FBI, argued strenuously that advances in telecommunications technology would soon make it impossible for law enforcement agencies to execute court-ordered electronic surveillance, thereby allowing criminals to carry out serious criminal activity without detection. In some cases, Justice argued, advanced technology and features had already frustrated intercept orders. Comprehensive legislation was necessary, the Administration claimed, to preserve a critical investigative technique.

It rapidly became apparent, however, that the legislative proposal was premature and perhaps unnecessary:

-- The wiretap laws already impose a duty on all companies to cooperate with wiretap orders by providing all necessary information, facilities and technical assistance.

-- A number of the technologies or features cited by the FBI (digital telephony, PBXs, and call forwarding) have been around for many years, undercutting the claim that the problem is new and urgent.

-- The telecommunications industry flatly denied that the major new technologies would be impossible to tap.

-- When pressed, the FBI could not cite a single clear case of an emerging technology frustrating a wiretap order. The telephone companies stated that they knew of no case either. (Some cellular systems, while they can be tapped, could not accommodate a large number of intercepts simultaneously -- a

problem of capacity, not one of incapability.)

-- The General Services Administration, which is responsible for maintaining the federal telephone system, opposed the FBI proposal, concluding that it would make it easier for criminals, spies and hackers to penetrate the phone network, could hurt US industry, and might not be necessary.

-- The phone companies promised to cooperate with the FBI in developing solutions to any future problems, and formed a technical working group for that purpose.

The Administration's first draft bill, which attracted immediate, widespread opposition, was withdrawn and a second, quite different version was issued. It, too, was unacceptable to industry and privacy advocates, and was never introduced.

Contrary to Justice Department and FBI claims, the Bush proposal would not have merely preserved the status quo. It would have mandated, for the first time ever, that interception features be incorporated in the design of telecommunications and computer equipment. Broadly interpreted, it would have required major redesign and retrofitting of telecommunications systems. Finally, it required a comprehensiveness in surveillance coverage that has never been available to the government.

Undeniably, developments in telecommunications pose both challenges and opportunities for law enforcement. But at this point, there is no agreement between law enforcement and industry on what the problem is, let alone on the cost and benefits of possible solutions.

Finally, it should be noted that the Administration proposal did not address encryption, which also threatens law enforcement electronic surveillance. Virtually unbreakable encryption is now available. Government control of encryption technology is intensely controversial itself. Hoping to avoid that debate, the Bush Administration digital telephony proposal did not address encryption. That led many to ask why the FBI wanted to force equipment redesign to allow it to capture the message stream to a particular target if it could not decode the signal anyhow.

Recommendation

The legislative proposal remains premature. The work of the industry technical committee should be supported and its intercept recommendations should be analyzed carefully before new legislation is advanced. The electronic surveillance statutes, which already mandate cooperation with intercept orders, may need to be clarified. But if legislation is pursued, it should be narrow and focused, to avoid unintended harm to the security and privacy of telecommunications.

Background

The FBI's concerns can be traced to two major trends in telecommunications: the proliferation of service providers following the break-up of the Bell system, and the explosion of technologies and services. Irreversibly, law enforcement cannot conduct electronic surveillance as it has in the past. While more information is susceptible to law enforcement interception, it is sometimes harder to intercept and translate into useable form. One stop shopping is no longer possible: a particular target may communicate by regular telephone, cellular phone, E-mail and fax, using different service providers for each medium.

One key point to recognize, however, is that the FBI and other agencies have been very successful in intercepting a wide range of voice and data transmissions, despite the introduction of new technologies. The FBI routinely intercepts cordless and cellular calls, data transmissions, and faxes. Much more information about people's lives and business dealings is being transmitted electronically, and law enforcement -- led by the FBI -- has been aggressive in capturing that information. Cellular systems, for example, allow law enforcement to track a subject's location whenever he uses his phone.

On the other hand, the new technologies do make it harder to conduct telecommunications surveillance. Of primary concern to the FBI is the gradual transition of the national phone system from an analog mode to a digital mode. In addition, fiber optics, call forwarding services, personal communications networks, advanced cellular technologies, other radio based technologies, and encryption also pose challenges. For each technology, the FBI has a daunting amount to learn and new equipment to acquire. (Some of the specific technologies are discussed at greater length in an attachment, Tab 1.)

For research on these technologies, the Bureau has a state-of-the-art Engineering Research Facility on the Marine base at Quantico. For research on telecommunications interception alone, the FBI received \$15 million in funding in fiscal year 1992 and sought \$12.7 million more for FY 93. This is part of a 5 year research effort budgeted at about \$80 million, intended to preserve and enhance the FBI's communications intercept capabilities. In addition, the Bureau spends considerable sums on the acquisition of other surveillance equipment.

But it is unclear that the Bureau has pursued in a timely manner the development and procurement of new equipment that would overcome the problems posed by the new technologies. Indeed, the FBI is pursuing legislation because it would like to minimize the number of software and hardware components it has to develop and procure to intercept all the various systems available now and in the future.

Bush Administration legislative proposals

Over the past 4 or 5 years, the FBI has discussed its concerns with telephone company security managers, corporate executives and legal counsels. The companies promised cooperation, but neither the companies nor the FBI ever developed specific interception strategies for specific technologies or services. The FBI became frustrated with the lack of progress and concerned that services and technologies were being designed without conscious effort to accommodate law enforcement surveillance needs. This led the FBI to press for legislation.

In February 1992, the Bush Administration began circulating legislation to require the FCC to set design standards for telecommunications equipment, to ensure that it could be readily tapped. The proposal immediately attracted widespread opposition and was never formally presented to Congress.

In late April 1992, the Bush Administration began circulating a second proposal, which placed the regulatory authority with the Attorney General rather than the FCC and specified six general performance criteria for telecommunications systems. The legislation would have required that all telecommunications equipment and technology be designed, and all existing equipment be retrofitted, to meet the six criteria, unless the AG granted a waiver. (All government phone systems were automatically exempt.) The Attorney General would have the exclusive authority to decide whether or not a system met the criteria. This second proposal was formally transmitted to Congress on September 14, but was never introduced. A copy is attached as Tab 2.

A coalition of telephone companies (including AT&T, NYNEX, US WEST), computer companies (including IBM and Digital Equipment Corp.), cellular service providers, software developers, equipment manufacturers and civil liberties advocates formed in opposition to the legislation. A copy of a paper prepared by the coalition opposing the legislation is attached as Tab 3.

Is the problem immediate or prospective?

To date, law enforcement has not provided us case-specific examples where it was unable to carry out a court-authorized wiretap because of a new technology. At a March 18 hearing in the House, the FBI Director could not cite a single case where technology had frustrated a wiretap order.

The FBI is conducting a survey through its field offices. Problems are being reported, but the survey does not yet have the details necessary to determine whether claimed difficulties were the result of local lack of expertise, or technology that has been around for a long time and had always posed problems.

Several limited problems have been identified, but none of them is new:

(1) The cellular systems in New York have not been able to handle the unanticipated volume of interception orders. That is not a problem inherent in the technology. The cellular systems can be tapped quite easily, but they could not accommodate simultaneously the number of orders that were issued. The problem primarily affected dialed number recorders (pen registers), not voice wiretaps. In any event, the cellular companies are voluntarily modifying the switches at their central offices so they can accommodate multiple simultaneous intercepts.

(2) Call forwarding has long posed a problem: calls that are forwarded upon a target's request to another number evade a tap placed anywhere on the target's line. This was cited as a problem in the 1976 report of the national wiretap commission.

(3) PBXs (private branch exchanges) are switchboards which distribute internally the many calls to large businesses. PBXs are connected to one or more trunk lines, which carry many messages at once. Some PBXs have not allowed the isolation of calls to and from a particular office within a system, if law enforcement is targeting a specific person in a company. Law enforcement can effect the tap through a surreptitious entry to the person's office, but that is risky. They would rather go to the PBX manager and attach the tap at the PBX. Some systems allow that, some don't.

Not a status quo proposal

The Bush proposal does not merely preserve the status quo. In addition to protecting law enforcement's wiretap ability against future erosion, it would rectify problems law enforcement has faced for years:

- The first cellular systems began operating in 1983. The wiretap capacity problem arose soon thereafter with the unexpectedly rapid growth of cellular use.
- PBXs have been a feature of offices for decades, and there have long been PBXs that could not isolate calls from a particular extension.
- Call forwarding has been available since 1965, and law enforcement has long known that forwarded calls will circumvent a tap placed on the target's line.

These problems may need to be fixed, but it is not accurate to say, as the FBI has, that addressing them merely preserves the status quo.

In another respect, the Bush proposal went beyond the status quo: it was premised on a notion of 100% coverage, an assumption that the wiretap laws entitle law enforcement to 100% of the electronic communications of a target regardless of equipment, medium or physical location. Such coverage has never been available. Mandatory 100% coverage finds no support in the language or legislative history of the wiretap laws. While the debate over whether there should be wiretapping was resolved in 1968, when the current wiretap law was adopted, the 1968 law did not address the kind of issues the FBI is today raising.

In June 1992, the FBI issued a list of law enforcement "Requirements" (Tab 4) to spell out what the legislation was intended to achieve. Specific provisions in the Requirements and in the bill itself show that this is not a status quo proposal:

(1) It has always been the case that when an intercept subject uses pay phones or travels out of town, the government cannot intercept his calls unless it knows or can guess what phone will be used and places a separate tap on that phone. If the subject uses a cellular phone and roams outside his normal service area, placing his calls through a new service provider, the government again cannot capture those calls. But the FBI's Requirements make it clear that the government wants to capture all a subject's calls regardless of the location from which they are made. The Requirements specifically state that telecommunications systems should be designed to rout all a subject's calls to an intercept access point. That may or may not be desirable, but it is not the status quo.

(2) The proposed statute says that the intercepted conversation must be provided to law enforcement at a "remote" facility. In defining what remote means, the Requirements note that "coast-to-coast transport may be required." The FBI is apparently seeking to be freed from the geographic constraints that have previously limited interceptions. Transferring calls across the continent so they pass through interception nodes may or may not be appropriate, but it is certainly not the status quo.

(3) The Requirements state that law enforcement wants to collect identifying information on forwarded calls, including information identifying "intermediate points if a call is forwarded multiple times." The phone system has not been designed uniformly to provide information that comprehensive. As a call is forwarded from number to number, the message may carry with it only the amount of routing information necessary to get it to its next location; identifying information on intermediate locations, if not necessary for billing purposes, may drop off.

(4) Inexplicably, the Bush proposal deviated from current law. The wiretap law currently requires all electronic communication service providers to furnish all information, facilities and technical assistance necessary to carry out an interception "unobtrusively." The FBI's proposed bill, while leaving that language in place, would also require electronic service providers to ensure that intercepts are carried out "without detection by the subject of the intercept or any subscriber." Is "without detection" the same as "unobtrusively" or is it a higher standard? If it is the same, why use different words?

(5) Current law provides that interceptions must be accomplished "with a minimum of interference" to the services being tapped. The new proposal would require that the intercept be accomplished "without degradation" to services. "Without degradation" sounds more absolute than "with a minimum of interference." Is it the same or not?

Industry cooperation -- technical committee

The phone companies' position has been that they have always cooperated with law enforcement to ensure that wiretap orders were carried out, and that they would continue to do so in the future, so legislation was not necessary. The FBI's response has been that legislation is necessary to require the smaller service providers to comply. The Bureau has not cited any failure by smaller companies to cooperate.

The threat of legislation did focus industry resources on the issue. In March 1992, in response to circulation of the initial draft legislation, an industry technical committee was formed with FBI participation. The technical committee and action teams focusing on specific issues have been meeting regularly to examine each problem area identified by law enforcement. The committee is preparing a series of reports detailing precisely how law enforcement can intercept each of the new technologies and features. The costs and risks of the various approaches have not yet been analyzed. The so-called switch or software solution, which the FBI favors, is expensive and poses serious security risks.

Last summer, Attorney General Barr told the regional Bell operating companies (RBOCs) that the Justice Department would be of no assistance to them on anti-trust issues unless the RBOCs began serious compromise discussions on the wiretap legislation. The discussions took place, but were inconclusive.

This is not, however, an RBOC vs law enforcement issue. The Bush Administration apparently believed that if it could make a separate peace with the RBOCs then everybody else would have to come along. The telecommunications industry has become far too complicated for that.

Implications for Security, Privacy and Competitiveness

The very technologies that concern the FBI make telephones more secure from intrusion and fraud and more private. Indeed, subscribers to telephone services, especially business subscribers, are demanding greater security in the phone systems they use, and consequently phone systems are being designed so they are harder to penetrate.

The Bush Administration proposals could have mandated a "dumbing down" of U.S. telecommunications security, leaving the communications of private citizens and American companies vulnerable to hackers, criminals, competitors, and foreign intelligence services. Telephone fraud is already a serious problem. If the phone companies were to create a way for the FBI to get into a phone system, that vulnerability could be exploited by others with fraudulent motives.

If U.S. companies forego certain security measures to accommodate the FBI, that will likely hurt the competitiveness of American products abroad. Who abroad would buy American-built phone equipment designed so the FBI could easily tap into it?

One indication that the Administration recognized the security implications of their proposal is found in the fact that, under the latest draft, phone equipment used by the federal government would not have to meet interception standards. The government did not want to be required to buy equipment meeting DOJ wiretap standards, presumably because it is worried about the vulnerability of its own communications.

Attachments

Attached are:

- (1) a summary of some of the technologies and services at issue;
- (2) the Bush Administration's second legislative draft and supporting materials;
- (3) a paper signed by computer and telecommunications companies and public interest groups, opposing the legislation;
- (4) the "Requirements," a statement of asserted law enforcement needs, prepared for the FBI.

What are the technologies and services at issue?

In presentations of the Bush Administration proposal, the term "digital telephony" is often used to encompass a number of related but quite distinct technologies and services.

Digital telephony refers to the electronic transmission of information in discrete, discontinuous binary form, as a string of ones and zeros, as compared with "old-fashioned" analog transmission, which employs a variable, continuous waveform where the height and length of the waves represent the information value. Digital encoding of information forms the basis of many modern technologies, from computers to compact disks; in telecommunications, it offers large advantages in terms of carrying capacity, speed and flexibility.

Law enforcement cannot use its old analog equipment to listen in on a digital line. New equipment must be purchased and personnel trained in its use. But digital transmission, per se, is not the problem; with the proper equipment, digital signals can be translated to voice.

A complicating problem is that digital transmission allows multi-plexing, the melding of communications from multiple customers on a single pair of wires. Conversations are broken up into tiny packets and transmitted in a stream of data with many other conversations. The challenge is to isolate the calls associated with a particular target, to the exclusion of all others. In an analog system, telephone companies would provide the FBI with "cable and pair" information, identifying a particular set of wires exclusively associated with a single customer. That unique set of wires appeared at numerous points (known as an "appearances") in the transmission infrastructure.

The FBI is concerned that in a digital system these appearances are disappearing. When the phone network is digital from end-to-end (that is, all the way down to each customer's premises), the FBI fears there will no longer be a pair of wires unique to each subscriber. The telephone companies claim that this is not really so. They argue that they will always have the ability to isolate a particular customer's calls at several points, since the ability to do so is crucial to their providing quality service.

A term used to describe the end-to-end digital system is ISDN, which stands for Integrated Services Digital Network. The ISDN is embodied in an international standard -- a set of technical and operational specifications -- that defines how to transmit voice, data, facsimile, and video in digital form over a common network linking telephones and computers.

PBX stands for Private Branch Exchange, which means a switchboard, the private switching system used in most offices and businesses. PBXs allow intra-office calling and they allow

calls made from the outside to a general number to be routed to individual employees. PBXs may provide such features as voice mail and individual station call accounting (recording the number called from each extension and other data).

Cellular telephones (such as car phones) use radio signals. Each city or county is carved up into small areas called cells, each of which has a low power receiver/transmitter, which all connect through a switching center to the local phone network.

Law enforcement may have been limited in carrying out intercepts of cellular calls in some cities, but that was a capacity problem, not a capability problem, i.e., the technology allowed taps but the switches did not have enough "ports" to hook the taps to. The switch manufacturers have been upgrading their switches. One of the two major cellular companies in New York recently implemented a change in its switch that can be expanded to accommodate 1500 simultaneous intercepts.

Call forwarding is a service offered by most local telephone companies, by which a customer who will be away from home can direct that his calls be forwarded to another number where he will be. The call forwarding order is lodged in a computer at the phone company's central office switch, and can be changed as often as desired.

There are other services that are under development or in the early stages of deployment:

The term personal communications service (PCS) encompasses a broad range of radio communications services that free individuals from the constraints of the wireline public switched telephone network and enable them to communicate when they are away from their home or office telephone. Basic forms of PCSs include the cordless telephone and cellular phones. In the future, it is expected that PCSs will be based on hand-held portable phones, permitting individuals to use the same device regardless of location and to be reached in any place using a single telephone number.

A personal communication number (PCN) is a single phone number that rings wherever you go. PCN is already available on a limited basis through AT&T, which offers subscribers a permanent long-distance number that begins with "700." The subscriber can program the service to direct that any calls to his 700 number be routed to the nearest phone. This is similar to call-forwarding, but call-forwarding requires that the subscriber go back to the original phone to enter the new destination.