Statement of

William E. Kennard, General Counsel

Federal Communications Commission

Oversight Hearing on Cellular Privacy

before the

Subcommittee on Telecommunications,

Trade and Consumer Protection

U.S. House of Representatives

February 5, 1997

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to testify on behalf of the Federal Communications Commission regarding cellular radio privacy issues.

Under Section 705 the Communications Act (47 U.S.C. §605), the interception of a radio communication and the divulgence or beneficial use of radio communications is generally prohibited. The Communications Act, however, does not prohibit the mere interception of the radio communications. Therefore, people who listen to police channels, or a cellular or cordless phone conversation, but do not divulge or publish what they hear or use the information for their own benefit or benefit of another, would not be violating Section 705. Other federal criminal statutes, including the 1986 Electronics Communications Privacy Act, which is part of the federal criminal code, do generally prohibit the intentional interception of some cellular transmissions. Many states also have statutes in this area.

Section 705 of the Communications Act includes criminal penalties. Accordingly, and in light of its close relationship to the wiretapping and related provisions of the criminal code, and at the request of the Department of Justice (DOJ), it is the FCC's longstanding general practice to coordinate complaints regarding potential violations of section 705 with DOJ in order to make sure that our administrative actions do not interfere with any DOJ criminal investigation. This is in accordance with a Memorandum of Understanding (MOU) with DOJ (effective since 1953 and revised and re-executed in 1989). The MOU specifically states that DOJ assumes responsibility for conducting investigations into complaints of alleged criminal violations of Section 705, and the Commission is to provide technical assistance when specifically requested by DOJ. DOJ typically asks us not to investigate until it has conducted its own criminal investigation and has made a prosecutorial determination. While we receive many telephone inquiries asking for information regarding the interception of cellular telephone calls, we have received very few written complaints alleging unlawful interception and divulgence or use of cellular calls.

In 1992, Congress took additional action to protect the privacy rights of cellular telephone users. It passed the Telephone Disclosure and Dispute Resolution Act (the "TDDRA"). Among other things, this statute added a new Section 302(d) to the Communications Act to require the Commission to prescribe regulations denying equipment authorization for any scanner that is capable of:

-receiving transmissions in the frequencies allocated to the domestic cellular radio service;

-readily being altered by the user to receive transmissions in such frequencies; or

-being equipped with decoders that convert digital cellular transmissions to analog voice audio.

The TDDRA further provides that, beginning one year after the effective date of the regulations adopted pursuant to the Act, no receiver having such capabilities shall be manufactured or imported into the United States. In April of 1993, the Commission adopted rules implementing these provisions of the TDDRA. The rules (found at 47 C.F.R. §15.37(f)and §15.121) prohibit the FCC authorization of and the manufacture or import of scanners and associated frequency converters that are capable of tuning or being readily altered to tune frequencies in the cellular bands. Under the rules, receivers are deemed capable of readily being altered by the user if the ability to receive transmissions in the cellular telephone bands can be added by clipping the leads of or installing a simple component such as a diode, resistor, and/or jumper wire; replacing a plug-in semiconductor chip; or programming a semiconductor chip using special access codes or an external device, such as a personal computer. In addition, under our rules, scanners and frequency converters designed to be used with scanners must be incapable of converting digital cellular transmissions to analog voice.

In order to ensure compliance with the new rules prohibiting the manufacture or import of

scanners which are capable of tuning to the cellular frequencies, the Commission required in its rules (47 C.F.R. §2.1033(b)(12)) that applications for equipment authorization for scanners include a statement describing the methods the applicant employed to comply with the new rules in addition to the engineering schematics describing the design of the equipment already required. Equipment that does not comply with the new rules could not be manufactured in, or imported into, the United States after April 26, 1994. Where questions arise in the equipment authorization process, the Commission requests additional information and, in some instances, the equipment itself.

Further, as directed by the TDDRA, in June of 1993, the Commission provided the Congress with a report entitled "Available Security Features for Providing Cellular Telephone Privacy." That report surveyed the methods of intercepting cellular telephone calls and concluded that it was difficult, but by no means impossible, to intercept entire conversations. It also described the various methods that are available to cellular telephone subscribers who desire to encrypt analog cellular calls and pointed out that once cellular carriers converted to digital signal transmission, it would become considerably more difficult to intercept cellular calls. The report concluded that, while no foolproof encryption technique was readily available, it was likely to become more difficult and expensive to eavesdrop on cellular telephone calls as time progressed and the move to digital conversation developed.

We believe that, by and large, the conclusions reached in that report have been borne out. Our rules seem to have been effective in decreasing the availability of scanners capable of tuning to cellular frequencies. Since the effective date of our rules, we have denied five applications for scanners which are capable of tuning to cellular frequencies. In addition, in one instance, we learned that a large electronics retailer was, apparently inadvertently, marketing scanners that could be programmed to receive cellular frequencies. We required that retailer to cease marketing those scanners until the units were redesigned and we checked them to ensure the redesigned units were compliant.

While we believe that our efforts to limit the availability of scanners that are capable of tuning to cellular frequencies have generally been successful, you should be aware that it is not impossible to obtain a scanner that can tune to cellular frequencies. There are several reasons for this.

First, a large number of scanners capable of receiving cellular conversations were legally manufactured or imported prior to April 1994. These scanners were grandfathered by the TDDRA and it is legal to possess units manufactured or imported prior to the April 1994 cut-off date even though use of such scanners may lead to a violation of the Section 705 prohibition on intercepting and divulging or using cellular conversations.

While we do not have any estimate of the number of units exempted by the TDDRA that remain in circulation, in the five years preceding adoption of the 1993 rules, the Commission certified 22 different models of scanners which were capable of receiving cellular conversations. The Commission also certified ten other models that tuned to nearby frequencies, many of which could easily be altered to tune the cellular band. And, while the statute prohibited the manufacture and import of scanners that tune to the cellular band after April 1994, it explicitly exempted sales of preexisting equipment. As a result, stockpiles of scanners that were imported or manufactured before the cut-off can still be sold legally. Many of these units may still be legally on the market.

Second, while we have made it difficult to modify units manufactured since 1994, it is, of course, not impossible for someone with the technical know-how to modify scanners to pick up cellular frequencies. (Section 705(e) of the Communications Act makes such modification a crime, but only if the person doing the modification knows that the customer intends to use the modified scanner not just to intercept cellular calls but also to divulge or use them.)

Third, it has come to our attention that some scanners can pick up cellular conversations even though they are not tuned to the cellular band. In other words, although you cannot

program the unit to tune in the cellular frequencies, when you program it to tune to other nearby frequency bands, you can pick up cellular conversations because the receiver does not contain adequate filtering. Our Office of Engineering and Technology (OET) is currently investigating this phenomenon and ways in which it can be prevented. OET believes that manufacturers can take steps to improve the filtering of their receivers, albeit at some additional cost. OET expects that we will be able to work with manufacturers to address this problem.

Fourth, it has come to our attention that entities in foreign countries are using the Internet to advertise scanners which are capable of intercepting cellular telephone calls and presumably shipping them to purchasers in this country. The Commission has no reason to think the volume of such shipments is large, but despite successful efforts of U.S. Customs inspectors in preventing bulk importation of illegal scanners, it may be very difficult to prevent such individual shipments from entering the U.S.

I should point out that the TDDRA prohibits only scanners capable of intercepting cellular telephone calls. It does not regulate devices which intercept personal communications service (PCS), air-to-ground, or other over-the-air transmission services. At the present time, we are not aware that interception of PCS or other transmissions is prevalent. However, it would probably not be unreasonable to anticipate that enterprising individuals might develop and market devices which could intercept such transmissions. In the event the Subcommittee elects to consider legislation to amend the TDDRA, you may wish to weigh the extent to which PCS and other over-the-air services should be accorded similar privacy protections.

We at the Commission are committed to effective enforcement in this area. In response to Chairman Bliley's recent request, we are undertaking a thorough examination of our current scanning device authorization and enforcement processes to ascertain whether our rules and implementation efforts are as effective as they can be. If our review finds any areas where improvements can be made, you may be assured that we will make them.

With me today is Richard Smith, Chief of our Office of Engineering and Technology (OET). OET (in conjunction with our Compliance and Information Bureau) is responsible for implementation and enforcement of our rules regarding scanners. Mr. Smith is also available to answer technical questions about wireless technology and interception, questions about Section 302 applications and enforcement and any questions about the Commission's role in implementation of the Communications Assistance for Law Enforcement Act of 1994 (CALEA) relating to encryption issues.

Thank you.