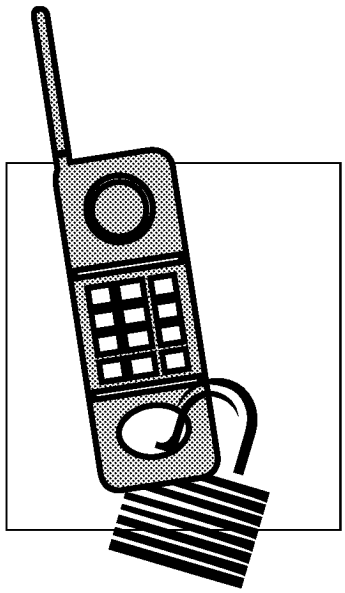
Privacy, Security, and Fraud 10

As wireless technologies become more widely used and more closely integrated into the National Information Infrastructure (NII), concerns about privacy, confidentiality, the security of communications, and protection from fraud will become increasingly important (see box 10-1).[1] Although laws that address such issues do exist, users of wireless technologies generally have less assurance of confidentiality and protection from fraud than do users of traditional wireline systems. This is due to the fact that most radio transmissions are much easier to intercept than those transmitted over a wireline system. The extent to which the public is aware of these problems is unclear, but among radio enthusiasts the open nature of radio signals has long been recognized, and is the basis of the popular pursuit of scanning or recreational eavesdropping.[2]

Until recently, privacy violations and fraud affected a relatively small number of users and technologies. Today, as wireless communications systems proliferate and the number of radio communication devices expands, the problems are becoming more severe—the worst of which is theft of service through fraud. Concerns about the confidentiality and security of wireless data transmission, for example, are rising as more companies turn to



[1] OTA has done several studies of aspects of telecommunications privacy and security. See U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606 (Washington, DC: U. S. Government Printing Office, September 1994) and U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information,* OTA-TCT-576 (Washington, DC: U. S. Government Printing Office, September 1993).

[2] Scanners have their own magazine, *Monitoring Times,* which has a circulation of 30,000.

BOX 10-1: Definitions

Many of the terms used in this chapter to discuss privacy and security have ambiguous meanings, and are used in various ways by different people. ' In this report, OTA uses the following definitions:

- *Confidentiality* refers to the nondisclosure of information beyond an authorized group of people.
- *Privacy* is distinguished from confidentiality in that privacy refers to the balance struck between an individual's right to keep information confidential, and society's right to have access to that information for the general welfare. Privacy laws codify this balance, and also provide for some level of individual control over information about themselves.
- *Security* refers generally to the protection individuals desire against unauthorized disclosure, modification, or destruction of information they consider private or valuable. Security is maintained through the use of safeguards, which can be implemented in hardware, software, physical controls, user or administrative procedures, and the like. In practice, security and safeguards are often used interchangeably.
- *Fraud* refers to the use of deception to gain something of value, such as someone using another's telephone account number or other identifier to steal telephone service.

[1] For more detailed discussion of these definitional issues, see U.S. Congress, Office of Technology Assessment, */formation Security and Privacy in Network* Environments, OTA-TCT-606 (Washington, DC: U. S. Government Printing Office, September 1994), pp. 26-29,82-83.

SOURCE: Office of Technology Assessment, 1995.

wireless technologies to meet their data communication needs. The use of radio technologies in the context of the NII is especially problematic because the vulnerability of the radio link to eavesdropping also exposes the wireline portion of public voice and data networks to privacy and security violations and fraud, and in ways that are difficult to guard against. This chapter examines the problems of privacy, security, and fraud in today's wireless networks, and discusses possible technical, regulatory, and administrative solutions.

FINDINGS

Wireless technologies invite privacy and fraud violations more easily than wireline technologies due to their broadcast nature. The privacy implications of widespread use of mobile wireless technologies are potentially serious for both individuals and businesses. There will be a continuing need to guard against eavesdropping and breaches of confidentiality, as hackers and scanners develop ways to listen in and track wireless commu nications devices.

- It is unclear how successful efforts to address privacy and security concerns regarding wireless telecommunications have been. Laws designed to protect wireless telephone users, while potentially helpful, may not go far enough, and enforcing them is difficult. Likewise, the success of the efforts of wireless service providers to combat fraud and provide secure communications is hard to measure. Technical changes may make systems more secure than they are today, but each time new security measures are implemented, criminals find new ways to "beat the system." For the most part, industry implements technical changes that frustrate fraud and prevent violations of personal privacy. However, it is unlikely that wireless fraud will ever be completely eliminated.
- The true extent of service theft through fraud in the wireless (primarily cellular) industry is un-

known, but is estimated to directly cost the industry $482 million per year. Indirect costs may range as high as $8 billion per year. Unfortunately, this cost is distributed across all paying wireless customers in the form of higher bills. Customers can help protect themselves from fraud through vigilant scrutiny of their wireless telephone bills, but it is unclear how well the general public understands its vulnerability or the extent and cost of wireless fraud. Greater public awareness—through education and warnings provided by wireless service providers and equipment manufacturers—could help combat the problems.

- Wireless systems, coupled with improved location identification technologies, may make it easier to track people's movements. In the course of listening in on a conversation or intercepting a data communication, an eavesdropper may be able to determine the location of the user. Location information is a particular concern to individuals, especially when it can be gathered in the normal course of wireless telecommunications operations.[3] Businesses using wireless systems for voice and/or data communications may be monitored for purposes of industrial espionage. Treatment of location information in law is not yet consistent.

Options

If Congress feels that wireless privacy, security, and fraud are problems, it could consider three principle options:

1. Congress could amend the U.S. Code to make possession of scanning equipment and number-altering software illegal.[4] Currently, possession of specialized scanners and software is not illegal—only its purchase and use with intent to defraud.
2. Congress could require cellular carriers and equipment manufacturers to give explicit warnings about the possibility of fraud and breaches of privacy in service agreements, instruction manuals, bills, or other service agreements; on handsets in the form of labels; and elsewhere to help educate consumers.
3. Congress could consider authorizing increased funding of the Electronic Crimes branch of the Secret Service, and of the enforcement division of the Federal Communications Commission, to combat wireless crimes. The Secret Service estimates that its electronic crimes enforcement effort would be at optimum staffing levels with 50 more agents, which would cost an estimated $4.5 million.

CONFIDENTIALITY AND PRIVACY

People using wireless communication systems—for either voice or data applications—may incorrectly assume that because their cellular telephone or portable computer operates roughly like their wireline counterparts that they are subject to the same privacy laws and possess the same safeguards. But there have been numerous widely publicized cases of eavesdropping on and recording of cellular telephone calls, including those of prominent political or society figures, such as Virginia Governor Douglas Wilder, and Princess Diana of Wales. Both the mayor and police chief of New York City reportedly have had their telephone calls monitored. Businesses routinely warn their employees not to conduct sensitive business on cellular telephones.[5]

Telecommunications privacy and security have been the subject of gradually evolving law and

[3] See Internet posting Subject: Does GSM track the physical location of a phone?, Date: 20 April 1995 08:32:19 +0200, From: mobile-rg@dxm.ernet.in, To: cellular@dfv.rwth-aachen.de, Message-ID: <9504200632.AA02651@lorien.dfv>.

[4] 18 U.S.C., sec. 1029 (a).

[5] Milo Geyelin, "Cellular Phone May Betray Client Confidences," *The Wall Street Journal*, Sept. 1, 1994, p. B1.

regulation since the early days of telephony (see box 10-2).[6] Telephone communications are generally protected against unauthorized listening or recording under the Communications Act of 1934 and other privacy statutes, principally the Electronic Communications Privacy Act of 1986 and the Communications Assistance to Law Enforcement Act of 1994. Fraudulent use of someone's telephone accounts is prohibited under the criminal code concerning access device fraud.[7]

There are two main types of information that merit protection in the wireless context: 1) the contents of a call or transmission and 2) the location of the sender or recipient. The privacy of call contents is easily understood, and has generated the most concern and regulation. Privacy of location information, however, is a relatively new concept, and may pose unusual management and social challenges.[8]

Privacy of Transmission Contents

As a practical matter, listening or scanning are generally not prosecuted, particularly when the contents of intercepted transmissions are kept confidential and when not used for a commercial purpose by the unauthorized recipients. This degree of privacy is sufficient for many people, such as those who use cordless telephones, but is nevertheless troublesome for those who desire confidentiality comparable to that of traditional wireline telephones. This relative insecurity of wireless telecommunications is responsible in part for interest in technological safeguards to protect confidentiality.

There are some security-protecting features of mobile communications, however, that make widespread and intrusive wireless monitoring less likely. While scanners can pick up conversations fairly easily, finding any particular one is difficult. It is even harder in networks with many simultaneous conversations and where one or both of the participants is mobile. Calls are handed off from cell site to cell site, making it hard to track a specific conversation for very long. Despite large investments in technologies that could pick out individual conversations from all those passing through the public switched networks, even the government, much less private individuals or organizations, still cannot do this well.[9]

Wireless data network providers, such as RAM and Ardis, claim that their systems are inherently more secure than analog cellular telephony, because of their digital formats, and error-checking and correction protocols. Data are typically transmitted in digital packets, each containing an address instructing that packet where to go and in what order. Eavesdropping would require intercepting the right packets, identifying the header

---

[6] James E. Katz, "U.S. Telecommunications Privacy Policy," *Telecommunications Policy*, vol. 12, December 1988, p. 354.

[7] 18 U.S.C., sec. 1029.

[8] Because wireless telecommunications systems are typically interconnected to other telecommunications networks, privacy of wireless signals can be compromised in either the wireless or the wireline portion of a transmission. Privacy also may be compromised by someone scanning the frequencies used for the wireless portion of a cellular call; in this case, the wireline portion of the call will also be compromised. The base station or the wireline system itself may be physically tapped as well. This section will focus only on attacks on the wireless portion of a call.

[9] Unclassified information on government surveillance capabilities is difficult to obtain. Public statements by current and former intelligence officials can give some indication of these capabilities, as in this report of a presentation given by former National Security Agency head, Adm. Bobby Inman: "Inman [pointed out to an MIT seminar] that current cellular phones are difficult to monitor because "there's no technology that can sweep up and sort out phone conversations" despite very large investments in this. He drew an analogy to a case where he had to inform President Carter that an insecure dedicated private land line to the British Prime Minister had been compromised. Inman told Carter that the nature of the public phone system, with its huge volume and unpredictable switching, would have made using a pay phone more secure." Internet posting to Red Rock Eater listserver, Date: Wed, 23 Nov. 94 09:54:12 EST, From: lethin@ai.mit.edu (Rich Lethin), Subject: Admiral Inman visits MIT.

BOX 10-2: Wireless Communications Privacy and the Law

The legal status of the privacy of wireless communications has evolved overtime. Since most wireless signals can be received by anyone with a radio or scanner tuned to the correct frequency, they are inherently less secure than their wireline counterparts—undermining any reasonable expectation of privacy. Congress has, however, established limitations on the right of people to receive or intercept wireless transmissions. These limitations have grown more extensive and explicit as wireless telecommunications systems have become more widely used.

Historically, the struggle over the privacy of communications has been a battle between an individual's right to privacy and the legitimate needs of law enforcement to conduct surveillance (wiretapping, interception) in the investigation of crimes. Striking a balance in this area has proven difficult for the courts and Congress as wired and wireless communication technologies have advanced—new technologies made old assumptions, decisions, and regulations about privacy and surveillance obsolete. In fact, for the first 70 years of this century, the specific implications of privacy and wiretapping laws for wireless services (and vice versa) generally were not even considered because the public generally did not use radio systems to communicate with one another.

The first general set of communications privacy limitations are found in the Communications Act of 1934.[1] The act made the intercepting or divulging of private communications, by whatever medium, illegal, except by authorized communications company employees or on lawful demand by law enforcement officers.[2] In 1967 the Supreme Court ruled in *Katz v. United States* and *Berger v. New York*[3] that certain wiretapping operations violated the Fourth Amendment protection against unreasonable search and seizure. Largely in response to these cases and to law enforcement concerns about its ability to conduct wiretapping operations, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968.4 Title Ill of this act tried to strike a balance between individual privacy rights and law enforcements' needs, and set forth the conditions under which law enforcement could intercept private communications. Subsequently, some courts found that the protections of the Act against unauthorized interception generally did not apply to radio-based communications, while others protected some radio communications.[5]

As wireless technology developed and came into more widespread use, the special problems of privacy in a wireless environment became clearer-especially in the case of cordless and cellular phones. Early court cases limited an individual's reasonable expectation of privacy when using a wireless phone, holding that such calls were exposed to many people who could easily listen in—intentionally or by accident.[6] The Electronic Communications Privacy Act (EC PA) of 1986 extended the privacy provisions of Title Ill to cellular telephones, most pagers, and other electronic communications, including electronic mail, but specifically exempted cordless phones from privacy protections.[7] The Act also made the disclosure of protected communications illegal. In response to concerns about increased monitoring of cellular telephone calls, leg is-

---

[1] Ch. 652, Title Vll, sec. 705, 48 Stat, 1064, 1103 (June 19, 1934), codified at 47 U.S.C. sec. 605 (a),

[2] In *Nardone v. United States,* 302 U.S. 379,380-81 (1937), the Supreme Court ruled that Section 605 of the Communications Act generally prohibited interception and subsequent disclosure of wire communications. In the middle third of this century, however, law enforcement authorities continued to use wiretaps, and the number of court cases over wiretaps arising in the 1930s and 1940s makes it clear that section 605 prohibitions did not end the practice of wiretapping.

[3] 389 U.S. 347 (1967), 389 U.S. 41 (1967).

[4] See especially Title Ill, Pub. L. 90-351, June 19, 1968; 82 Stat. 197.

[5] *State v. Delaurier,* 488A.2d 688 (R.I. 1985). In *United States v. Hall,* however, the court held that a transmission between a mobile telephone and a landline telephone was protected, but a call between two mobile telephones was not. 488 F.2d 193 (9th Cir, 1973).

[6] See *United States v. Hoffa, 436* F2nd 1243 (7th Cir. 1970).

[7] Pub, L. 99-508, Oct. 21, 1986, 100 Stat. 1848.

(continued)

BOX 10-2 (cont'd.): Wireless Communications Privacy and the Law

lation banning the manufacture or import of scanning devices capable of receiving cellular frequencies was passed in 1992.[8]

The Communications Assistance to Law Enforcement Act of 1994 (CALEA) finally extended to cordless telephones and wireless data communications systems—including wireless local area computer networks-the same protections cellular telephones enjoyed.[9] In several cases since 1986, the courts had found that users of cordless phones had no objectively reasonable expectation of privacy—as cordless telephones operate in readily accessible public spectrum used by a variety of unlicensed devices—and could be intercepted without a wiretap authorization.[10] By 1994, however, the use of cordless phones had become ubiquitous, and lawmakers found that the public believed their cordless phone calls were as private as a wired telephone-when, in fact, they were not. Responding to this sentiment, Congress made a legislative determination that such communications should be protected.

Conceptually, the limitations on intercepting wireless communications fall into two groups: those involving possession of scanning or listening devices, and those involving the actual receiving, using or divulging the contents of transmissions.

As noted above, the manufacture or import of cellular frequency scanning equipment is illegal. However, legitimate scanners (used to monitor police, fire, emergency and other public radio services, and manufactured without the ability to monitor cellular frequencies) can easily be adapted to receive cellular frequencies; information on how to make such adaptations is easy to acquire, and kits to make such adaptations are not banned and may be purchased legally. Even prohibiting all scanners outright is not sufficient to prevent scanning: nearly any cellular telephone call can be picked up using another cellular telephone.[11] It is estimated that there are over 5 million scanning units in the United States today; a unit typically costs $300 or less, Thus, possession of scanners or equivalent equipment capable of listening to cellular telephone calls is difficult to prevent; such devices are essentially available on the open market, and are widely used recreationally by some radio enthusiasts.

Apart from possessing a scanner or receiver, unauthorized and intentional listening to cellular and cordless telephone calls is also illegal, regardless of the frequencies monitored, as is divulging or making use of their contents.[12] *Inadvertently* received transmissions, such as when someone is scanning the spectrum for some legitimate purpose, may not be divulged or published either, and the person receiving such transmissions is enjoined from benefiting in any way from the communication. Broadcasts intended for use by the general public, such as communications to ships, airplanes, amateur or citizens band radio are not prohibited.

---

[8] Pub. L. 102-556, Title IV sec. 403(a), Oct. 28, 1992; 47 U. S. C., sec. 302a (d). The law denies authorization of equipment that can receive transmissions in the cellular telephone frequencies, of equipment that is capable of being altered to receive such transmissions, or that can convert digital signals in those frequencies to analog voice audio. The U.S. manufacture or Importation of such devices is also illegal. In addition, under a different statute, 18 U. S. C., sec. 2512, the export, import, manufacture, assembly or possession of equipment whose primary function is the surreptitious interception of private electronic communications, including wireless transmissions, is illegal, and violators are subject to fines and/or five year prison terms.

[9] Pub.L. 103-414, Oct. 25, 1994; 108 Stat. 4279.

[10] See, e.g., *United States v. Smith,* 978 F.2d 171 (5th Cir. 1992); *United States v. Carr,* 805 F. Supp. 1266 (E.D.N.C. 1992).

[11] Some old television sets with UHF tuners can be tuned to cellular frequencies because these frequencies Were allocated from the upper portion of the UHF band, channels 70 to 83.

[12] Two statutes apply in this general area. Under 47 U.S.C., sec. 605 (a) violators are subject to fines and/or months imprisonment, for the first conviction, and maybe subject to civil damages as well, unless the court finds that the person was unaware of the violation, when damages may be reduced to a fine only. For violations involving commercial advantage, the penalties are fines and/or two years imprisonment for a first offense, and fines and/or five years for subsequent offenses. Under 18 U. S. C., sec. 2511(1), violators are subject to fines and/or a five-year prison term; first offenders are only fined.

SOURCE: Office of Technology Assessment, 1995.

codes, and then reassembling them, probably requiring weeks of work per message, and consequently the results in most cases would not be available in real time.[10]

Several different methods are being used or developed to make wireless networks more secure. Special modulation formats may be used. If signals are encoded in some way, an eavesdropper must have decoding equipment as well. Numerous techniques for encoding are undergoing testing or already deployed. In the future, digital transmission schemes, which were developed to make more efficient use of limited radio spectrum, may also make transmissions more secure. In addition, signals can be encrypted. Both types of technologies are discussed below.

Transmission Schemes

Analog cellular and other traditional radio systems typically transmit information over a single channel in what is known as "circuit switched" transmission. That channel is dedicated to the user for the duration of the call. The technologies are relatively simple and inexpensive, but they use radio spectrum inefficiently. They are also easy to listen in on—once a call has been found, a scanner can lock onto it until the conversation ends, or one of the parties leaves the cell and drops the channel.

New digital communications systems, such as time division multiple access (TDMA) or code division multiple access (CDMA) use spectrum much more efficiently because they break conversations into digital bit streams in order to carry more conversations simultaneously over the same amount of spectrum (these systems are described in more detail in chapter 3). These separate fragments are reassembled by the receiver and presented to the listener as a complete and intelligible conversation. These techniques also make transmissions more difficult to intercept. Without knowing what the disassembly scheme is, an eavesdropper will hear only unintelligible noise. Thus, digital transmission schemes are desirable for reasons of both economy and security.

TDMA and CDMA differ considerably, however, in the degree of security and efficiency they provide. With TDMA, conversations are broken into segments based on a timing scheme. Each user of a channel is "assigned" one of three time slots by the cellular base station equipment. The time sequences must be known in order to separate out all the conversations occurring on that channel, and to reassemble any particular transmission. This is a straightforward technical task, but it is more difficult and costly to do than monitoring a comparable analog cellular conversation.

CDMA transmission schemes are based on a different principle, known as "spread spectrum." Instead of assigning a time slot on a single channel, CDMA uses many different channels simultaneously, and the network assigns a code to each fragment of a conversation like an identifying label. The receiver recognizes the specified code, sent at the beginning of the transmission, selects all transmissions with this code, and reassembles them into a coherent whole. CDMA is also inherently more difficult to crack because the coding scheme changes with each conversation, and is given only once at the beginning of the transmission. Receivers lacking the proper code to intercept will only hear digital noise.[11] Keeping track of codes is a demanding signal processing task, and it is not likely that eavesdroppers will have the technical or financial wherewithal to monitor CDMA traffic in the near future. Thus, monitoring transmissions on CDMA systems is considerably more difficult than with TDMA and far harder than with analog systems, providing a greater degree of security. However, since the technical standards for both TDMA and CDMA are open and published, they are theoretically susceptible to attack.

---

[10] Ellis Booker, "Is Wide-Area Wireless Secure?" *Computerworld*, vol. 26, No. 39, Sept. 28, 1992, p. 59.

[11] The inherent properties of this scheme explain its attractiveness to and use in the military.

Encryption

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

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

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

Privacy of Location

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> Many of these technologies involve surveillance of the location and behavior of identified vehicles and/or people, and the collation of such data for further use. These and other aspects of IVHS technologies raise concerns amongst the community, and have delayed adoption of some systems.[20]
>
> [S]ome proposed designs require the system to collect vast amounts of data on individuals' travel patterns, thus raising the potential for severe invasions of privacy. To make social choices about IVHS, it is necessary to reason about potentials for authoritarian uses of an IVHS infrastructure in the hypothetical future.[21]

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

Location and legal jurisdiction

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

---

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

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

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

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

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

ly meaningless. Work on transborder data flows has attempted to address this problem, but its resolution is unclear. The Internet also poses similar problems of geographic location, jurisdiction, and the law.[22]

CELLULAR AND OTHER WIRELESS FRAUD

With widespread use of wireless telephony has come widespread theft of service by fraudulent means. The true extent of cellular telephone fraud is unknown, but the number of attempted fraudulent calls may run as high as 3 million per month.[23] The Cellular Telephone Industry Association (CTIA) estimates that fraud amounts to about $482 million a year, based on estimates of out-of-pocket costs to companies for customer-identified calls for which the company reimburses customers.[24] Other analysts believe the cost is substantially higher. The government has no independent estimate of the extent of wireless telephone fraud.

For wireless technologies to enjoy the same public acceptance as wireline telecommunications, they will probably need to provide similar levels of security from fraud and misrepresentation. Fraud increases service costs for both businesses and consumers, and may make wireless less competitive than wireline services. Cellular customers ultimately pay for cellular phone fraud in the form of higher costs because companies pass these costs along to consumers.[25] It is also costly for law enforcement agencies to enforce fraud statutes, and it fosters the expansion of criminal activities, both directly and indirectly. Fraudulent phones are frequently used in the commission of other crimes, and hinder law enforcement efforts against those criminals.

This section will discuss cellular telephone fraud and how it is committed. It will also describe some of the technical and organizational cost-benefit tradeoffs the industry has made that shape the incidence of fraud. Finally, technical measures that might be taken to limit fraud in the future will be addressed briefly. The focus is on cellular telephones because currently experience widespread fraud. Although the pirating of satellite television signal is still a problem, it is not addressed here. The heyday of pirating is long since passed, and with the introduction of new digital transmission and encryption systems, fraud is expected to drop further.

Tumbling and Cloning

Cellular telephone fraud is conducted through what is known as "tumbling" and "cloning." Understanding how these work requires a brief description of how a cellular telephone identifies itself to the cellular network, and how billing is managed.

Every cellular telephone has a unique electronic serial number (ESN), "burned in" on a chip by the manufacturer. FCC regulations require that every phone have a unique ESN. In addition, every cellular telephone subscriber is issued a mobile identification number (MIN) when the phone is assigned a telephone number and activated by the service provider. For example, when a subscriber buys a cellular telephone at a retail store, the service provider assigns a telephone number from a batch of numbers provided by the local telephone

---

[22] Dan L. Burk, "Transborder Intellectual Property Issues on the Electronic Frontier," Arlington, forthcoming in vol. 5, *Stanford Law & Policy Review,* available at URL gopher://gopher.gmu.edu:70/00/academic/colleges-depts-insts-schools/ law/working/dburk2.

[23] Susan Kumpf and Nora Russell, "Getting the Jump on Fraud," *Cellular Business*, vol. 9, No. 10, October, 1992, p. 24.

[24] "Secret Service, CTIA Crack Down on Cellular Fraud," *Telecommunications Reports*, vol. 61, No. 15, Apr. 17, 1995, p. 32. Cellular telephone firms are unwilling to give an accurate accounting of cellular telephone fraud to CTIA. Telephone toll fraud generally may be as much as $8 billion per year, with international toll fraud comprising 65 to 80 percent of the total. Dan O'Shea, "Security Products Abound, But Is Toll Fraud Too Tough?" *Telephony*, vol. 225, No. 9, Aug. 30, 1993, pp. 7, 13.

[25] Because cellular companies are unregulated, there are no public ratepayer issues with cellular fraud.

monopoly, and records both the MIN and the ESN as an associated pair.

When a call is initiated, the phone transmits its ESN and MIN to the cellular switch. This is done over a signaling channel, reserved for setting up a call between the handset and the switch. If the two match, then the call is permitted to proceed and a voice channel is opened. If a call is made outside the regular service area, the remote cellular company relays the ESN/MIN pair to the home company or to a regional database to check whether the number is valid (the negative number list), in accordance with an industry standard, IS-41. If it is authenticated, the call is permitted to go through. The air time and roaming charges are forwarded to the home company at the end of the call, and the two companies settle up periodically to clear outstanding balances.

With traditional analog cellular systems, "tumbling" is quite simple. A fraud perpetrator (or "bandit," the preferred term) randomly or sequentially changes the ESN and/or the MIN after each call. Because the cellular switch takes some time to verify each number, some proportion of calls may get through the system before the system denies access. Tumbling is currently not very prevalent because cellular operators have installed systems that can defeat it fairly easily. When GTE installed its pre-call validation system in December 1991, 25 percent of attempted fraudulent calls were denied connection. Other cellular carriers have even higher levels—for example, up to 61 percent by Ameritech Mobile Systems in Detroit, MI.[26] Once the technology is deployed, bandits typically move on to other forms of fraud.

"Cloning" works a bit differently. Cloners pick up ESN/MINs on busy streets or highways with scanning equipment that is legally available, although their use for this purpose is illegal.[27] The devices typically monitor cellular signaling channels, and display broadcasted ESN/MIN pairs. Cloners record these number pairs, and send them to other cities, whose carriers may be unable or unlikely to verify that the number is in use elsewhere or was so recently used in another place as to be fraudulent. In the remote city, a participant in the fraud scam uses a standard personal computer or laptop with legally available software to reprogram the ESN/MIN in a cellular telephone, which can be done with existing external connectors to the phone.[28]

This phone is then either sold or used by someone wanting to make free calls or who does not want to be traced, either by law enforcement agencies who might have a wiretap order on a known number or by the telephone company for billing purposes.[29] Because a fresh number has not yet been identified as fraudulent in the negative number list, checking that database will not prevent fraud the first time it is tried. Depending on whether the original owner of the stolen number notices the charges on the bill, and how often the databases are updated, a cloner may be able to use the cloned phone for some time and run up a substantial bill. Real-time access to subscriber lists and activity records between companies handling calls is available in some markets for the purpose of defeating such scams. Industry officials esti-

---

[26] Kumpf and Russell, op. cit., footnote 23, pp. 24-25.

[27] These scanners are legitimately used by technicians in servicing cellular telephone equipment. They are designed to work within a very short range, about 10 to 15 feet. However, it is a simple matter to make them receive over a larger area by boosting the power. These scanners are readily available, including by mail-order.

[28] Phones could be made unreprogrammable, but there are legitimate reasons to keep them reprogrammable. One is the ability to change the number if the service provider changes, without having to change phones. Another is to allow changes in case the phone is compromised by a cloner.

[29] Some reports put the street price of a cloned phone at $300, with a guarantee to replace it if the number is turned off. Michael Meresman, "The Phone Clone Threat," *Mobile Office*, vol. 5, No. 11, November 1994, p. 62.

mate that, by the end of 1995, up to 70 percent of the U.S. carriers will have this capability.[30]

Today, if the customer notices fraudulent charges and notifies his or her company, the company will remove the charge, pay the long distance charges, reimburse costs to the remote company if roaming has occurred, and absorb the loss. Companies have done this since beginning operations in the early 1980s, but are under no legal obligation to do so.

Call Selling

Call selling is an illegal activity conducted with cloned cellular telephones. In the view of CTIA, this may be a greater revenue drain on firms than simple cloning. In essence, in a call selling operation, perpetrators set up their operation in a hotel room or an apartment with a number of cloned cellular telephones. They advertise informally to immigrant communities, among others, that they will sell calling time to their home countries significantly below international rates. The defrauders not only do not pay for the use of the telephones, but they also receive cash payments for their use. Immigrant communities are willing to spend a significant portion of their monthly income to call overseas, and are typically looking for ways to reduce their calling costs.

Such fraud operations are highly profitable, less risky and much less physically dangerous than other types of organized crime, such as drug trafficking. As a result, some law enforcement officials believe that cellular fraud will continue to grow significantly in the future.[31] Cloners move quickly to break new protection schemes, often succeeding within six months of their introduction.[32] The switch to digital technologies will offer users some protection, but analog systems will continue to operate and be susceptible to fraud for many years.

Law Enforcement

Altering the ESN/MIN pair of cellular telephones by counterfeiting these numbers is covered by the same statutes as credit card or currency counterfeiting, in that fraudulent means are used to gain access to the telecommunications system.[33] Thus, identifying and arresting perpetrators of cellular fraud is primarily the responsibility of the U.S. Secret Service, which has primary federal jurisdiction over fraud. State and local law enforcement officials are also involved to some extent, as well as the U.S. Drug Enforcement Administration, U.S. Customs Service, and the Federal Bureau of Investigation, depending on what other crimes are perpetrated using a cellular telephone. The Secret Service has recently put 20 of its 1,200 agents through the Electronic Crimes Special Agent Program, which prepares them for all types of electronic crimes, including wireless fraud.

Fraud investigation usually begins when a subscriber or carrier identifies some suspicious activity—for example, a rapid increase in traffic at a particular cell site. The carrier will then locate the source of activity using radio triangulation techniques, and will turn this information over to the Secret Service, who will attempt to get a warrant and make an arrest. The cities with the most cellular fraud are New York, Los Angeles, and Miami, but some of the recent large cellular phone fraud operations have been outside these three centers: in late 1991 and early 1992, over 57,000 calls were made in 19 days by Palestinians in the West Bank and Gaza to other countries in the Middle East via Phoenix, AZ, in a three-way calling scam.[34] Because the most costly element of cellular tele-

[30] Ibid, p. 64.

[31] Ibid, pp. 60-69.

[32] Tom McClure, CTIA Fraud Taskforce head, interview, July 5, 1994.

[33] 18 U.S.C., sec. 1029.

[34] Anthony Ramirez, "Theft Through Cellular Clone Calls," *The New York Times*, Apr. 7, 1992, p. D-1.

phone fraud is international calling, companies are beginning to offer international service only to those customers who specifically request it, about 5 percent of all cellular subscribers.

A number of technical efforts are under way to combat cellular (and by extension, other wireless telephone) fraud. Handsets can be made more secure and difficult to clone,[35] and cellular switches can be equipped with database and signal processing equipment and software to detect fraud and stop it there. Carriers are adopting personal identification numbers (PINS) that must be entered manually by the subscriber before a call can be completed, as is done with electronic bank cards.[36] The disadvantage of this method is that customers have to key in additional numbers, making calling less convenient.

Call screening systems with fast database and call pattern-recognition software are also being deployed. These systems work by monitoring the past activity of a particular subscriber. If new activity does not fit the established pattern, the calls are flagged and the owner of the phone is contacted to confirm unusual use. AirTouch, NYNEX, and Bell Atlantic Mobile have all begun to use these services within the past two years, and report reductions of up to 75 percent in stolen minutes.[37]

Experiments are also under way with systems that would identify the particular electronic signature of individual phones (each phone has slightly different electronic characteristics due to variation in the electronic value of components, which gives each phone a distinctive and identifiable profile).[38] Digital technologies will also make cloning more difficult. However, digital encoding schemes are known and can be broken, given enough time and computing power, even though the equipment to pick out numbers is more costly.

In fact, digital telephone standards IS-41 and the Global System for Mobile Communications (GSM) provide one such digital scheme. Cellular telephones would be programmed with a secret number that would never be transmitted. During call setup, the handset would prompt the cellular switch to transmit back to the handset a one-time number. The handset would then generate a one-time response based on its own secret number and the transmitted number to validate the call to the cellular switch. Since one of the two numbers lies in the carrier's database and changes with each call, and the other number is never transmitted, each number is unique and impossible to reverse-calculate.[39] Next-generation digital cellular telephones could perform this validation function easily, but existing analog telephones could not without expensive retrofitting.

It appears that cellular telephone fraud could be minimized by technical means, if the costs of

---

[35] Originally, the ESN was to be unprogrammable, a permanent part of the phone. However, cellular handset resellers resisted marketing such handsets, because the cellular carriers (in general unrelated to the resellers) charged the resellers for establishing service, making accounting changes, and the like. Resellers insisted on programmable cellular telephones, which the carriers ultimately did not oppose, primarily because the carriers depend heavily on the resellers to market their system and provide customer service. Some observers believe that this business dynamic between resellers and carriers is responsible for the technical configuration of cellular phones, which is inherently less secure than an ESN that is not reprogrammable. Internet posting to Telecom Digest, coyne@thing1.cc.utexas.edu, Subject: Re: Bell Atlantic Mobile Joins the PIN Crowd, Date: 10 Jan 1995, 20:12:46 GMT, Organization: the University of Texas at Austin, Austin, Texas.

[36] This service configuration was introduced in late 1994 by NYNEX Mobile Communications and Bell Atlantic Mobile. The ESN/MIN pair is transmitted over the reverse signaling channel, while the PIN is sent over the voice channel. Cloners are unlikely to be listening to both channels simultaneously or be able to associate the two numbers. If the PIN is compromised, the subscriber can simply get a new PIN by phone, rather than a whole new ESN/MIN, which is much more costly. Other companies have used variations on the PIN concept.

[37] Meresman, op. cit., footnote 29, p. 62.

[38] Ellis Booker and James Daley, "Cellular Carriers Gain New Fraud-Detection Weapon," *Computerworld*, vol. 27, No. 44, Nov. 1, 1993, p. 71.

[39] Meresman, op. cit., footnote 29, p. 32.

stopping it were lower than the level of fraud, and if users would be willing to forego the convenience of simple number dialing. Law enforcement officials and other industry observers agree that the problem is tractable. With more competitors in the marketplace for PCS, the ability of carriers to pass along these fraud costs will be limited. Carriers will likely have a greater incentive to limit costs by more vigorously limiting fraud. They could press equipment manufacturers for handsets that contain unclonable technologies, to overcome the weakest link in the wireless security chain. As new technology is deployed the problem will diminish. However, industry officials believe that analog phones will be used in North America for a number of years, and will undoubtedly be targeted by bandits because they are inherently less secure. It is likely that the fraud problem will decrease, but it is unlikely that it will disappear altogether. Bandits are notorious at learning new techniques to defraud operators and subscribers, and will likely continue their efforts with new technologies.

The level of effort the Secret Service devotes to wireless fraud is difficult to indicate in dollar amounts. Agency officials told OTA that the Secret Service would only handle major fraud cases. Because there are technical fixes to much of the fraud activity, it appears industry will have to deal with lower level criminal activities on its own. The Secret Service sees its primary role as identifying new fraud techniques, and then working with industry (which is itself conducting an extensive antifraud program) to develop countermeasures to combat those techniques. The agency is satisfied that carriers have been cooperative in responding to suggestions by law enforcement; changes suggested by the Secret Service usually are made within three or four months.

The Secret Service and the industry agree that easy availability of scanners capable of picking up ESN/MIN pairs, and software used in altering ESNs, contributes to law enforcement's problem in policing fraud. Although *sales* of scanners are illegal[40]—other than to an employee, agent, or contractor of a cellular carrier or government employee with specific need—their *possession* is not. The FCC is formally responsible for enforcement of this provision in the law, but has few resources to do so. In fact, scanners are readily available through retail electronics stores and mail-order companies. These scanners are intended to be used for bench-testing only. They are supposed to comply with FCC rules limiting their range to 15 feet, but this limitation is easily defeated by extending the devices' antennas. Under current law, a scanner is only illegal if it is used with intent to defraud,[41] which is difficult to prove. Possession of or sale of ESN-altering software is currently not illegal. Penalties for cellular fraud include prison terms of up to 15 years, and fines up to $250,000.

Law enforcement and the industry would like to make the *unauthorized possession* of a scanner illegal, thereby closing what they consider to be a significant loophole in the current law. They would also like to make illegal the production, use, or trafficking in software used to alter ESNs. They argue that such legislation would also spread the burden of law enforcement to more agencies, enabling better enforcement.

Consumer Protection

Consumers are not well informed about cellular fraud, its frequency, its methods of perpetration or means of identifying it. Many consumers do not receive itemized bills, and have no way of verifying billing accuracy.[42] Service agreements, owners' manuals, and bills themselves usually do not warn users about the possibility of fraud. As noted above, wireless companies will generally absorb

[40] 47 U.S.C., sec. 302(a).

[41] 18 U.S.C., sec. 1029(a).

[42] Many companies charge a supplementary fee to provide itemized bills.

the cost of fraud that consumers identify. But unidentified fraud costs are borne by the user, and all fraud is reflected in higher costs to all customers. While service providers are moving steadily to combat fraud once it is found, they may not be alerting their customers to its possibility. Despite efforts to inform them, many users believe that cellular telephones are as secure as, and operate in the same manner as, traditional wireline telephones. Clearer warnings that this is not the case may be in the public's best interest.