Summary of Testimony Of Thomas E. Wheeler

Cellular Telecommunications Industry Association

February 5, 1997

House Commerce Committee

Subcommittee on Telecommunications, Trade and Consumer Protection

Federal law prohibits eavesdropping on electronic communications, and the law does not make privacy rights dependent on the technology used for that communication. As a result, calls made on traditional wireline telephones, cellular telephones, cordless phones, or other forms of electronic communication such as e-mail all receive the highest degree of communications privacy protection under federal law.

Throughout most of the history of analog FM signaling, a lack of demand for low-cost analog scanners made these communications relatively secure. As low-cost radio scanners became more prevalent, Congress, in 1986, first expanded the law to specifically protect the privacy of electronic communications, and then again, in 1992, amended the Communications Act of 1934 to further strengthen the privacy rights of wireless phone users by banning FCC authorization, or the manufacture and importation, of cellular frequency radio scanners. Despite these prohibitions, low-cost scanners that can receive cellular frequencies remain readily available to the public. A gray market in scanner modification has mushroomed in response to demand from electronic stalkers and confusion over legal prohibitions.

Instead of reacting to privacy concerns after new technologies become popular, policy-makers should make sure privacy principles are applicable to all forms of protected communications on a forward looking basis. Extending protections or trying to ban a specific type of eavesdropping gear after it has already become widely available is difficult. For instance, while our current law addresses scanners used to eavesdrop on cellular frequencies, it does not clearly prohibit equipment that can intercept signals from personal communications services, or

other forms of commercial mobile radio services. Unless Congress takes a forward-looking approach, history will likely repeat itself as digital scanners and decoders, though expensive now, drop in price in the future.

Deployment of more secure digital commercial mobile service equipment is being frequently delayed or blocked at the local level in contravention of Congress' intent to promote the availability of wireless services nationwide at reasonable cost. Policy-makers can and should act to mitigate arbitrary barriers to the development and deployment of this infrastructure.

The burgeoning ranks of Americans who utilize electronic communications and who subscribe to commercial mobile services are entitled to the fullest extent of privacy protection the law and regulations can provide. In order to address specific privacy problems relating to scanners, policy-makers should consider making clear the intent to prohibit the availability of devices that facilitate the unlawful interception of protected communications; and, if necessary, tighten or better enforce laws and regulations applicable to scanner alterations and their illegal use. Policy-makers should also act to remove arbitrary barriers to the cost-effective and timely deployment of or conversion to more secure digital commercial mobile services wherever practical.

TESTIMONY OF

THOMAS E. WHEELER

PRESIDENT & CEO

CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION (CTIA)

BEFORE

THE HOUSE COMMERCE COMMITTEE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

FEBRUARY 5, 1997

Thank you, Mr. Chairman, and members of the Subcommittee, for the opportunity to present testimony on an area of law and commercial enterprise where there seems to be a good deal of confusion about what is permissible behavior and what is not. I am Thomas E. Wheeler, President and CEO of the Cellular Telecommunications Industry Association (CTIA), representing all categories of commercial wireless telecommunications carriers, including cellular, personal communications services (PCS), enhanced specialized mobile radio (ESMR), and mobile satellite services.[1] My testimony today will focus on the law as it applies to electronic privacy, discuss how that law is often ignored or circumvented with respect to wireless communications, demonstrate the ease by which legal scanners may be modified to illegally intercept wireless calls, and discuss steps Congress and the FCC can take to ensure that Americans engaging in electronic communications get the privacy protection they deserve.

General Principles of Privacy

Federal law prohibits eavesdropping on electronic communications, and the law does not make privacy rights dependent on the technology used for that communication. As a result, calls made on traditional wireline telephones, wireless telephones, cordless phones, or other forms of electronic communication such as e-mail all enjoy the highest degree of communications privacy protection under federal law.[2] Importantly, these

[1] CTIA is the international organization which represents all elements of the Commercial Mobile Radio Service (CMRS) industry, including cellular, personal communications services, enhanced specialized mobile radio, wireless data, and mobile satellite services. CTIA has over 750 total members including domestic and international carriers, resellers, and manufacturers of wireless telecommunications equipment. CTIA's members provide services in all 734 cellular markets in the United States and personal communications services in all 50 major trading areas, which together cover 95% of the U.S. population.

[2] In the original 1934 Communications Act Congress made unlawful the unauthorized interception and divulgence of the contents of any radio communication. [47 USC §605 (a)] In addition, 18 USC § 2511

privacy protections for electronic communications are prospective, meaning that they extend forward to these services and variants of electronic communications that have not yet reached the mass market. This prospective privacy protection for electronic communications will become increasingly valuable to all American as the next five years will witness explosive growth in the use of these technologies by consumers.

Wireless Subscribers

	1996	2001	2005
Cellular			
Donaldson[3]	43,500,000	74,125,000	91,463,000
Paul Kagan[4]	44,300,000	79,900,000	94,900,000
PCS			
Donaldson	300,000	19,775,000	40,438,000
Paul Kagan	300,000	18,400,000	37,200,000
ESMR			
Paul Kagan	480,000	4,268,000	10,355,000
Mobile Satellite			
Business Week[5]			7,000,000
Cordless*			
CEMA[6] w/7% annual growth	59,000,000	83,000,000	108,000,000

*Cordless is not a subscription service. Number refers to units in use.

makes it illegal to intercept, to use a device to intercept, to disclose, or to use information that was obtained through interception of a wire, oral, or electronic communication.

[3] Donaldson, Lufkin & Jenrette, "The Wireless Communications Industry Report, Summer 1996," Table 4, pg. 14.

[4] Paul Kagan Associates, Inc., "Wireless Telecom Investor," No. 91, 9/30/95 & No. 102, 8/29/96.

[5] Business Week, January 27, 1997, pg. 63.

[6] "Consumer Electronics Industry to Experience 37% Growth by New Millennium" from http://www.cemacity.org

To continue the analogy between the wireline and wireless environments, the same criminal penalties will apply to someone who intercepts an electronic e-mail as to someone who eavesdrops on the hardwire delivery of e-mail to a computer system.

Electronic communications carried by a variety of means other than CMRS are also susceptible to eavesdropping, with an example being cordless telephones. Cordless telephones connect into the public switched telephone network and are recognized by the FCC as component elements of the network. As such, cordless telephones now receive the same level of privacy protection under federal law as do calls made on traditional wireline telephones. However, cordless telephone communications did not receive full privacy protection until 1994. Further, while the manufacture and importation of cellular scanners has been criminalized, this prohibition does not extend to scanners used to intercept other types of electronic communications, such as cordless telephones.

Cordless telephones are not mobile, and they are more susceptible to eavesdropping than a cellular telephone. Because a cellular telephone changes frequencies as it travels from cell to cell, it is difficult to intentionally listen to a cellular conversation for more than a few minutes if the caller is moving. As a cellular telephone moves from cell to cell, the network automatically selects one channel out of 790 available on which to carry the conversation. As a result, the person eavesdropping on the conversation has only one chance in 790 of picking the signal up again unless he intentionally searches for it. With a cordless telephone, on the other hand, the telephone usually has only between three and 25 potential channels, and the cordless telephone is relatively stationary, so once the scanner finds you, there is no getting away.

The example of the cordless telephone raises an important policy consideration. Instead of reacting to privacy concerns after new technologies become popular, policymakers should make sure general privacy principles are applicable to all forms of protected communications on a forward looking basis. Extending protections or trying to ban a specific type of eavesdropping gear after it has already become widely available is difficult. As we will see, for most of the history of analog communications a lack of available, low-cost scanner equipment made those analog communications relatively secure. In the case of digital wireless communications, although digital scanners and decryption techniques are expensive now, they will certainly become less so in the future.

A Brief History of The Development of Wireless Communications

In 1935, Edwin Howard Armstrong unveiled a breakthrough technique for taming radio static known as analog frequency modulation, or analog FM. Analog FM became the standard for radio transmissions in the United States for the next 50 years, and is still utilized for over the air broadcasting, television audio signals, and public safety communications. During the 1940s, the strategic value of wireless communications for military use forced refinements in mobile communications and two-way radio, and in 1946 the FCC licensed the first commercial public radiotelephone in St. Louis, Mo.

Cellular radio technologies were developed in the 1970's, when new techniques to improve spectrum efficiency, improved call switching technologies, and microelectronics combined to yield a service that offered the potential for portable, ubiquitous wireless service. A crucial development in cellular technologies was the ability to seamlessly "hand off" calls between cells in a network and between networks, thus allowing both mobility and the opportunity for the reuse of channels as callers entered and left specific cells.

Analog FM signaling was used in these early cellular systems, and in fact was the only proven and widely available voice signal technology at the inception of cellular commercial mobile radio services in 1983.

While it was understood that standard, unencrypted analog FM signaling could be passively intercepted with a simple FM receiver tuned to the relevant frequencies being utilized, this drawback had also applied to the various forms of mobile communications that cellular service began replacing.

Demand for cellular services grew rapidly as customers migrated from the older mobile radio systems to the new cellular systems. Even though these subscribers generally understood that their communications were susceptible to eavesdropping, interest and demand made cellular telephones the fastest growing consumer electronics market in history. While add-on security features were developed for analog systems that can thwart passive eavesdropping in most cases, those features typically require specialized handsets that cost substantially more than standard analog handsets.

This growth in "electronic" communications, led by cellular telephony and the rapidly developing computer industry, led Congress to recognize that federal privacy protections should apply equally to both landline communications and electronic communications. In 1986 the Electronic Communications Privacy Act (ECPA) was enacted, which extended federal privacy protections to wireless telephone users. ECPA made it a federal crime to eavesdrop by "intentionally" intercepting wireless conversations or to disclose the contents of the conversation. [18 U.S.C. §2511] The ECPA also made it a Federal crime to manufacture, sell, assemble, possess, or advertise any device,

knowing that the design of the device renders it "primarily useful" for surreptitiously intercepting wireless communications. [18 U.S.C. §2512]

As microchip technology continued to advance through the late 1980's, a new era of digital electronics developed, bringing with it the opportunity to create intelligent mobile handsets and switches and to provide an unprecedented number of features and services for customers. The deployment of digital equipment to supplant existing analog cellular systems and the deployment of new, fully digital systems will provide the opportunity for increased system efficiency, better transmission quality, and, until digital scanners and decryption equipment drop in cost and become more easily available, improved security.

As a result, in the near term it is appropriate to consider actions to curtail the modification of scanners and to remove persistent barriers to the rapid deployment of digital equipment. Most importantly, however, policymakers must realize that it is only a matter of time until history repeats itself and digital communications also become exposed to eavesdropping. Extending scanner and decoder prohibitions to all commercial mobile services is critical.

Despite Prohibitions, Scanning Devices Are Readily Available

As low-cost scanners capable of intercepting cellular frequencies became more prevalent, in 1992 Congress amended the Communications Act of 1934 to strengthen the privacy rights of wireless phone users by banning FCC authorization, or the manufacture and importation, of radio scanners which are: (A) capable of receiving or intercepting transmissions on frequencies assigned to the domestic cellular service, (B) able to be

"readily altered" by the user to receive these transmissions; or (C) equipped with decoders that convert digital cellular transmissions to analog voice. [47 U.S.C. §302a(d)]

The legislative history associated with the 1992 amendments to the Communications Act that banned the manufacture and importation of scanners equipped to receive cellular frequencies clearly evidences the intent of Congress to stop illegal scanning by restricting the availability of scanners with this capability.[7] To accomplish this, the amendment banned the manufacture and import of scanners equipped or readily alterable to receive transmissions in frequencies assigned to the domestic cellular service. Unfortunately, the problem Congress acted to solve in 1992 persists.

At the time of enactment of the provisions in 47 U.S.C. 302(d) the House Commerce Committee observed that, unlike other provisions of that section, the new provisions being added do not bar the sale or use of non-complying scanning receivers because "the Committee expects that the stock of new non-complying scanners available for sale will diminish rapidly once the regulations are adopted." [See House Rpt. 102-207, p. 31]. While the on-the-shelf stock of non-complying equipment may have been depleted as Congress expected, a new generation of scanner modification technology arose, aided

[7] The legislative history for the 1992 amendment reads, in part; "The Committee finds that scanning receivers continue to be manufactured with the capability of monitoring the frequencies allocated to cellular telephone service. Such equipment enables users to violate the provisions of the 1986 Electronic Communications Privacy Act (ECPA), which extends Federal privacy protections to cellular telephone users. Equally disturbing, even equipment that blocks out cellular calls can often be easily modified to receive cellular transmissions, often by cutting a single wire. Moreover, the Committee has receive numerous examples of "how-to" manuals for modifying scanners so that they can be used to eavesdrop on cellular calls. The Committee has obtained copies of advertisements for scanners that do not block out the cellular frequencies or that pitch easy restoration of such frequencies. This amendment is intended to address these ongoing problems, and bring the Commission's certification process in line with ECPA." (U.S. House of Representatives, Report 102-207, Federal Communications Commission Authorization Act of 1991, pp. 31-32.)

and abetted by scanning publications and the Internet, and fueled by the scanner's credo that if it's in the air it can be intercepted regardless of privacy rights.

To make matters worse, despite the seemingly comprehensive set of federal privacy protections discussed above, scanning enthusiasts openly advertise that the modification of scanners is not illegal. As a survey of the Internet and electronics magazines shows, modification of scanners to receive cellular frequencies is inexpensive, and is offered with impunity. According to a prominent monitoring guide:

> "You should be aware that the law makes it illegal to monitor cellular communications, not possess a device that can monitor them. In other words, it is not against the law to modify a scanner to pick up these frequencies. It is just against the law to listen to them." (Modifying the PRO-43, Copyright 1996 by Howard Bornstein).

Numerous magazines and Internet websites advertise new scanners with cellular frequency blocking components that may be easily defeated with relatively minor alteration. Information and equipment to perform these modifications are widely advertised for that purpose. Even the purveyors of scanners advertise with impunity their own offers to restore the missing cellular frequency monitoring functions after the equipment is purchased. For example, an advertisement for the "AOR AR-8000" on the Internet reads:

> **AOR AR-8000**
> **Full Frequency Restorable!**
>
> **With wide frequency coverage --500 kHz-1900 Mhz (less cellular, restorable when programmed with Scancat-Gold Software).**
>
> **After you purchase your AR 8000, we can restore the missing 800 Mhz for only $40 plus return shipping.** (See Attachment # 2**)**

The FCC Report and Order implementing Congress' ban on the manufacture of scanners with the capability of eavesdropping on cellular calls stated that the Commission would impose sanctions on retailers of scanners who also offer to modify scanners to receive cellular frequencies.[8] However, if the numerous advertisements (such as the one reprinted above) on the Internet and in monitoring magazines are any guide, individuals who currently provide that service do so with little fear of prosecution. Further, while some of these scanners may not be "readily alterable by the user" per 47 USC 302(d), numerous outlets seems able to readily alter the scanners at a nominal price. Finally, it is important to note that the law, and the FCC's order, ban scanners that monitor frequencies assigned to the domestic cellular service, but do not address scanners that can monitor PCS or other types of commercial mobile services.

Definitional issues in the applicable criminal statute [18 U.S.C. §2512] further complicate efforts to convict and punish those who manufacture and sell illegal eavesdropping equipment. This section of the criminal code prohibits/penalizes the sale, possession, or manufacture if the design of the device renders it "primarily useful" for prohibited interception purposes and the user knows or should know that. The ability of these devices to scan other frequencies or perform other permissible functions may be interpreted to make it difficult or impossible in many circumstances to prove the device is "primarily useful" for illegal activity.

In addition, statutory prohibitions in the Communications Act appear to address only prohibitions on devices which intercept transmissions in "cellular" frequencies, and

[8] The Report and Order states, in part, "....Furthermore, any retailer marketing a scanner that also performs alterations to that scanner so customers can receive cellular frequencies will be violating FCC

appear not to apply to similar services at different frequencies. Since enactment of those provisions a new category of services called commercial mobile radio services (CMRS) has been created, into which cellular, as well as additional mobile services at different frequency ranges, have been added, *e.g.*, PCS, ESMR and mobile satellite.[9] The law does not appear to prohibit manufacture and sale of devices equipped to intercept those frequencies or equipped with digital decoders that operate at other than "cellular" frequencies. As a result, unless Congress clarifies its intent and broadens the scanner prohibitions to all CMRS, history will likely repeat itself and policymakers will need to revisit the laws and regulations regarding scanners yet again.

Until the law clearly makes modification and use of cellular scanners illegal and is consistently enforced, eavesdroppers who want to listen in on private conversations will have little difficulty getting and using the gear they need.

Deployment of Digital Systems

Standard analog scanners cannot read digital signals. Encryption of digital signals, as provided by some carriers, will provide even better security. While scanners are available that do read digital signals, they currently cost many thousands of dollars, and decryption capabilities are similarly limited. As a result, as wireless carriers build out digital systems or replace analog equipment and handsets with digital, eavesdroppers will be at least temporarily stymied.

---

rules and the Communications Act, and therefore will be subject to appropriate enforcement sanctions." (U.S. Federal Communications Commission, Report and Order, ET Docket No. 93-1, April 22, 1993)

[9] The FCC specifically declined to enact rules prohibiting manufacture of scanners able to receive signals from other services such as PCS and ESMR because to do so would exceed statutory requirements (Report and Order, 8 FCC Record 2911 at paragraph 8.

Despite provisions in the Telecommunications Act of 1996 that ban arbitrary prohibitions on facilities sitings, in some parts of the country local governments are slowing the deployment of digital equipment with moratoria on new facility siting or excessive fees associated with the placement of digital antenna. While most of CTIA's PCS member companies have already begun service and plan to greatly expand system operations in their license areas during1997, service to some localities within those license areas may not proceed on the same schedule due to procedural or financial barriers thrown up by those local governments.

Prior to enactment of Section 704 in the Telecommunications Act of 1996, each State and local land use authority had free reign to apply their respective zoning ordinances and statutes according to the prevailing sentiments of an affected community. This often resulted in the arbitrary denial of siting applications in response to unsubstantiated fears, specious allegations and junk science claims. Additionally, some authorities resorted to moratoria, referenda, and recordless procedural tactics to forestall wireless facility location decisions indefinitely.

In 1996 Congress restricted the right of state and local governments to engage in procedures or render decisions which prohibit or have the effect of precluding the siting of wireless facilities, or which unreasonably discriminate between similar, competing services. Violations of this provision can be appealed in either State or federal court. Unreasonable moratoria are no longer permissible by statute. Nor can there be an arbitrary refusal to accommodate the technologic, geographic and capacity limitations of a carrier seeking to provide competitive wireless services to a new area or to one already served by other carriers.

Nonetheless, deployment of digital equipment is being delayed and blocked by local governments. Imposition of lenghly moratoria are common, while moratoria that are limited to a short and reasonable duration are frequently renewed again and again. Either has the effect of blocking the deployment of the digital equipment that will help reduce the opportunity for illegal eavesdropping. Attachment #3 of this testimony is a listing of active moratoria in municipalities around the United States that are blocking the deployment of digital systems.

Fixing The Problem

Today, over 43 million Americans use CMRS. The Paul Kagan research group recently released figures showing that over 10 million Americans signed up for wireless service in 1996 alone. Additionally, nearly 60 million U.S. households contain a cordless telephone. These Americans deserve to have their privacy protected. As discussed above, there seems to be widespread ignorance of the law with respect to maintaining the privacy of wireless telephone conversations. As a result, we should take additional steps to maximize and enforce the privacy rights of persons using CMRS. The following are policy considerations to address wireless privacy issues.

1. Policymakers may wish to make explicitly clear that modification of a scanner to enable it to intercept any CMRS call is an illegal act, just as manufacture of such scanner is prohibited under 47 U.S.C. §302a(d).
2. Policymakers should require scanning devices which are manufactured and/or sold in the U.S. to be effectively hardened to prohibit illegal modifications. The FCC could require that the microprocessor chip in scanners be difficult to remove for modification, replacement, or reprogramming. This will prohibit users from following simple

instruction from the Internet to defeat a scanner's built-in blocking of CMRS frequencies.

3. Although current law [18 USC 2512] criminalizes the possession of interception devices, the "primarily useful" language in the statute may make enforcement and prosecution difficult. The term "primary" could be dropped, since a scanner that is modified to be merely "useful" for eavesdropping can do so just as well as a scanner that is "primarily useful" for eavesdropping.
4. Congress should extend equal protection under law to all of the commercial mobile radio services.
5. Since digital technologies will help ameliorate the problem of eavesdropping, policymakers should act to mitigate barriers to the development and deployment of this infrastructure.
6. While it is currently illegal to manufacture or import a scanner with cellular monitoring capabilities, there appear to be few barriers to individual mail orders of such scanners from Canada, England, and other countries.
7. Increased penalties for intentional unlawful interception of electronic communications will discourage electronic stalkers.

Each of these suggested considerations attacks one or more elements of the problem of ensuring the privacy of Americans who use wireless communications. Taken together these actions would, over time, significantly improve the security of wireless communications in the United States and provide the Americans who use wireless communications with the privacy protections under law they deserve.

Attachments

1. Print-outs of advertisements for scanner modifications to enable cellular scanning.
2. List of active moratoria banning the placement of digital facilities.