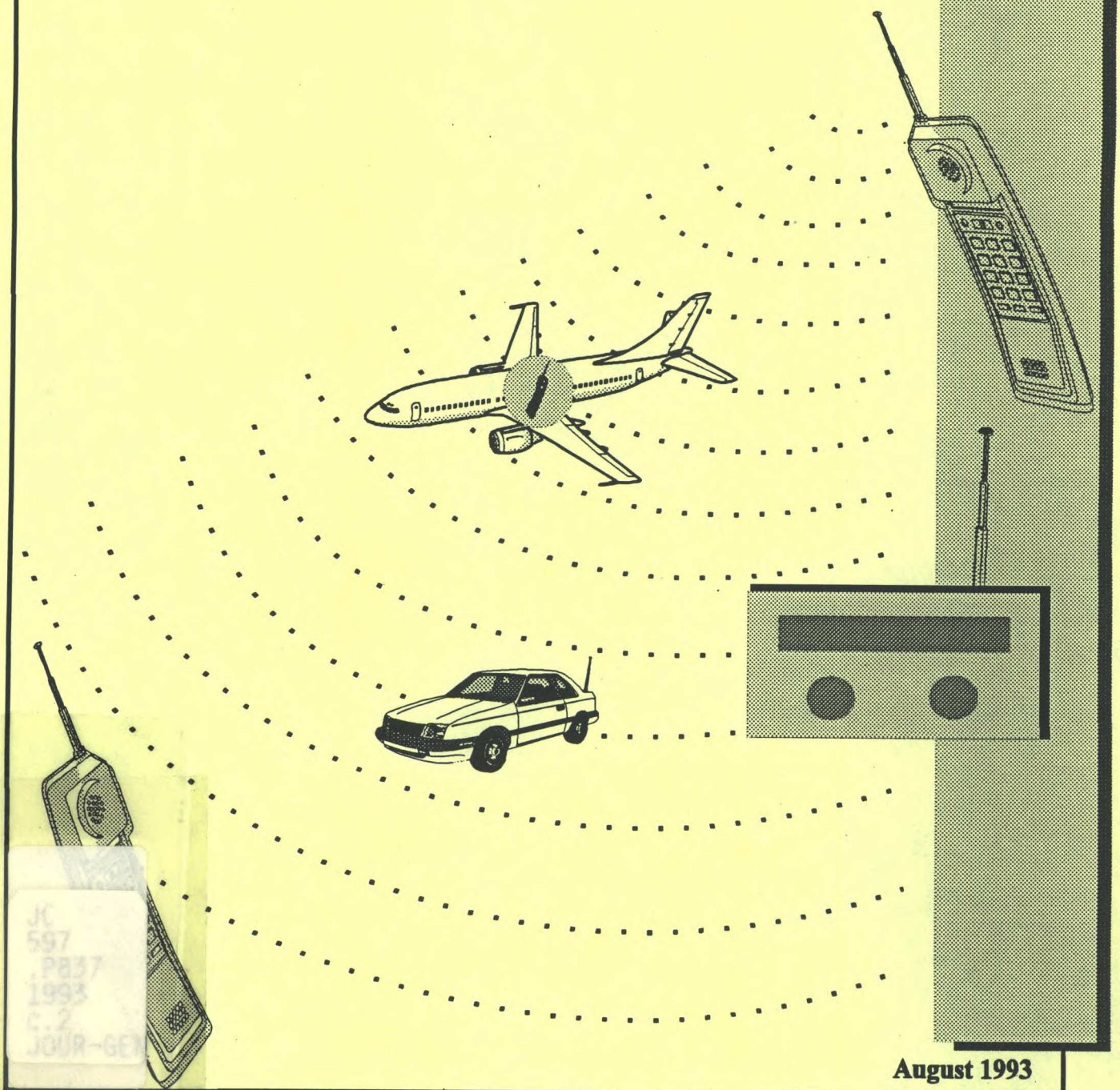
Canada

Public Discussion Paper on Radio-Based Telephone Communications and Privacy



August 1993

Industry and Science
Canada

[redacted]

INDUSTRY AND SCIENCE CANADA

RADIOCOMMUNICATION ACT

NOTICE NO. DGTP-008-93

Public Discussion Paper on Radio-Based Telephone Communications and Privacy

Notice is hereby given by Industry and Science Canada of the release of a public discussion paper on radio-based telephone communications and privacy. Written submissions are invited from all interested parties on the options set out in the aforementioned paper.

Copies of the public discussion paper are available from Information Services, Industry and Science Canada, 300 Slater Street, Ottawa, Ontario K1A 0C8 (telephone (613) 990-4900), and from the former Department of Communications regional offices at Moncton, Montréal, Toronto, Winnipeg and Vancouver.

Submissions should be addressed to the Director General, Telecommunications Policy Branch, Industry and Science Canada, 300 Slater Street, Ottawa, Ontario, K1A 0C8. To ensure consideration, submissions must be received within 90 days of the date of the publication of this notice in the *Canada Gazette*, Part I. All submissions must cite the *Canada Gazette*, Part I, the publication date, the title and the notice reference number.

All submissions received in response to this notice will be made available for viewing by the public two weeks after the closing date of this notice, during normal business hours, at the Industry and Science Canada Library at 300 Slater Street, Ottawa, Ontario, and at the above-identified regional offices at Moncton, Montréal, Toronto, Winnipeg and Vancouver, for a period of one year from the close of comments.

Also, approximately two weeks after the closing date of this notice, copies of the comments may be obtained by telephone, mail order or over the counter from ByPress Printing and Copy Centre Inc., 300 Slater Street, Unit 101A, Ottawa, Ontario K1P 6A6, (613) 234-8826, facsimile (613) 234-9464. Reasonable costs of duplication and distribution will be charged.

Dated at Ottawa this 16 day of August, 1993.

Michael Helm
Director General
Telecommunications Policy

TABLE OF CONTENTS

RADIO-BASED TELEPHONE COMMUNICATIONS AND PRIVACY

1. INTRODUCTION AND OBJECTIVES

Having regard to the recent initiatives undertaken by the Minister of Communications to enhance the privacy of telecommunications, cellular service providers, among others in Canada, have urged that measures be implemented to restrict the proliferation of scanning receivers capable of tuning cellular frequencies.

This paper looks at the feasibility of, and the possible concerns related to, the imposition of restrictions in Canada on monitoring devices capable of providing access to radio-based telephone communications[1]. Its purpose is to encourage, and to provide a focus for, the public consultations which are being sought in this respect.

Because the concerns expressed to date have been directed to the derogation of the privacy of cellular telephone users occasioned by the use of scanners, the paper focuses on these issues. However, analogous concerns are evident in respect of other radio-based telephone communication systems (such as public cordless and air-to-ground telephony) currently in operation or planned for implementation, and in the use of radio receiving equipment other than scanners. Accordingly, comments in respect of such matters are also sought.

In this paper, privacy of communications means a reasonable expectation that a conversation is not being intercepted and divulged or used. Security of communications means the virtual certainty that, even if the conversation is intercepted, it cannot be rendered intelligible without the use of special measures.

The objective of the first part of this discussion paper is to outline a number of technical considerations relating to cellular privacy issues and to explain the technical implications involved in restricting cellular scanners. The second part canvasses the various operational issues involved in controlling radio receivers. The third part considers the legislative and regulatory aspects of the proposal to restrict scanners in Canada, after summarizing the corresponding activities that have recently transpired in the United States. The final part sets out

---

[1] The term "radio-based telephone communication" in this document is based on the definition contained in the Radiocommunication Act (as amended). It means any radiocommunication (within the meaning of the Radiocommunication Act) that is made over apparatus that is used primarily for connection to a public switched telephone network.

the matters on which public comment is being sought. Annexes provide additional details about various aspects of cellular technologies. The remainder of this introductory section briefly looks at the initiatives undertaken within the past several months to enhance the privacy of telecommunications users in Canada.

Recent Legislative and Ministerial Initiatives

Bill C-109, which received Royal Assent on June 23, 1993 and came into force on August 1, 1993, contained a number of provisions intended to enhance the privacy of communications made over radio-based telephone services by limiting the activities of interception and use, but not by limiting the availability of the devices used for interception. The Bill amended the Criminal Code so as to:

(1) deem an encrypted radio-based telephone communication to be a private communication;

(2) prohibit the interception of radio-based telephone communications which is carried out maliciously or for gain; and

(3) prohibit the disclosure or other use of information obtained from the interception of radio-based telephone communications.

The Bill also amended the Radiocommunication Act to make it an offence to make use of, or divulge, information obtained through eavesdropping on radio-based telephone communications. As well, a right of civil action was provided to persons whose radio-based telephone communications have been or may be used or divulged.

These amendments comprise a package of comprehensive and enforceable measures. It will be some time, however, before it is known how effective these measures will be in enhancing the overall level of privacy provided to cellular and other radio-based telephone communications.

The Minister of Communications also announced, on December 9, 1992, two other measures to increase the privacy protection afforded to cellular users. First, cellular service providers will be required to offer effective, reasonably-priced encryption services as an option for their customers. Second, telephone

companies were asked to explore the feasibility of ensuring that any call made using a cellular link is identified by an audible signal on the line. The Minister can require the implementation of these measures pursuant to the Radiocommunication Act.

In addition, a public education campaign, to be undertaken by the cellular service providers, will clarify for cellular telephone users the ambit of privacy protection afforded by both the basic service and the various options available therewith.

It is within this framework that public comment is being solicited about the appropriateness of implementing measures to restrict the proliferation of receivers capable of providing access to the cellular frequency bands, as well as to other frequency bands used for radio-based telephone communications.

2. MONITORING CELLULAR TRANSMISSIONS

The cellular telephone system uses a radio link for a portion of its transmission path, and thus if the voice signal is not scrambled or encrypted over the radio link, it can easily be monitored by third parties using various radio receiving devices. (A description of how cellular telephony works is provided in Annex 1.) The objectives of the initiatives undertaken in relation to cellular privacy have been, firstly, to make people aware, and to remind parties during a cellular telephone conversation, that cellular telephony uses a medium subject to relatively easy interception, and secondly, to promote the deployment and use of affordable encryption devices, so as to bring the protection afforded to the radio segment of the transmission to at least the same level as that provided to the (unencrypted) wireline portion.

Monitoring Analog Cellular Transmissions

Currently, in the case of analog cellular systems, cellular telephone calls can be intercepted in the following ways:

(1) A radio scanner purchased from electronics stores at modest cost (approximately $300) can function, or be modified to function, as an effective cellular frequency scanner. Any required modifications can be completed within hours, and instructions for making these modifications are readily available; some technical skill is required to avoid damaging sensitive circuitry in the scanner.

(2) An old TV set can be turned into a cellular receiver by adjusting the fine tuner in the UHF band between Channels 72 and 83. (The spectrum used by cellular systems had been allocated to television prior to 1979.)

(3) All analog cellular phones are inherently also cellular scanners. By pressing certain codes on the keypad, the phone will operate in the maintenance mode and will be able to scan through all the cellular frequencies. These keypad codes are normally not disclosed to users by the equipment manufacturers.

(4) Sophisticated electronic hobbyists can build a scanner from the cellular phone specification (EIA/TIA IS-553[2]), which is widely available.

In spite of the fact that cellular telephones change channels as they move from cell to cell, making it difficult for eavesdroppers to follow a complete conversation, monitoring of cellular conversations can still be quite successful, for the following reasons:

(1) Often, cellular conversations are relatively brief, the average call duration for cellular calls being less than that for wireline calls. In those situations where the conversation is of short duration, it is quite probable that even a vehicular cellular telephone will operate entirely within one cell, and hence use the same frequencies, during the entire conversation. This is especially likely when the cells are relatively large, or when the mobile unit is only changing position slowly because of traffic.

(2) Hand-held cellular phones which are used by pedestrians, in buildings or on the street, seldom move from cell to cell. Hand-offs are therefore not usually necessary, and the entire cellular conversation will most likely be carried out on a single channel.

---

[2] Electronics Industry Association/Telecommunications Industry Association Interim Standard 553

(3) Even if there is a hand-off of a call to another cell using a different channel, the cellular scanner can be put on a "search" mode to try to seek out the desired conversation. Because so many cellular radio channels are usually in use, some part of that conversation will not be monitored during the time the new channel is being located.

Technology that provides solutions to the problems of monitoring analog cellular systems currently exists. Techniques for scrambling analog voice transmissions are described in Annex 2 of the paper.

Analog to Digital Cellular Conversion

Rogers Cantel has converted some analog cellular channels to digital use; it began installing digital equipment in Toronto in July 1992 and subsequently installed equipment in the Montreal and Vancouver areas. Bell Mobility Cellular introduced digital cellular in the Toronto and Montreal areas in early 1993. Other Mobility Canada members will also be installing digital radio equipment at a number of their cell sites.

Monitoring Digital Cellular Transmissions

While digital techniques do not in themselves increase the protection afforded against interception of signals in the radio medium, the conversion to digital cellular transmissions will make monitoring more difficult. As the signal is digital, the conversations cannot be monitored using analog scanners, analog cellular telephones, or old TV sets, since the digital signals cannot be demodulated by analog receivers. Digital scanners will have to use the same modulation technique (QPSK) and be equipped with the same voice decoder (VSELPC) as digital cellular transceivers before digital cellular conversations can be listened to.

Nevertheless, monitoring digital cellular conversations will still be possible. Digital cellular telephones will be capable of being set in a maintenance mode that will allow the cellular frequencies to be tuned. Digital scanners are being built and sold today as professional (and costly) equipment; eventually they may, if they follow the same decreasing supply price curve as other consumer electronic products, drop sharply in price, to levels where consumers can easily afford them.

Digital Encryption

Encryption techniques are available which can make the radio link more secure than the (unencrypted) wireline portion. Encryption techniques are easier to employ with digital radio links than with analog transmissions, and the level of security is also higher. There are a number of ways in which encryption can be applied to digital cellular transmissions. An example is given in Annex 3 of this paper.

The Cellular Telecommunications Industry Association (CTIA), of which Canadian cellular manufacturers and service providers are members, has started discussions on introducing encryption capabilities into the next generation of digital cellular telephones. Further work is required to identify the best encryption technique that is to be used.

The introduction of digital cellular itself provides, at least at this time, some measure of privacy protection. However, if digital scanners were to become commonplace, then digital encryption would have to be offered by the cellular service providers as an option to subscribers who wished to have a reasonable expectation of privacy.

Considerations Involved in Adopting Encryption Techniques

Introducing encryption into the next generation of digital cellular telephones involves changing the specifications of such equipment not only in Canada, but in North America as a whole. In spite of the fact that the introduction of encryption to digital cellular systems is relatively simple, the cost of cellular telephones and service with the encryption option will increase, as encryption keys will have to be distributed and the management of the network, the tariff structure and the associated processing software will become more complicated. Since not all subscribers require the same level of privacy, cellular service providers may wish to provide their subscribers with different levels of privacy protection.

While the adoption of encryption techniques obviously involves some effort and expense on the part of the cellular service providers, the service suppliers also stand to garner some benefits. As various forms of personal communications services become available, cellular telephony will become only one of a number of means by which users can keep in touch while remaining mobile. Cellular service providers thus have an incentive to ensure that their market is not eroded by competing services able to offer such attractive features as enhanced security of communications.

3. RESTRICTING CELLULAR MONITORING DEVICES

In considering the restriction of "cellular scanners", it is important that the definition of such a device be clear. In the context of this paper, a cellular scanner is a radio receiver which is capable:

(1) of receiving transmissions in the frequencies assigned to the domestic cellular radio telecommunications service[3], or of readily being altered to receive transmissions in such frequencies, with the capability of automatically switching between four or more frequencies anywhere within the cellular bands and of stopping at and receiving a radio signal detected on a frequency; and

(2) in the case of a digital cellular scanner, of also being equipped with decoders that convert digital cellular transmissions to analog voice audio signals.

It is obviously not the objective to ban all cellular transceivers (transmitters and receivers), since to do so would ban cellular telephones. Hence the restrictions would have to be applied to devices capable only of reception.

It should also be noted that banning scanners would not preclude existing cellular telephones from being used as cellular scanners or receivers, through activation of the maintenance codes. Initiatives to limit the availability of cellular scanners may thus also have to consider the feasibility of imposing restrictions on the maintenance-mode capabilities of cellular telephones.

4. SUMMARY OF TECHNICAL CONSIDERATIONS

(1) The monitoring of digital cellular transmissions is more difficult than that of analog cellular transmissions, but it is not impossible.

(2) Currently available encryption technology can effectively prevent monitoring of both analog and digital cellular radio transmissions. There is a cost associated with the provision of encryption.

---

[3] In North America, the cellular system operates in the frequency bands of 824-849 MHz and 869-894 MHz.

(3) An encryption standard for digital cellular systems still needs to be identified. Through the CTIA, in which Canadian cellular equipment manufacturers and service providers participate, a common standard for North America is under development, in order to achieve compatibility and to avoid significant cost penalties.

(4) At present, the digitization of cellular service is enough to provide a measure of privacy protection to users of digital cellular. In the longer term, privacy will be diminished unless steps are also taken to introduce encryption to digital cellular radio transmissions or to limit the availability of receivers capable of monitoring digital cellular.

5. OPERATIONAL IMPLICATIONS OF CONTROLLING RADIO RECEIVERS

Historical Background

Until April 1, 1953, the Department of Transport, then responsible for radiocommunications matters, licensed all receivers, including broadcast receivers. It was subsequently decided that such comprehensive licensing performed no useful function, and the requirement in respect of broadcast receivers was accordingly abolished. Regulations were promulgated to remove the licensing requirement for radiocommunication receivers.

In the late 1980s, the Courts decided that, under the extant legislation, a radio user seeking to restrict access to its transmission of "pay TV" (and thereby seeking, in effect, a measure of radiocommunication privacy) would have to take steps to "scramble" the communication that was being sent. As a result, the Broadcasting Act of 1991 provided for the protection of encrypted signals, and many programming signals delivered by satellite today are encrypted.

The Radio Act (antecedent legislation to the current Radiocommunication Act) did contain provisions that made it an offence to make use of or divulge radiocommunications with which a person had "become acquainted". The Radiocommunication Act restated the offence as consisting of intercepting and making use of or divulging the radiocommunication. Thus, pursuant to the Radiocommunication Act, anyone in a sense is allowed to "listen" to a radiocommunication, but that same listener cannot "divulge" or "use" the information without facing the risk of prosecution. As noted above, Bill C-109 expands the privacy protection afforded to radiocommunications.

Operational Considerations

Proposals concerning the restriction of scanners and other radio receivers give rise to a number of operational considerations. One key concern for the Department is, of course, the workload involved in any new enforcement activity. For a number of years, the Department has been endeavouring to reduce the regulatory and administrative burden on both radio users and the Department. To that end, the Department has made a number of changes in its licensing approach: it has introduced system licensing and fleet licensing, has exempted CB (GRS) radios from licensing altogether, and is currently giving consideration to one-time licensing for fixed parameter services (for example, aircraft and ship radios). These initiatives have contributed greatly to rationalizing the use of increasingly scarce governmental resources, without in any manner diminishing the Department's ability to manage the spectrum.

Endeavouring to enforce a prohibition on scanners would add to the responsibilities of the Department, and could have a significant impact on Departmental workload and on that of such other federal organizations as the RCMP and Revenue Canada drawn upon to help enforce the ban.

Because there are a number of radio-based telephone communication technologies, directing measures to the protection of only one kind of radiotelephone communication (such as cellular) could invite criticism. By way of example, the digital cordless telephone service that is being introduced in Canada will initially operate on frequencies just above the cellular band, at 944-948.5 MHz; similarly, air-to-ground telephones operate in the frequency bands adjacent to those of cellular, at 849-851 MHz and 894-896 MHz. To expand the ban to include those frequency bands that now carry radio-based telephone communications would be difficult, and any such ban would in any event have to be continually updated as new telecommunications services were introduced in other frequency bands. As well, expanding the restriction to cover similar services would raise the problem of how to deal with other radiocommunication users, including amateur radio operators, who may share those bands.

The perceptions of the public and of industry are also important in this matter. Banning scanners could engender a false sense of security on the part of cellular users and, indeed, on the part of the cellular service providers; this would be particularly true in the case of analog scanners, where a ban would be of only limited effect because of the large number of scanners in the field and the relative ease with which new ones could be obtained. An unwarranted sense of security could, in turn, have

the adverse effect of creating delays in the adoption by consumers of encryption, the implementation by cellular service providers of such measures as audible warnings of cellular use, and the incorporation by the industry of encryption in the technical standards for digital cellular telephony.

The effect of any such ban on distributors would also have to be considered. Since little electronic equipment of any kind is developed exclusively for the Canadian market, the U.S. prohibition against scanners capable of operating in the cellular bands is likely to make the continued manufacture and distribution of such devices unprofitable. A ban would nonetheless go part way toward harmonizing the Canadian regulatory process with that of the United States, an objective of NAFTA.

While measures to limit the distribution of receivers would clearly have a major effect on the casual user of scanning equipment, for whom the easy availability and relatively low price of such equipment are important factors, it would not prevent dedicated "hackers", or persons harbouring malicious intent, from gaining access to such radio transmissions.

As well, any proposal to limit scanners must acknowledge that legitimate uses for scanning equipment exist: regulatory, operational, and safety considerations mean that some persons, other than users of the service, would have to be given access to the frequencies in question, at least from time to time. To preclude the perception of any such exemptions being granted or withheld by inappropriately subjective or administratively arbitrary action, the eligibility criteria, for those persons who would be able to obtain, or hold radio authorizations for, devices capable of monitoring transmissions in the cellular frequency bands, should be set out in regulations. (Similar restrictions currently exist in order to provide exemptions from the prohibition contained in the Radiocommunication Act respecting the disclosure and use of intercepted radiocommunications.) Were the Department to impose restrictions on scanners, it foresees allowing law enforcement officials, investigative bodies, security and intelligence services, cellular service providers, and Departmental officials to hold such authorizations, since they would require access to the cellular frequency bands in order to carry out their respective duties and responsibilities.

Given the widespread availability of analog scanners and the different means by which unencrypted analog cellular transmissions can be intercepted, it is evident that the imposition of restrictions on the availability of analog scanners

would not immediately have an impact on the privacy protection afforded to users of analog cellular telephones. On the other hand, the foreclosure of opportunities to obtain new equipment can be expected to have an increasing effect as time passes, even though, as noted above, monitoring unencrypted analog cellular calls will remain a relatively simple matter. In the case of digital cellular, precluding the widespread introduction of digital scanners could significantly strengthen the protection afforded to users of that new technology. However, in both cases it will remain important for consumers to understand the vulnerability of unencrypted radiocommunications, and to realize that the existence of a legal restriction on equipment is but one additional measure to help support personal telecommunications privacy.

6. LEGISLATIVE AND REGULATORY MEASURES

The U.S. Initiative

The recent (and still preliminary) experience of the U.S., in endeavouring to effect a ban on scanners, may be instructive. The Electronic Communications Privacy Act of 1986, among other things, made it illegal to intentionally intercept cellular communications or to manufacture equipment primarily useful for the surreptitious interception of cellular communications. However, the Federal Communications Commission (the "FCC") was not given specific authority to deny equipment authorization to scanners that receive cellular frequencies, and the FCC continued to authorize scanners capable of receiving transmissions in such frequencies. In the U.S., scanners must receive equipment authorization (certification) from the FCC before they are marketed; the purpose of the equipment authorization requirement is to control the potential of devices to cause harmful interference to authorized radio communications. Scanning receivers ("scanners") had been defined as radio receivers that automatically switch between four or more frequencies anywhere within the 30-960 MHZ band and that are capable of stopping at and receiving a radio signal detected on a frequency.

To address these limitations, the Telephone Disclosure and Dispute Act of 1992 required, among other things, the FCC to prescribe regulations denying equipment authorization for any scanning receiver capable of receiving, or being readily altered by the user to receive, transmissions in the frequencies allocated to the cellular radio telecommunications service, or capable of being equipped with decoders that convert digital

cellular transmissions to analog voice audio. Furthermore, one year after the effective date of the regulations, no receiver having such capabilities was to be manufactured or imported in the United States.

On January 13, 1993, the FCC released a Notice of Proposed Rule Making (NPRM), in which, as part of its regulatory formulation process, it solicited public comment on the implementing amendments; on April 22, 1993, the FCC adopted the final rules needed to implement the statutory requirements set out in the Telephone Disclosure and Dispute Act. Included in the restrictions are scanners that convert 800 MHz and 900 MHz signals to lower frequencies; also included in the definition of devices that can be readily altered by the user are scanners and converters that can be programmed to receive cellular transmissions by entry of an access code or by the reprogramming of a memory module.

Because existing U.S. law already prohibited the intentional interception of cellular communications, the ban on cellular scanning receivers was perceived by many as constituting only a limited measure intended to give greater effect to settled policy about the unacceptability of eavesdropping on cellular telephone conversations. In effecting the restrictions on scanners, policy-makers had regard to the limitations of the 1986 law, including the difficulty of demonstrating "intentional" interception, the limited resources available for enforcement activities, the essential absence from the marketplace of equipment "primarily" useful for surreptitious interception (all equipment having a number of uses), and the lack of specific authority for the FCC to withhold equipment authorization from scanners capable of receiving cellular transmissions. At the same time, both FCC officials and Congressional policy-makers recognized that the prohibition would, in itself, have only a limited and longer-term impact on the privacy of cellular users. They were cognizant of the fact that the (existing) definition of scanning receivers is limited to radio receivers that have automatic switching capability, and that the FCC regulations would consequently leave unaffected manually tuned receivers; that some persons would be able to violate the law by constructing receivers capable of providing access to the cellular frequency bands, or by otherwise obtaining such equipment; and that the benefits afforded by even this limited step would accrue only to users of cellular telephones, since the restrictions do not encompass other radio-based communications technologies. They were also aware of the difficulties inherent in the question of what constitutes "readily altered" equipment, and of the potential problems

associated with frequency converters capable of being used with scanning receivers and of converting cellular radio transmissions in the 800 MHz band to lower frequencies, and accordingly sought public comment on these issues in the NPRM. Notwithstanding the identified concerns and limitations, U.S. officials expect that the vast majority of persons will obey the law and that the legislation will have an increasingly significant impact as time passes, and especially as digital cellular telephony is introduced.

Implementing Restrictions in Canada

As noted above, the approach to enhancing privacy in Canada has to date been directed to restricting harmful activities, rather than, as in the most recent U.S. initiative, to restricting equipment.

Were it to be decided that restrictions should be imposed on (all, or some class of) scanners, the means by which such restrictions would be implemented would, of course, have to be given further consideration. The following two possible measures have been identified by Departmental officials:

1. Licensing of Scanners

The current exemption from licensing for radio apparatus designed solely for the reception of radiocommunications, set out in the General Radio Regulations, Part II, subsection 6(13), could be amended so as to provide that scanners do not fall under that exemption. Thereafter, pursuant to section 4(1) of the Radiocommunication Act, the installation, operation or possession of such cellular telephony monitoring receivers would require authorization from the Minister.

As discussed above, it would then be necessary to determine which persons, or classes of persons, should be eligible for licensing. This could be achieved by making regulations prescribing the eligibility of persons to whom radio licences for scanners could be issued. Alternatively, a (non-binding) policy could be developed in respect of persons eligible for licensing.

2. New Offence and Related Right of Civil Action

The Radiocommunication Act could be amended in order to create a new offence prohibiting the manufacture, importation, distribution, or sale of cellular scanners, except as prescribed in regulations. A new right of civil action would also be created to allow third parties, including cellular service providers, to recover damages as a result of conduct that is contrary to the new prohibition, or to obtain another remedy such as an injunction. Because of the difficulties involved in detecting radio receivers, the possession of scanners would not itself be prohibited.

Again, it would be necessary to determine which persons, or classes of persons, should come within the regulatory exemption.

As a further step, to be undertaken with either or both measures, it could be advantageous to establish a requirement for a technical acceptance certificate in respect of scanners, under the provisions of section 4(2) of the Radiocommunication Act. The issuance of type acceptance to manufacturers and importers would enable the Department to keep track of the number of scanners and their disposition, and might make any restriction more effective.

Enforcement Considerations

The retail sector could generally be expected to adhere to legal requirements and prohibitions. (Indeed, the major manufacturers/retailers in the United States apparently did not oppose the 1992 legislative restriction on scanners.) Without the relatively widespread advertising activities of major retailers, and the many outlets that such enterprises provide, the distribution of scanners would be expected to drop very sharply. Some enforcement activities could well, however, have to be undertaken.

To strengthen the potential effectiveness of any new measures, consideration was given to whether and how provisions could be implemented to allow private persons (including cellular service providers), who had become aware of illegal activities involving scanners and other such receiving equipment, to participate in the enforcement of the requirements and prohibitions. Particular regard was had to initiatives that could be effected under the existing or amended Radiocommunication Act. Such initiatives, in turn, raised issues of both criminal and civil law.

It was concluded that in order to provide means by which persons affected by the distribution of restricted equipment would have recourse to civil courts of competent jurisdiction to halt such activities or to obtain compensation for harm suffered, a new offence and civil right of action would have to be added to the Radiocommunication Act. The section permitting the new civil right of action would then parallel the section of the Act that was added by Bill C-109 to allow a civil course of action for those persons directly harmed by the divulgence or use of intercepted information.

Such a measure, by focusing on the manufacturers, importers and distributors of equipment, rather than on individual users, would likely make enforcement more effective. It would also permit the participation of third parties in the enforcement of the restrictions, thereby potentially lessening the enforcement burden on the Department. Further study will be necessary to determine the effectiveness of the proposed right of civil action as an enforcement tool: a third party (such as a cellular service provider) would have to suffer harm before action were taken, and proof of such harm due to the manufacture or importation of a digital scanner might be difficult to demonstrate.

7. OPTIONS

Accordingly, Industry and Science Canada invites public comment on the following options:

Option 1 - No restrictions would be imposed on devices capable of monitoring cellular conversations.

Considerations favouring this option include the current existence of large numbers of analog scanners (and of other devices) capable of providing access to cellular transmissions, the difficulty of enforcing a ban, the fairness of imposing a ban on only those radio receivers and scanners capable of providing access to the cellular bands, and the ease with which scanners could be modified (and with which equipment could be built) to receive cellular frequencies. As well, regard must be had to the expenses of enforcement, to the economic consequences to retailers of restrictions on analog scanners, and to the impact on existing owners and would-be hobbyists.

Adoption of this option would, however, preclude utilization of an important measure in an overall strategy directed to the enhancement of the privacy of cellular telephone users.

Option 2 - Restrictions on cellular monitoring devices would be imposed, with respect either to all radio receivers and scanners, or only to those devices capable of monitoring digital cellular.

The differences in technology, and the existing widespread availability of analog scanners, may mean that different treatment should be accorded analog and digital scanners.

In respect of this option, parties are invited to also comment on the following issues:

(i) the means of enforcement, which could include -

(a) removal, from the current general exemption of receivers from the radio authorization requirements of the Radiocommunication Act, of radio receivers capable of monitoring (digital, or all) cellular communications, by means of amendments to the General Radio Regulations, Part II;

(b) amendment of the Radiocommunication Act to create a new offence prohibiting the manufacture, importation, distribution, or sale of radio receivers capable of monitoring (digital, or all) cellular communications, and to create a new right of civil action to enable persons harmed by the distribution of such radio receivers to bring civil proceedings against the person causing the harm;

(c) both (a) and (b) as noted above; or

(d) other or additional means of enforcement;

(ii) whether regulations should be promulgated to define the eligibility of classes of persons to obtain, or to hold radio authorizations for radio receivers capable of monitoring (digital, or all) cellular communications;

(iii) the desirability of establishing a requirement for a technical acceptance certificate in respect of (digital, or all) cellular scanners, or other cellular telephony monitoring receivers;

(iv) the optimal definition of "scanner" or "cellular telephony monitoring device", so as to include within the ambit thereof the devices sought to be restricted, without adversely impacting on legitimate users and uses of telecommunications equipment;

(v) the restrictions, if any, that should be imposed with respect to cellular telephones that can be programmed to act as cellular scanners.

Additional Comments

Parties are also invited to submit comments on whether radio-based telephone communications other than cellular should be extended protection equivalent to that afforded cellular telephony.

8. PUBLIC SUBMISSIONS

Industry and Science Canada invites written submissions from all interested parties on the above options and issues. Submissions should be addressed to the Director General, Telecommunications Policy Branch, Industry and Science Canada, 300 Slater Street, Ottawa, Ontario, K1A 0C8. To ensure consideration, submissions must be received within 90 days of the date of the publication of this notice in the *Canada Gazette,* Part I. All submissions must cite the *Canada Gazette,* Part I, the publication date, the title and the notice reference number.

All submissions received in response to this notice will be made available for viewing by the public two weeks after the closing date of this notice, during normal business hours, at the Industry and Science Canada Library at 300 Slater Street, Ottawa, Ontario, and at the former Department of Communications regional offices at Moncton, Montréal, Toronto, Winnipeg and Vancouver, for a period of one year from the close of comments.

Also, approximately two weeks after the closing date of this notice, copies of the comments may be obtained by telephone, facsimile, mail order or over the counter from ByPress Printing and Copy Centre Inc., 300 Slater Street, Unit 101A, Ottawa, Ontario K1P 6A6, (613) 234-8826, facsimile (613) 234-9464. Reasonable costs of duplication and distribution will be charged.

ANNEX 1

HOW CELLULAR TELEPHONY WORKS

General Operation of Cellular Systems

The cellular radio system is a mobile radio telephone system. It is controlled by a Mobile Telephone Switching Office (MTSO), and has a number of cell sites. The MTSO serves as the central coordinator and controller and as the interface between the cellular and the wireline networks. In North America, the cellular system operates in the frequency bands of 824-849 MHz (for mobile transmit) and 869-894 MHz (for base transmit). The transmit frequencies of the base stations and cellular telephones are separated by 45 MHz. The bands provide a total of 832 paired radio channels of 30 kHz bandwidth. In Canada, these channels in any given area are divided equally between the two cellular operators (i.e., 416 channels/operator).

The cellular system employs a high degree of frequency reuse. The available channel frequencies are distributed among a group or cluster of cells. Normally, a cluster consists of four, seven or nine cells, which form the basis of a repeating pattern. (The radius of a cell varies from 1 km to several km.) The channel frequencies are then reused in the next cluster of cells. Within a service area such as a city, a number of these clusters may need to be deployed, depending on the size of the area to be covered.

While a telephone conversation is taking place on a cellular system, it is entirely possible that the cellular telephone will move from one cell to another. When this happens, the system informs the cellular telephone and a hand-off of the call from one cell to another takes place. Since different adjacent cells are served by different channels, the continuation of the conversation is transmitted over a different pair of frequencies.

Difference Between the Analog and Digital Cellular Systems

The North American analog cellular system is called the AMPS (Advanced Mobile Phone Service). It uses the FDMA (Frequency Division Multiple Access) technique, in which the voice signal frequency modulates (FM) the carrier frequency.

The digital cellular system is different from the analog system in a number of ways. Some of the major differences are:

(1) In the digital cellular system, the voice is transmitted in the form of digitized numbers (which represent speech in a very efficient manner), rather than as an analog waveform.

This technique is called VSELPC (Vector Sum Excited Linear Prediction Coding), and is a low-bit-rate voice coding technique.

(2) The digital cellular system has a higher capacity. Since it uses a TDMA (Time Division Multiple Access) technique, one channel is capable of serving three users in a time-shared fashion; basically, the channel is available to each user one-third of the time. During the period available to each user, a speech burst is coded and transmitted. At the receiving end, the speech burst is decoded and converted back to the continuous analog format of the speech signal.

(3) The digital cellular system uses a digital modulation technique called QPSK (Quadrature Phase Shift Keying), which is different from the analog FM technique.

The North American digital cellular standard which encompasses the above was developed by the Cellular Telecommunications Industry Association, and is referred to as EIA/TIA IS-54 (Electronics Industry Association/Telecommunications Industry Association Interim Standard 54).

ANNEX 2

VOICE SCRAMBLING FOR ANALOG CELLULAR SYSTEMS

In analog cellular systems, at least two techniques exist that can be used to scramble the cellular voice transmissions:

(1) The first technique, called Variable Split Band Inversion (VSBI), is currently being introduced by Bell Mobility Cellular as the Privacy Plus system. VSBI operates by altering (scrambling) the arrangement of high and low speech tones to the point where speech cannot be recognized. The arrangement of high and low tones is changed many times per second, according to a sequence called a "cipher". The two scrambling units agree on a cipher sequence at the beginning of each private conversation and that particular cipher is known only to the two units. It is virtually impossible for an unauthorized listener to find out what the cipher sequence is and descramble the speech. This system, which was developed by Cycomm Corporation, is now available from Bell Mobility Cellular at a cost ranging from $20 to $50 a month, depending on the contract chosen.

(2) The second technique is based on time domain scrambling, significant work in this area having been done by the Communications Research Centre for High Frequency, or short-wave communications, applications. It is different from the first technique in that the inversion takes place in the time domain rather than in the frequency domain. Here, the voice signal is divided into many time segments, which are then moved around according to a sequence known only at the two ends of the desired communications. A time delay of half a second may be experienced using this technique. There is no system using this technique available in the market at this time, but the technique can quite readily be converted into a commercial product.

In both techniques, two devices are required, the first to scramble the caller's voice and the second to descramble the voice for the intended listener. One unit is connected to the subscriber's cellular phone, and the corresponding unit is connected to the Mobile Telephone Switching Office (MTSO); this

arrangement secures the transmissions between the cellular phone and the MTSO. The wireline portion of the call is not itself scrambled. Of course, if the other party is using a cellular phone as well, it will be necessary for that other party to also use a scrambler in order to ensure a conversation that is secure from end to end.

In response to the concerns which were raised about cellular telephone privacy, the Minister of Communications indicated that each cellular service provider would have to offer effective and affordable encryption measures as an option to its subscribers. This requirement was announced by the Minister on December 9, 1992, and is currently being implemented. Either of the described scrambling techniques (and perhaps others) would appear to fully satisfy, for analog cellular transmissions, the obligation to provide the encryption option.

While both of these techniques work in the analog cellular system, they cannot be applied to digital cellular systems. Because the voice signal in digital cellular is not transmitted as an analog waveform, but rather in the form of digitized numbers which represent speech, the scrambling of the voice signal either in the frequency or time domain would cause severe problems to the voice coding technique used in digital cellular systems. Hence, other techniques have to be used instead.

ANNEX 3

AN EXAMPLE OF AN ENCRYPTION TECHNIQUE FOR DIGITAL CELLULAR

To encrypt a digital signal on a cellular telephone requires the introduction of encryption circuits in the digital cellular telephone at a point between the codec (the voice encoder and decoder) and the modem (the modulation and demodulation hardware which converts information from electronic signals to radio frequency signals); equipment is also required at the Mobile Telephone Switching Office to decrypt the coded signal. Modifications to the digital cellular standard will be necessary, but these are not expected to be difficult to effect. With encryption, the security of the cellular radio link will be very high, but an increase in the cost of the service and the hardware can be expected.

The successful operation of digital encryption on a cellular radio channel, which is at times subject to interference and noise, depends on the encryption method used. The preferred encryption method is a relatively simple one called stream cypher. Stream cypher causes the data transmitted to be "modulo 2" added to the output of a pseudo-number sequence generator. Upon reception, the demodulated data is "modulo 2" added to another sequence generator, restoring the encrypted data to its original form. Of course, the two generators have to be in synchronization, and error detection and correction can also be applied to the data.

The security of the stream cypher is compromised if the encryption key is known, because the encryption key defines the pseudo-number sequence that is used in the process. Such systems are vulnerable to plain text attack if a large number of messages encrypted with the same key are intercepted. This can be avoided by changing the encryption key as often as possible, thereby denying code breakers the opportunity to find the key by applying statistical methods. The "Diffie-Hellman key exchange" can be used at the start of every call to change the encryption key automatically.

The combination of Diffie-Hellman key exchange and stream cypher encryption offers sufficient protection for the transmission of most commercial information.