Wireless Communications: Voice and Data Privacy

Wireless phones are very popular, and the number of people who use them is steadily growing. There are 140 million subscribers in the U.S. But even though wireless devices have many advantages, privacy is not one of them.

Depending on the kind of phone you use, others can listen to calls you make. Pagers can also be intercepted. And if your computer is connected to a wireless network ("Wi-Fi"), the data you transmit to other computers and printers might not be secure.

It pays to be aware of the privacy and fraud implications of using wireless devices. A few simple precautions will enable you to detect and prevent fraud as well as to safeguard the privacy of your communications. This guide covers:

- Cordless Phones
- Other Wireless Devices with Privacy Risks
- Cellular Phones
- Pagers and Other Messaging Devices
- Laws Regarding Wireless Eavesdropping
- Wireless Data Networks
- Resources for More Information

A word about terminology: This guide uses the terms "analog" and "digital" when describing wireless communications. Analog cellular services have been available for 25 years and are now accessible across 95% of the U.S. They send a voice through the air using a continuous radio wave. Digital services, available since 1995, convert the signal into the ones and zeros of computer code. In contrast to analog signals which are continuous, digital transmissions are sent as discrete pulses of electricity. In cell phone networks, digital coverage is rapidly catching up to analog coverage and now accounts for more than 85% of the calls made. Digital calls are generally clearer and more secure than analog.

CORDLESS TELEPHONES

Cordless phones operate like mini-radio stations. They send radio signals from the base unit to the handset and from the handset back to the base. These signals can travel as far as a mile from the phone’s location.

Can other people listen to my cordless phone conversations?
Yes, depending on the kind of phone you use. In most cases, your cordless phone conversations are probably overheard only briefly and accidentally. But there are people who make it a hobby to listen to cordless phone calls using radio scanners. These devices pick up the full range of wireless transmissions from emergency and law enforcement agencies, aircraft, mobile systems, weather reports, utilities maintenance services, among others. Signals from analog cordless phones can also be picked up by other devices including baby monitors, some walkie-talkies, and other cordless phones.

Newer digital cordless phones have better security, but cheaper or older phones have few if any security features. Anyone using a radio scanner can eavesdrop on older analog cordless phone calls, even if the phone has multiple channels.

**What privacy features should I look for in a cordless phone?**

When you shop for a new cordless phone, ask the sales clerk for an explanation of the privacy and security features. Read the product descriptions on the box, and visit the manufacturer’s web site to obtain more information.

Cordless phones that operate on the higher frequencies (900 MHz, 2.4 GHz, or 5.8 GHz pronounced "megahertz" and "gigahertz") are more secure, especially if they use digital spread spectrum technology and scramble the signal. But don’t get a false sense of security that your conversations are totally immune from monitoring. Skilled hobbyists and determined professionals can monitor just about anything.

The fact that laws prohibit eavesdropping (discussed below) is rarely a deterrent. Unless the eavesdropper reveals details of the monitored conversations to you, it’s virtually impossible to know if others are listening.

Since others can listen to cordless phone conversations, you should avoid discussing financial or other sensitive personal information. If you buy something over a cordless phone and give your credit card number and expiration date, you might end up the victim of credit card fraud.

Experts advise that the safest cordless phones operate at the higher frequency of 2.4 or 5.8 GHz. Digital models that use spread spectrum technology (SST) offer the best security. This feature breaks apart the voice signal and spreads it over several channels during transmission, making it difficult to capture. Because 2.4 and 5.8 GHz SST phones operate at higher power, they have another advantage, increased range.

Another security feature to look for is digital security codes. Both the handset and the base must have the same code in order to communicate. Look for phones that randomly assign a new digital code every time the handset is returned to the base.

Security codes do not prevent monitoring by radio scanners. But they do keep people nearby with similar handsets from attaching to your phone line to make their own calls and driving up your long distance bill. If your phone does not automatically change the security code for you after each use, remember to change it yourself. Do not use the security code set by the factory. Professional eavesdroppers know to search for those codes.

Don’t be confused into thinking that just because your cordless phone has many channels it is more secure. However, if the phone automatically changes the frequency during communications, called channel hopping, it does provide more security by making it difficult for the eavesdropper to follow the call from one channel (frequency) to the next.

Beware of so-called security features that simply distort the analog signal. They make eavesdropping difficult but not impossible.

High-tech cordless phones are more expensive. If your budget is limited and you are not able to purchase a phone with these security features, remember to use a standard wired phone for all sensitive communications, including financial transactions. Be sure both you and the person you are talking to are on standard phones.

**Special note about high-risk communications.** If you have a high-profile occupation (entertainer, politician, corporate executive, high-ranking government official), if you’re involved in a high-stakes lawsuit, if you are active in controversial political, religious, or social activities, or if you are a victim of stalking or domestic
violence, you may be a more likely target of a phone voyeur. In fact, all of your electronic communications, whether wireless or wired, could be at risk. It is beyond the scope of this guide to suggest security strategies in these situations. Professional services are available that provide advice and technical assistance on securing high-risk communications.

OTHER WIRELESS DEVICES WITH PRIVACY RISKS

Are there other gadgets or services that may be broadcasting my conversations?

Home intercom systems. Baby monitors, children's walkie-talkies and some home intercom systems may be overheard in the vicinity of the home in the same manner as cordless phones. Many operate on common radio frequencies that can be picked up by radio scanners, cordless phones, and other baby monitors nearby. If you are concerned about being overheard on one of these devices, turn it off when it is not in use. Consider purchasing a "wired" unit instead.

Speakerphones. If your standard wired phone has the speakerphone feature, be aware that some models may emit weak radio signals from the microphone even when the phone's handset is on-hook, (that is, hung-up, inactive). For short distances, a sensitive receiver may be able to pick up room noise in the vicinity of the speakerphone.

Wireless microphones. Radio scanners can intercept wireless microphones used at conferences, in churches, by entertainers, sports referees, and others. Fast-food employees at drive-through restaurants use wireless systems to transmit order information. Their communications can also be received by scanners in the vicinity. Scanners can also pick up conversations on some walkie-talkies.

Wireless cameras. Wireless videocameras have been installed in thousands of homes and businesses in recent years. The camera sends a signal to a receiver so it can be viewed on a computer or TV. These systems are advertised as home security systems, but they are far from secure. While they are inexpensive and relatively easy to install, they are also easy to monitor by voyeurs nearby who are using the same devices.

Images can be picked up as far as 300 yards from the source, depending on the strength of the signal and the sensitivity of the receiver. Before purchasing a wireless videocamera system, ask yourself if you want to be vulnerable to electronic peeping toms. Research the security features of such systems thoroughly. You might want to wait until the marketplace provides wireless video systems with stronger security features at an affordable price.

Air-to-ground phone services. Conversations on the phone services offered on commercial airlines are easily intercepted by standard radio scanners. They are a favorite target of hobbyists.

CELLULAR TELEPHONES

Cellular phones send radio signals to low-power transmitters located within "cells" that range from the size of a building to 20 miles across. As you travel from cell to cell, the signal carrying your voice is transferred to the nearest transmitter.

Can others listen to my cellular phone calls?

Yes, depending on the phone system's technical features. Cellular phone calls usually are not picked up by electronic devices such as radios and baby monitors. But analog cell phone transmissions can be received by radio scanners, particularly older model scanners and those that have been illegally altered to pick up analog cell phone communications.

With advances in digital technology, wireless voice communications are much more difficult to intercept than analog phones. The digital signal that is received by a standard radio scanner is undecipherable and sounds like the noise made by a modem or fax machine when transmitting over phone lines. Law enforcement-grade scanners can monitor digital communications, but these are expensive and generally not available on the open marketplace

Many digital phone models are dual- and even tri-mode. They enable the user to switch to analog mode
when digital services are not available. Remember that in analog mode, conversations can be monitored on standard radio scanners.

**What technical features should I look for in cell phones to protect my privacy?**

As with cordless phones, digital cell phones are more secure than analog phones by default. Phone conversations on digital phones cannot be picked up by the kinds of radio scanners used by casual hobbyists. Nonetheless, there are features you should consider regarding digital phone security.

Digital communications that are encrypted provide the highest security. Several digital technologies are available in the U.S., primarily CDMA,* TDMA,* and GSM.* But few carriers here encrypt digital transmissions, in contrast to Europe.

In the U.S., CDMA systems use spread spectrum technology (SST) to provide strong security, difficult to intercept except by law enforcement and skilled technicians. The next generation of GSM systems, 3G, will also use SST and according to experts will have strong security.

*Terminology: These abbreviations designate the technical interface used by the carrier. CDMA stands for code division multiple access. TDMA is time division multiple access. GSM means Global System for Mobile Communications. GSM is more common in Europe, but some U.S. carriers are converting to it. Two other interfaces are ESMR, or Enhanced Specialized Mobile Radio, and iDEN, which is based on TDMA.

Another term associated with digital phones is PCS, personal communications services. While "standard" digital cellular operates at 800 MHz, PCS operates at 1900 MHz. The types of services available on PCS are much the same as digital cellular. To learn more, read "How Wireless Phone Technology Works," at [www.ctia.org](http://www.ctia.org), the web site of the industry organization Cellular Telecommunications and Internet Association.

**Are there other privacy risks of cell phone use?**

Some cell phone models can be turned into microphones and used to eavesdrop on conversations in the vicinity. This is why some businesses and government agencies prohibit cell phones in areas where sensitive discussions are held.

And don’t forget (although many cell phone users do): Your side of the conversation can be heard when you talk on your cell phone in crowded public places like restaurants, airports, malls, public transportation, and busy city streets. If you don’t want others to listen to your personal conversations, be discreet and speak softly. Better yet, move out of earshot of others or save those conversations for the privacy of your home or office.

**What are the privacy implications of location-tracking features?**

By 2005 the Federal Communications Commission has mandated that the majority of wireless providers be able to locate 911 calls within about 100 feet of the originating cellular phone so that emergency services can find the callers. This feature is called E-911. ([www.fcc.gov/911/enhanced](http://www.fcc.gov/911/enhanced)) Carriers can either provide the location information that resides in the cellular network (triangulation of location based on the distance of the cell phone’s signal to nearby cellular towers), or they can rely on satellite data from global positioning system (GPS) chips embedded in the handsets of their customers.

The requirement that cell phones be embedded with location-tracking technology has spawned a new industry – location-based services such as targeted advertising. Here’s how it is expected to work. As your car approaches a freeway exit where a restaurant features your favorite food, you could receive a text message on your phone or handheld device with a special offer. Or as you walk past a coffee house, your phone could receive an ad offering you a discount on a double latte'.

While some might welcome this form of advertising, others are concerned about the privacy implications of location-based advertising. After all, in order to send you such ads, the service must know something about your interests as well as your specific location. If location records were kept over time, an in-depth profile could be compiled for both marketing and surveillance purposes.
One of the first location-based services to enter the marketplace is AT&T’s Find Friends. It enables users to pinpoint another AT&T user’s cell phone location with their permission, depending on how close that person is to the nearest cellular tower. Find Friends can also locate nearby businesses and invite another user of the service to meet there by sending them a text message. Find Friends uses a feature similar to “buddy lists,” borrowed from Internet instant messaging systems. The user invites others to be on the list and therefore to be “locatable” in order to receive text messages on their cell phones. Buddies can key instructions into the phone to become “invisible” when they do not want to be located. Other wireless carriers are expected to develop similar services.

The wireless industry is aware of consumers’ privacy concerns and has been working to develop consent-based guidelines for the development of wireless advertising. (See the Resources section at the end of this guide.) In August 2002, the Federal Communications Commission (FCC) turned down the wireless industry’s request to adopt location information privacy rules. The proposed rules were based on the privacy principles of notice, consent, security, and integrity of consumer data.

Because of the federal government’s reluctance to regulate location-based wireless services, consumers must carefully research the privacy implications of these services before subscribing. Individuals are encouraged to only subscribe to services that offer maximum user control. Not only must users be able to turn off location-tracking features, industry must ensure that the wireless devices come out of the box with location tracking turned off, with the exception of E-911 calls. Further, one’s “locatability” and the receipt of targeted ads should be subject to an “opt-in,” requiring the user’s affirmative consent.

Be sure to carefully read the privacy policy of any wireless service you are considering, usually available on the company’s web site and on product brochures. Pay attention to how the service captures and stores data, and what it says about the retention of customer and location data. To maximize privacy protection, avoid services that store location data.

Are there fraud risks involved with using a cellular telephone?

There are three types of fraud risks – cell phone "cloning," theft, and subscription fraud. Cloning has declined dramatically in recent years, while subscription fraud is increasing.

In the mid-1990s, cloning of cell phone electronic serial numbers (ESN) was rampant. Cell phone companies lost several hundred million dollars each year to cloning. The ESN is a unique serial number programmed into the cellular phone by the manufacturer. The ESN and the Mobile Identification Number (MIN) are used to identify a subscriber. One way the ESN is cloned is by capturing the ESN-MIN over the airwaves. The ESN-MIN is then reprogrammed into a computer chip of another cellular telephone. The phone calls made by the cloned phone are listed on the monthly bill of the person whose phone was cloned.

Cell phone cloning has declined significantly in recent years. The industry developed authentication features that have greatly reduced cell phone cloning, although some still occurs on systems that do not authenticate.

Theft occurs when a cellular phone is stolen and used to place calls. The charges appear on the legitimate consumer’s monthly statement. Cell phone carriers will not always remove these charges from the customer’s account. So if your phone is stolen or lost, immediately contact the cellular carrier to terminate the account. The customer may be held accountable for all charges up until the phone is reported lost or stolen.

Today, the cell phone industry is battling subscription fraud, also known as identity theft. An imposter, armed with someone else’s Social Security number, applies for cell phone service in that person’s name but the imposter’s address. As with other forms of credit-related identity theft, the imposter fails to pay the monthly phone bills and phone service is eventually cut off.

When the phone company or a debt collection company attempts to locate the debtor, it finds instead the victim who is unaware of the fraud. That person is then saddled with the long, laborious process of settling the matter with the phone company and repairing his or her credit report. The Federal Trade Commission reports that phone/utilities fraud is the second most common form of identity theft following credit fraud, half of which is wireless subscription fraud. (FTC Sentinel, [www.consumer.gov/sentinel](http://www.consumer.gov/sentinel))

What can be done to prevent cellular telephone fraud?
Early detection is crucial. Consumers usually learn about cell phone fraud when they receive their bill. When the phone has been cloned, customers typically see many (10 or more) calls they did not make. Most carriers do not charge consumers for cloned calls. If you fall victim to cloning, contact your cellular telephone provider immediately. If you are having a problem with your service provider, file a complaint with the Federal Communications Commission. See the Resources section at the end of this guide for more information.

The most effective way to prevent cloning is to get service that uses authentication. Check with the cellular phone company to find out what anti-fraud features they have. Make sure the service you select uses authentication technology to prevent cloning.

If your current phone company does not offer authentication:

- **Keep documents containing your phone's ESN in a safe place.**
- **Check your cellular phone bills thoroughly each month. Look for phone calls you did not make and report them immediately to the phone carrier.**
- **If you receive frequent wrong numbers or hang-ups, these could be an indication that your phone has been cloned. Report these to the phone carrier right away.**
- **Ask the phone carrier to eliminate overseas toll calls or North America toll calls if you do not intend to make long distance calls.**

In addition, take these precautions whether or not your carrier uses authentication:

- **Always use the phone's lock feature when you are not using the phone.**
- **Do not leave your phone unattended, or in an unattended car. If you must leave it in your vehicle, lock the phone out of sight and use the phone's lock code.**

And in all cases:

- **Report a stolen cellular telephone immediately to the cellular telephone carrier.**

Subscription fraud is another matter. Your existing cell phone is not the target of fraud as in cloning. Rather, an imposter has established a new phone account in your name, with the monthly bills sent to their address, not yours. You usually don’t find out about it until the bills are long past due and a debt collector tracks you down.

Early detection is the key to minimizing the aggravation of subscription fraud. Be sure to check your credit report at least once a year. If someone else has a cell phone in your name, you will notice an "inquiry" from the phone company on your credit report. And if the account has gone to collection, it is likely to be noted on the credit report. You will not be responsible for paying the imposter's bills, but you will need to take the necessary steps to remove the fraudulent account and/or inquiry from your credit report. California Penal Code 530.8 enables victims of subscription fraud to request documentation from the cell phone company pertaining to the fraudulent account, such as a copy of the application. (Read the PRC's Fact Sheet 17a, "Identity Theft: What to Do if It Happens to You," at www.privacyrights.org/identity.htm.)

**Are there laws that prohibit cellular telephone fraud?**

Yes. Federal law makes it a crime to knowingly and intentionally use cellular telephones that are altered, to allow unauthorized use of such services. (18 USC 1029) Penalties for violating this law include imprisonment and/or a fine. The Secret Service is the agency authorized by this law to investigate cellular phone fraud.

In California, it is a crime to intentionally avoid a telephone charge by the fraudulent use of false, altered or stolen identification. (California Penal Code 502.7) In addition, it is against the law to use a telecommunications device with the intent to avoid payment for service. Penalties include imprisonment and/or a fine. (California Penal Code 502.8)

The California Public Utilities Commission requires cellular telephone service providers to give their subscribers a notice that warns them of problems associated with fraud and provide them with information...
on ways to protect against fraud. (California Public Utilities Code 2892.3)

Subscription fraud is also a crime. The federal law is the Identity Theft and Assumption Deterrence Act (18 USC 1028). Most states have also criminalized identity theft. The Federal Trade Commission provides information about these laws and how to recover from identity theft. The FTC’s identity theft clearinghouse can be contacted at (877) IDTHEFT, and its web site is www.consumer.gov/idtheft. The Privacy Rights Clearinghouse (www.privacyrights.org) and the Identity Theft Resource Center (www.idtheftcenter.org) offer additional information.

PAGERS AND OTHER MESSAGING DEVICES

There are several types of pagers on the market: tone-only pagers (which are outmoded and rarely used any more), numeric, alphanumeric, and two-way pagers. Pagers can be either purchased or rented. The monthly fees can be significantly less than cellular or standard phone services. The costs depend on the type of pager and services the subscriber wants to receive.

Can pager communications be monitored? What about other text messaging systems?

Pager messages are not immune to monitoring. Pager networks are generally not encrypted. They transmit in the frequencies that can be monitored by radio scanners, although messages cannot be deciphered without special equipment attached to the scanner. Hackers trade tips on web sites on how to intercept pager messages. Law enforcement-grade devices are available that pick up pager communications.

The odds of your pager messages being intercepted and deciphered are probably low, especially given the cryptic nature of most messages. But individuals who engage in high-risk communications, as discussed in the cordless phone section of this guide, should take appropriate precautions.

Text messaging via cell phones and "handhelds" is much more advanced in Europe and Asia than the U.S., although it is rapidly growing here. (Handhelds are small, highly portable computer/communications devices such as personal digital assistants, or PDAs.) The jury is still out on whether or not short message services (SMS) on cell phones and other wireless devices can be intercepted. But there have been reports of the transmission of fake text messages, called "SMS spoofing."

Be sure to thoroughly research the security features of any messaging system that you use. Experts advise that you install security features on your handhelds to encrypt data that you transmit and to prevent others from accessing your data if the device is lost or stolen.

LAWS REGARDING WIRELESS EAVESDROPPING

Is it legal to intercept other people's cordless or cellular phone calls?

The Federal Communications Commission (www.fcc.gov) ruled that as of April 1994 no radio scanners may be manufactured or imported into the U.S. that can pick up frequencies used by cellular telephones, or that can be readily altered to receive such frequencies. (47 CFR Part 15.37(f)) The law rarely deters the determined eavesdropper, however.

Another federal law, the Counterfeit Access Device Law, was amended to make it illegal to use a radio scanner "knowingly and with the intent to defraud" to eavesdrop on wire or electronic communication. (18 USC 1029) Penalties for the intentional interception of cordless and cellular telephone calls range from fines to imprisonment depending on the circumstances. (18 USC 2511, 2701)

There are exceptions in electronic eavesdropping laws for law enforcement monitoring. The Communications Assistance for Law Enforcement Act of 1994 (CALEA) requires telecommunications carriers to ensure that their equipment, facilities, and services are able to comply with authorized electronic surveillance by law enforcement. (www.fcc.gov/calea) The FBI’s CALEA web site is www.askcalea.com.

Under California law it is illegal to intentionally record or maliciously intercept telephone conversations without the consent of all parties. This includes cordless and cellular calls. (California Penal Code 632.5-632.7) To violate the law, the interception of your cordless or cellular phone conversations must be done with malicious intent.
So, if your neighbor accidentally hears your cordless phone conversation on a radio scanner, it's probably not illegal. But unless the eavesdropper discloses what he or she has overheard, you have no way of knowing your conversation has been monitored. Even though an eavesdropper would be violating the law, it’s not likely that you or anyone else will detect it.

There are some exceptions to California’s all-party consent law. A judge can authorize the interception of an electronic cellular telephone communication in investigations involving specified crimes. (California Penal Code 629.50-629.98) California Penal Code section 633.5 states that if someone is threatening another person with extortion, kidnapping, bribery, or any other felony involving violence, the calls may be recorded by the person being threatened. Under special limited circumstances, phone company employees may monitor calls.


Are there laws related to the privacy of pagers?

Federal law prohibits anyone from intercepting messages sent to display pagers (numeric and alphanumeric) and to tone-and-voice pagers. Tone-only pagers are exempt from this provision. (Electronic Communications Privacy Act, 18 USC 2510)

Law enforcement must obtain a court order in order intercept your display or tone-and-voice pager. But under the USA PATRIOT Act, enacted in 2001 following the September 11 terrorist attacks, the standards for obtaining court ordered warrants have been loosened.

In California, a judge can authorize the interception of an electronic digital pager by law enforcement in investigations involving certain specified offenses. (California Penal Code 629.50)

Can telemarketers contact wireless phones, pagers, and other text devices?

Under the federal Telephone Consumer Protection Act, it is against the law to use autodialers or prerecorded messages to call numbers assigned to pagers, cellular or other radio common carrier services except in emergencies or when the person called has previously given their consent. (47 USC 227)

But the law fails to specifically prohibit "live" telemarketing calls to cell phones. Telemarketers claim they do not target cell phones with solicitations, but it can happen, especially if a wireline phone number is inadvertently assigned to a cell phone. Aside from the privacy and annoyance factors of receiving junk calls on cell phones, there is the further aggravation of having to pay for those calls. (Cell phone users generally pay for both the outgoing and incoming calls.) The Direct Marketing Association's wireless guidelines instruct DMA members to refrain from knowingly calling a phone number for which the called party must pay the charges, unless the recipient has given consent. (www.thedma.org/library/guidelines/wirelessmarketing.shtml)

As wireless text messaging systems become more widespread, it is only a matter of time before "spam" -- unsolicited electronic bulk advertising -- becomes a problem for wireless consumers. A bill introduced in Congress in 2001, the Wireless Telephone Spam Protection Act (H.R. 113), would make it illegal to transmit unsolicited ads to wireless devices, including cell phones, pagers, and PDAs enabled to receive wireless e-mail.

A new law in California, effective 2003, prohibits the transmission of text message advertisement to cellular phones or pagers equipped with short message capability. The law has exceptions if the company has an existing relationship with the subscriber or if it gives customers the option to not receive text messages. (California Business and Professions Code 17538.41)

WIRELESS DATA NETWORKS

An increasing number of households and businesses are establishing wireless networks to link multiple
computers, printers, and other devices. A wireless network offers the significant advantage of enabling you to build a computer network without stringing wires. Unfortunately, these systems usually come out of the box with the security features turned off. This makes the network easy to set up, but also easy to break into. Most wireless networks use the 802.11 protocol, also known as Wi-Fi.

What are the security risks of using wireless data networks?

Wireless networks have spawned a new past-time among hobbyists and corporate spies called war-driving. The data voyeur drives around a neighborhood or office district using a laptop and free software to locate unsecured wireless networks in the vicinity, usually within 100 yards of the source. The laptop captures the data that is transmitted to and from the network’s computers and printers. The data could include anything from one’s household finances to business secrets.

Wireless network units are equipped with many security options, but the typical automated installation process disables these features to simplify the installation. Not only can data be stolen, altered, or destroyed, but programs and even extra computers can be added to the unsecured network without your knowledge. This risk is highest in densely populated neighborhoods and office building complexes.

Remember, wireless data networks are in their infancy. To ensure that your system is secure, review your user’s manuals and web resources for information on security. The Home PC Firewall Guide provides access to independent, third-party reviews of Internet security products, including wireless computer networks and PDAs, on the web at www.firewallguide.com/index.htm. Two useful guides can be found on the web at www.practicallynetworked.com/support/wireless_secure.htm and at www.csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.

RESOURCES FOR MORE INFORMATION

Contact the Federal Communications Commission to file complaints about wireless phone services. Its web site provides guides on wireless services as well as information on laws and regulations:

- Federal Communications Commission
  Consumer and Governmental Affairs Bureau, Consumer Complaints
  445 12th Street, S.W.
  Washington, D.C. 20554

Phone: (888) 225-5322

E-mail: fccinfo@fcc.gov

Web: www.fcc.gov

- Read the FCC’s guide, "What You Should Know about Wireless Phone Services" at www.fcc.gov/cgb/wirelessphone.pdf


Your state’s public utilities commission may also oversee wireless providers and enable you to submit complaints. To find the contact information for your state’s utilities commission, consult The Consumer Action Handbook, available free from the Federal Consumer Information Center by phone at (888) 878-3256, and on the Internet at www.pueblo.gsa.gov/crb/utility.htm. The California Public Utilities Commission consumer complaint number is (800) 649-7570. It provides an online complaint form at www.cpuc.ca.gov.

The Wireless Consumers Alliance is a nonprofit consumer advocacy organization. Its web site provides a "what to know" section, as well as information on health and safety concerns, consumer rights, and legal and regulatory actions.

- Web: www.wirelessconsumers.org
- E-mail: mail@wirelessconsumers.org
The **industry association CTIA** provides information about the wireless industry, including the latest usage statistics.

- **Cellular Telecommunications and Internet Association**
  
  1250 Connecticut Avenue, N.W., Ste. 800  
  Washington, D.C. 20036  
  Phone: (202) 785-0081  

  Web: [www.wow-com.com](http://www.wow-com.com)

- Read "How Wireless Technology Works,”  

A **guide on security** by the Defense Personnel Security Research Center provides useful tips on wireless security and privacy for employees as well as consumers. It is available on the Texas A&M University website.

- "Employees' Guide to Security Responsibilities"
  
  [http://rf-web.tamu.edu/security/SECGUIDE/Home.htm](http://rf-web.tamu.edu/security/SECGUIDE/Home.htm)

To follow developments in the debate on wireless **location tracking services**, visit these industry sites:

- Mobile Marketing Association, [www.mmaglobal.com](http://www.mmaglobal.com)

- Wireless Location Industry Association, [www.wliaonline.com](http://www.wliaonline.com)

Location Interoperability Forum, [www.openmobilealliance.org](http://www.openmobilealliance.org)

The **AARP**'s website provides consumer information on wireless phones:


- "Understanding Consumer Use of Wireless Telephone Service,"  
  [http://research.aarp.org/consume/d17328_wireless.html](http://research.aarp.org/consume/d17328_wireless.html)

**Consumers Union**'s Wireless Watchdog website on wireless phones covers shopping, safety, service, and advocacy, [www.consumersunion.org/wireless](http://www.consumersunion.org/wireless).

You can read the texts of the laws and regulations cited in this guide at these sites:

- Federal laws: [www.law.cornell.edu/uscode](http://www.law.cornell.edu/uscode)
- California statutes: [www.leginfo.ca.gov/calaw.html](http://www.leginfo.ca.gov/calaw.html)

**Note:** Several commercial products and features are named in this guide. No endorsements are implied.