Section

2

Surveillance Technologies

Acoustic

2 - Audio
3 - Infra/Ultrasound
4 - Sonar

2

Acoustic Surveillance

Audio

1. Introduction

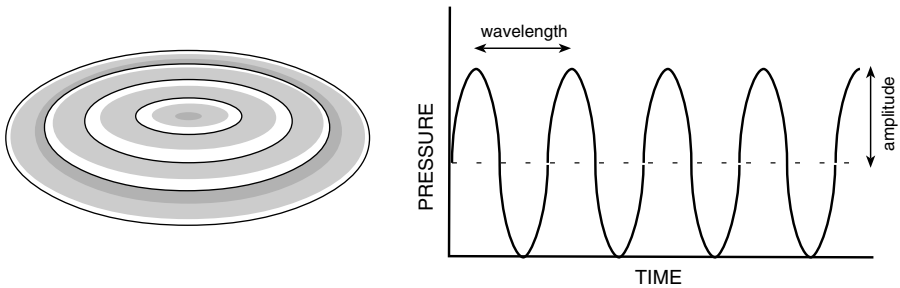
Acoustic surveillance is a broad category that includes sounds within human hearing and sounds outside of human hearing. For this reason, acoustic surveillance has been divided into sections. The two main subdivisions are Audio Surveillance, which primarily focuses on technologies that are *within human hearing ranges*, and Infra/Ultrasonic Surveillance, which focuses primarily on technologies that are *outside of human hearing ranges*. The third is a specialized section that concentrates on sonar, which includes both infrasonic and audio frequencies. Audio surveillance is conducted over both wired and wireless systems. While wireless systems are discussed in this chapter in a general sense, the main focus is on wired systems. This is because many wireless audio communications are converted into radio-wave frequencies before transmission and are discussed in greater detail in the Radio Surveillance chapter.

Encryption and acoustic surveillance are closely related, since encryption is one of the principal ways in which the privacy of communications is safeguarded. For this reason, acoustic surveillance, computer encryption, and cryptology share a common history in many respects. It's a good idea to cross-reference the Cryptologic Surveillance and Computer Surveillance chapters for more of the background related to encryption and secure audio communications.

Anson Stager was a telegraph expert during the Civil War. He had a unique way of intercepting telegraph communications that is described later in this chapter. [Library of Congress, copyright expired by date.]

The Phenomenon of Sound

To understand acoustic surveillance, it's helpful to have a short introduction to sound waves. Waves are periodic disturbances that occur in bathtubs, pools, oil slicks, wheat fields, forests, and large bodies of water. They even occur in walls, mountains, and chunks of metal. If you've put your ear to the ground, or to a wall in a building, you've probably noticed that you can hear distant sounds through these media better than you can hear them through the air.



Left: While it's not a perfect analogy, the ripples in a pond that result from throwing in a pebble are often used to help people visualize how sound waves propagate in a medium. Imagine, however, that the sound waves travel outward from the source in all directions where there is a medium (not just along the surface of the water, but down and out, as well, and through the surrounding air, where they can't be seen. Sound travels at different speeds in different media, depending on the density of the media; since water is denser than air, sound travels faster through water. Sound travels slower than light, an electromagnetic phenomenon, which is why we usually see lightening before we hear the thunder, especially if the storm is far away. Right: It is common to symbolically express sound as repeating sinusoidal waves. In this simple graph, the amplitude ('height') of the wave is represented in the Y axis and the length of the wave is represented in the X axis (and repeats over time).

When waves move through a medium, we say that they *propagate*. There are two common ways in which wave phenomena move through various gaseous or solid objects. There is actual movement *through* the medium (as radio waves penetrate through a wall) or there is a force *influencing* the medium that is intrinsically associated with the medium (as water is disturbed when a pebble penetrates its surface). There is an important distinction between these two types of wave phenomena:

- The first type of movement is similar to a small bird passing through the big holes in a chicken wire fence. Electromagnetic phenomena like radio waves can pass through a wall in somewhat the same way a small bird can pass through a wire fence.
- The second type of movement is like rapping on the wall, which has elastic properties, causing the sound to *propagate* longitudinally, using the wall as a medium. Pressure waves are built up in the wall as it responds to the energy, alternately compressing and decompressing. If the wall weren't there, there would be no waves.

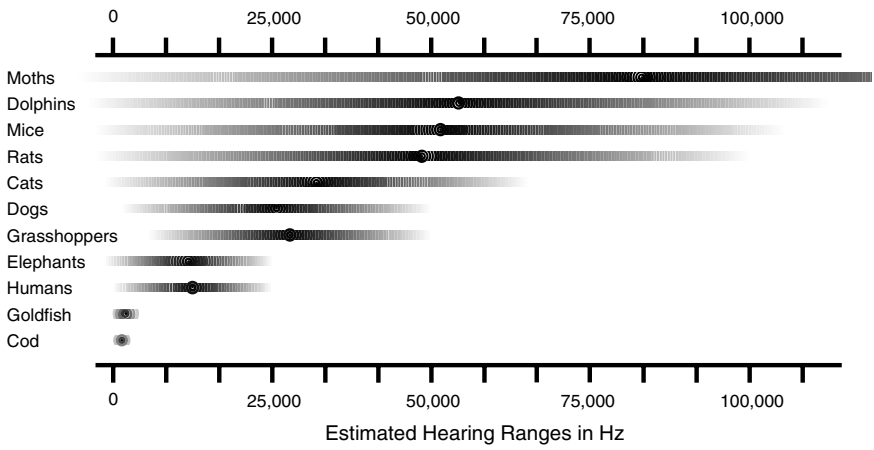
We have senses specialized to respond to the phenomenon of sound. If you put your ear on a wall that is being rapped, the disturbance causes your ear drums to vibrate, behind which small bones in your skull carry the vibrations to your nervous system. The nerve impulses are then interpreted by your brain as a swishing sound. This is the phenomenon of hearing. In fact, having two ears set a little distance apart gives us even more information. By slightly turning our heads and 'measuring' the relative loudness of the sound and the slight time delay in reaching each of our ears, we can determine the direction from which the noise is coming.

Human hearing

Audio surveillance is designed to enhance our sense of hearing, or to enhance other forms of stimuli and convert them to within our hearing range.

Sound waves stimulate the cilia and tiny bones in our ears and our brains interpret the type of sound, its intensity, and characteristics in such a way that we can determine its source and direction. Sound waves can also stimulate vibrations in various minerals and can be amplified or converted into energy or frequencies that our ears can hear through electronic devices.

Human hearing is quite limited. We may be superior in terms of abstract thinking abilities, but we fall far short of many other creatures in terms of our sight, hearing, and ability to detect infrared, ultraviolet, or magnetic disturbances.



Insects, rodents, and cetaceans (e.g., dolphins) apparently hear far wider ranges of sounds than humans. Cats and dogs are more similar to us, but even they can hear high-pitched sounds that are above our range of hearing. Humans are most sensitive to communications within about 1,000 to 4,000 Hz, which also correspond to the frequencies of human speech. Thus, most communications devices are designed to be clear and sensitive within these ranges. Surveillance devices, on the other hand, often utilize frequencies above and below human hearing and some are even patterned after the hearing capabilities of other animals.

Most children with normal hearing can hear frequencies from about 18 to 20,000 Hz. As humans age, or are subjected to various environmental stresses (illnesses, sudden loud noises, constant loud noises, or constant low-level noises), the sensitive mechanisms that allow us to hear are gradually damaged and both the sensitivity of our hearing and the frequency range gradually decreases. Adults typically hear frequencies of about 25 to 17,000 Hz and hearing may become impaired as we age.

Sound Surveillance

Almost all remote-sensing technologies involve *waves,* or phenomena that appear to behave like particles or waves, depending on how you study them, and since we can't see most of them, we resort to symbolic representations to measure and describe them. Since this volume focuses on the conceptual understanding and applications of surveillance technologies rather than on physics and engineering design, waves will be described with examples and a few basic diagrams rather than with mathematics. The Resources section lists more advanced texts that delve into the physics and math for those who want to better understand the physical theories related to sound.

The Character of Sound

Because sound is movement through a medium, it does not propagate in a vacuum. This characteristic seems to have inspired a lot of philosophical thought about whether sound even exists in our absence. If we momentarily borrow a concept from eastern thought, we can see how western thinking about sound sometimes has a Zen *koan*-like flavor. A *koan* is a statement or question intended to stimulate intuitive enlightenment. Koans typically seem paradoxical in the context of what we call 'reason.' They are to be 'understood' in a way that is different from the way in which we normally understand things through scientific investigation.* Common questions about sound with a koan-like flavor include "What is the sound of one hand clapping?" and "If a tree falls in the woods and no one is there to hear it, does it make a sound?" The Zen aspect of koans is outside the scope of this book (and perhaps any book), but these questions about sound are useful from a teaching perspective because they help stimulate inquiry into the characteristics of sound.

This text doesn't delve into the philosophical aspects of sounds, but from a physics point of view, the above questions help illustrate some of the basic terms and concepts associated with sound. The two characteristics of sound that are most relevant to surveillance are *frequency* and *volume*. Frequency is perceived by us as the *pitch* of the sound (the 'highness' or 'lowness' of the note) and volume, the *loudness* of the sound. The sound of one hand clapping is considered to be *infrasonic*, a frequency *below* the range of human hearing (though elephants might be able to sense it). One hand clapping is also considered to be *subaudible*, that is, a volume below which we are sensitive. For surveillance purposes, specialized instruments can be designed to pick up a low, soft sound and translate its frequency and volume into levels that we can perceive. Thus, if the sound of one hand clapping were both *amplified* and raised in *frequency*, we might hear a soft, rhythmic swishing from the disturbance of the air as the hand moves back and forth. These types of sound-processing techniques are useful in many aspects of audio surveillance.

Sound is not electromagnetic energy, but it has a lot of properties in common with electromagnetic technologies. If you place two tuning forks close together and hit one so that it vibrates, the other will begin to vibrate as well (though not as vigorously). This is called *resonance*. Resonance is a type of energy transfer. When objects are close together, they are more likely to resonate in response to those around them. Resonance is particularly noticeable if the objects are made of materials with good vibratory qualities. Tuning forks, guitar strings, and the surfaces of speakers are designed with materials known to resonate well at certain frequencies. Television antennas are designed with a particular shape and length so they resonate well in response to electromagnetic radio waves.

As with one hand clapping, sometimes a sound is not loud enough to be heard with the unaided ear. A guitar string that is not attached to the guitar can be stretched and plucked, but creates a soft, dead sound that isn't very appealing. When placed on an acoustic guitar, the vibrating string transfers energy to the air inside the guitar which bounces the sound around, giving it a warm, bright sound. The vibration (resonance) of the air around the string and in the wood itself aids in transfering sound from the string to the air inside the guitar, causing a melodious vibration we perceive as music. But what about an electric guitar? It doesn't have a sound box. There's no cavity inside to amplify the sound and no sound hole to direct the

*Tim Burton's movie "The Nightmare Before Christmas" gives a delightful illustration of the limitations of scientific reductionism when Jack Skellington systematically destroys a Christmas bauble in order to try to discern its nature.

sound. In an electric guitar, the amplification is accomplished by transfering the sound via a 'pickup' attached to the body of the guitar. As the strings vibrate, the body vibrates and the pickup converts this to electrical energy that is transfered through a cord to an amplifier and speaker system. Electronic amplification can be substantial, which is why rock stars prefer to use electric instruments rather than acoustic instruments in large amphitheaters.

Sound Conversion and Display

Sometimes sounds (or other inputs like radar or computer data) are converted to other forms of energy so they can be 'heard' without creating noise or so that they can be analyzed in some other way. Some devices have a blinking light to indicate the pattern or frequency of a sound or input from other sources. Most computer dialup modems have a programmable *sound on* mode that allows you to listen to the flow of data over the line. This can help diagnose problems, but the sound is also annoying; it's a rough, screechy sound and most of the time the modem speaker will be set to 'off' with blinking lights indicating the flow of data instead. Similarly, most consumer radar detectors will indicate the presence of a radar signal by beeping, but this can be distracting if a conversation is going on in the car, so some models allow the sound to be turned off and will display blinking lights instead. This conversion of energy into different forms allows us to monitor data in whatever form is appropriate for a task. Audible sounds can be converted to other forms, and other forms of energy can be converted to audible sounds, as these brief examples illustrate:

- The stress levels in a human voice can be converted into a graph to indicate whether a person is nervous and possibly lying.
- Infrasound monitors, which detect sounds below the range of human hearing, can be electronically enhanced to convert the data into graphs or the sound itself can be raised in pitch and amplified to bring it into audio frequencies and levels that can be interpreted by humans. Infrasound is used in the surveillance of explosives detonations and the prediction of natural disasters or severe storms.
- In broadcasting, audible sounds are converted into radio signals to allow them to be transmitted without wires, and then converted back in order to be understood when they have been received. Radio and television are the most common examples, although satellite voice broadcasts are now becoming common.

Sound and the various electromagnetic technologies that are covered in subsequent chapters are important because together they comprise the great majority of surveillance devices. Seven chapters in this book are collectively devoted to sound and electromagnetic technologies and it will be seen that they have many aspects in common. But despite their similar features, sound vibrations and electromagnetic radiation are not the same physical processes.

Remember that sound requires a medium through which to direct energy. In fact, it could be said that sound *is* energy directed through a medium. In contrast, electromagnetic phenomena (like light) are energy with both wave- and particle-like properties which propagate *with or without a medium,* thus allowing electromagnetic energy to travel through a vacuum.

This chapter provides some background information on the nature of sound and then describes surveillance technologies that take advantage of the properties of sound within the human hearing range. It includes a range of audio technologies, primarily listening and recording devices, since they are inexpensive and widely used in many types of surveillance.

2. Types and Variations

While there are many technologies to surveil the Earth, its structures, weather, wildlife, and its surrounding atmospheric envelope, the majority of surveillance is directed at monitoring human activities including travel, agriculture, construction, politics, and communications. People are especially intent on surveilling other people's conversations, trying to discern their intentions and planned activities.

Many conversations occur in noisy or private settings, out of earshot of covert listeners (restaurants, bars, boats, private golf courses), yet a tremendous amount of human intelligence is still gathered from monitoring conversations that *can* be amplified or overheard. Consequently, much of this chapter focuses on telephone tapping and various types of remote listening systems.

In addition to face-to-face conversations, common means of audio communications include traditional telephones, digital voice technologies (including videoconferencing and Internet phone systems), cell phones and other wireless phones, voice pagers, radios, and telegraph-sounding keys. Sometimes security measures are taken to safeguard or disrupt audio communications including voice changing, voice scrambling, encryption, or jamming. (Wireless communications are covered more fully in the Radio Surveillance chapter and electronic communications such as email and Internet discussion groups are introduced in the Computer Surveillance chapter.)

The main categories of audio surveillance include

audio amplification/reduction - making a sound louder/softer so that it can more easily be detected, recognized, heard, or understood

audio filtering - separating out particular aspects of a sound, which most commonly involves filtering out noise or other forms of interference, but may also include filtering out particular voices or frequencies

audio location - detecting the location, origin, or direction from which the sound is coming

audio recognition - determining the source, type, or speaker of a sound

audio translation - converting a sound from one form to another, such as making the frequency higher or lower or translating human speech from one language to another

audio listening - eavesdropping on sounds, which may or may not include recording the sounds

audio logging - creating a record of administrative aspects of a sound including time of day, duration, frequency, etc.

audio recording - creating a replayable record of a sound in analog or digital format (or a hybrid format)

audio processing - analyzing a sound for a variety of characteristics including direction, origin, source, veracity, content, and sometimes even specific voices

Logging, *listening*, and *recording* have traditionally been the most common categories of audio surveillance. However, *audio processing* is increasing in prevalence because it can now be done with computer hardware/software that wasn't previously available.

Audio surveillance devices can also be subdivided into wired and wireless varieties, each

with advantages and disadvantages:

wired *Wired devices are those which are physically connected through a solid medium to a speaker or recording device.* The connection is typically through common copper electrical wire, though it may also be through cable and fiber optic media. Wired listening devices are more difficult to use in covert operations because it is necessary to physically enter the premises for a period of time to install and hide the wire, which in some circumstances may be impossible. Wired bugs are not too difficult to detect, especially when they are in use. Activity on electrical wires can be found by current that 'leaks' through the insulation into the immediate surrounding area, while fiber optic is based on the transmission of light and doesn't create the same type of electrical emanation. Depending on the medium and the wire gauge (smaller wires are easier to hide), there may be limits to the effective length of the wire and the strength of the signal.

Fiber-optic cables provide greater security than wired connections, but they also require greater precision, as the end-couplings must be carefully spliced so as not to introduce kinks into the optical fiber, which would disrupt the travel of the light beam. Some installations use a wired connection that leads to a wireless connection elsewhere in a complex (the roof or a closet or wall) or vice versa.

wireless *Wireless devices are those which use air or water as the physical medium through which the sound travels* (remember that sound can't travel in a vacuum, so it can't be sent out into empty space unless it is first converted to another type of energy). With improvements in radio-frequency transmission technologies, wireless devices are increasing in prevalence.

Because it is not necessary to hide any wires, wireless transmitters are often favored for small hidden 'bugs.' The main disadvantage to wireless listening devices is that the transmission can be picked up by anyone in the vicinity with a receiver that can scan or tune to the transmitted frequency. Thus, they may be easy to detect when they are in operation and someone may be eavesdropping on the eavesdropper.

Another disadvantage to wireless listening devices is strict regulations about frequencies and ranges. If they have a range of more than 300 or 1,000 feet, they are typically subject to regulatory licenses and broadcast restrictions. Wireless communications are sometimes transmitted to a wired receiver which works as a relay station to further transmit the signal over a longer distance.

An understanding of the difference between analog and digital communications is important when choosing audio technologies. Communications used to be almost entirely analog, but now digital communications, which have some unique strengths, are being favored for more secure communications.

analog *Analog audio signals are those which are output as a continuous function.* The most common example used to describe an analog system is a clock with minute and hour hands that move smoothly through a 360° arc. As the hands sweep around the dial, *they pass through every point in the path of the arc*. Another example is an older dial radio in which AM stations are tuned by slowly moving the dial until the desired station comes in clearly. Old radios, clocks, tape recorders, and phones were based almost exclusively on analog technologies. By the 1980s, this was beginning to change.

digital *Digital transmissions are those which are output as discrete signals* such as high or low, on or off, in or out, etc. The common example of a digital display is a digital clock which, instead of sweeping through every second of the hour, 'jumps' from one second to the next, or one minute to the next without displaying intermediary moments of time. Another example is a pushbutton radio in which each button on the tuner 'snaps into' a specific frequency without scanning through individual stations as on older AM radios. (Besides the pushbutton concept, FM is used as an example because there are wide 'guard' frequencies around each broadcast frequency to guard against interference from nearby station frequencies and so is more illustrative of an 'on/off' system than AM broadcasts, which can overlap.) Many newer computerized electronics (including computers themselves) are based on digital logic and digital technologies. Digital devices provide two important advantages over analog devices:

replication Digital data can be perfectly replicated without degradation of the information. Data tend to degrade each time they are copied through an analog system. For example, a tape recording of a tape recording is never quite as perfect as the original. A photocopy of a photocopy of a photocopy gives a good illustration of how an image or signal loses information each time it is replicated. However, copying a computer software program from one computer to another, or a digital recording from one digital system to another or a digital CD from one CD to another makes a 'perfect' copy in the sense that the subsequent number of 'bits' equals the original number of 'bits' in quantity and content.

encryption Digital data are relatively easy to manipulate. You can move the bits around. You can change them into other bits to provide encryption, compression, or data processing. You can control them with computer electronics. Spread-spectrum technologies provide a means to 'hide' radio signals from eavesdroppers and encryption techniques make it difficult for eavesdroppers to interpret a signal even if they are able to capture it.

Eavesdropping and wiretapping of phone conversations appear to be exceedingly prevalent in business communications. Wiretapping and recording mechanisms are factory-built into some types of business phones. Telemarketing firms routinely monitor their employees' calls and many technical support lines are 'monitored for quality assurance' which means that either the supervisor listens in from time to time or the calls are recorded for later evaluation. The more common categories of devices used for monitoring purposes are listed here. Devices are further described in the *Description* and *Applications* sections.

pen register This was originally a device for analyzing *pulses* in a phone line to determine which number had been dialed. Since pulse phones are now rare, the phrase has come to mean a range of mechanical and electronic products that determine and display the number dialed, whether it is a pulse or tone signal. Pen registers may optionally be able to record the number for later review. Even more recently, the phrase has subtly changed to encompass numbers that have been dialed or 'otherwise initiated' since there are now autodialers and other electronic means of placing a call.

Pure pen registers are becoming less common. The trend in electronics is to bundle many features into one device. In other words, a device promoted as a 'pen register' might include other capabilities to log the time, frequency, and duration of a call. It is important, from a legal point of view, to define 'pen register' in its purest sense (of simply capturing/recording outgoing numbers), since there are laws governing who

may use them and when they may be used. If the name 'pen register' comes to encompass other features, then laws are 'changed' without due process. Thus, a value-added pen register should be considered a 'pen register and logging device,' for example, to keep the legal distinctions clear. The logging aspect and guidelines for its use should be stipulated separately.

The proper interpretation of the name 'pen register' does not encompass call *content* or other *characteristics* of the call (e.g., attributes such as voice recognition or stress levels). Combination pen registers/loggers are often used for cost-accounting by businesses that bill calls to specific departments or budgets. The more limited pen registers are used in authorized law enforcement wiretaps. Unfortunately, pen registers don't capture just a number dialed. They can also capture PINs, credit card numbers, and other confidential information that is dialed in conjunction with the number.

scanning In terms of wired phone connections, this is the act of automatically dialing a series, range, or pattern of numbers in order to make a connection or determine characteristics of the line. A 'war dialer' is a type of scanner. It is an automatic-dialing device used by many telemarketing firms (sometimes illegally). War dialers have become more sophisticated. In the early days, a war dialer was simply programmed to dial numbers sequentially, one after the other. Now they can be hooked into electronic computer directories to dial specific names or people with particular personal profiles. Computer hackers sometimes scan numbers to see if a modem or fax tone responds to the call.* This is one way of seeking unauthorized access to computer systems or finding unpublished fax numbers that might provide document-delivery systems for employee or product information. Phreakers (phone hackers) sometimes scan for anomalies that might indicate special maintenance numbers or access points for long-distance calls or other services. (Scanning has a broader meaning in wireless communications which is described further in the Radio Surveillance chapter.)

tapping This is covert or clandestine access to or interception of a call. If you hook in an extension line, a specialized wiretapping device, a lineworker's set, a computer, or other device that is directly or closely associated with the physical line or the radio frequency, it is considered to be *tapping*. If you listen through some device not directly associated with the line or frequency, e.g., a microphone hidden in a wall near a phone, it's considered to be *bugging*. The listener may be a person or a recording device, or both. The euphemism 'monitoring' is sometimes used to mean overt or clandestine tapping of a call, as in certain business applications.

trapping This is the application of technology to 'seize' a call so the caller can't terminate the connection. In other words, someone places a call from a phone booth to a bookie several miles away. The call is 'trapped' so that the line remains active to allow it to be traced to its origin. The caller is unable to hang up the call, even by putting the headset in the cradle. This allows the time needed to locate the origin of the call. Trapping is often used in conjunction with tracing, so often in fact that in law enforcement it's called *trap-and-trace*, *lock-and-trace,* or *lockin-trace.*

tracing This is the process of determining the communications route of a call or points along that route. *Origin-tracing* is the determining source of the call. *Route-tracing* is determining the path through which the call is connected. *Terminal-tracing* is determining the points at which the call enters or leaves a network node or station.

*The feature film "War Games" depicts a young hacker, played by Matthew Broderick, who uses various techniques to try to locate dialup modems so he can break into restricted systems.

A form of tracing is used by some 911 emergency systems to determine the origin of a call in case a frightened caller hangs up or experiences a medical emergency and is unable to provide an address. The term 'tracing' does not encompass the content, frequency, duration, or character of the call. In television programming, tracing is often depicted in kidnapping and ransom scenarios.

Traditional tracing occurs when a call is 'live,' but with computerized logs and playback systems, tracing 'after the fact' is becoming easier all the time. The simplest means of low-tech tracing for long-distance calls is to look at a person's phone bill. The next simplest means is to access common carrier records that log both local and long-distance calls for billing purposes. The live tracing of cell phone calls can be done by triangulation, i.e., the comparison of signal strengths between several cell transceiver nodes. New cell phones equipped with Global Positioning System (GPS) capabilities now allow more precise tracing.

Caller ID Caller ID is a form of tracing. It is a pay service offered by telephone carriers which 'broadcasts' the number of the person calling to the person being called. By paying a monthly fee, the caller's number can be accessed from the line and displayed on a Caller ID-compatible device. Many answering machines and telephones now have Caller ID displays, but it is still necessary to pay for the service to get the number.

Call Blocking is a series of numbers that can be dialed to block Caller ID so the person being called doesn't know who is calling. Call Blocking is free. There was a lot of debate, when Caller ID was first introduced, about whether the caller or the callee should pay for Caller ID-related service.

From a public safety point of view, the person using Call Blocking should be charged and Caller ID should be free. This is analogous to a person freely looking through a peephole in the door to see a stranger before letting the stranger into his or her house. Unfortunately, the phone service was implemented the other way around, analogous to a stranger freely wearing a mask at the door and the home-owner having to pay a fee to see the stranger through his peephole. Communications carriers probably prefer the current system for economic rather than safety reasons.

common carrier These are communications service providers, including local exchange carriers (LECs), competitive-access providers (CAPs), cellular carriers, interexchange carriers, and providers of PCS and other mobile radio services. It further includes those cable and utility companies that provide telecommunications services. The concept of the common carrier is very important because law enforcement agencies have been lobbying Congress for legislation that requires common carriers to adapt their circuitry so that law enforcement agents can wiretap the lines.

3. Context

Because eavesdropping has been around for a long time, society has had time to debate many aspects of the practice and build a social framework around the legality of eavesdropping and its cousin wiretapping.

The contexts in which audio surveillance are most commonly used include

sound monitoring in the field, home, or workplace Listening devices are used to record the sounds of birds and whales, to monitor an infant crying or children playing in a daycare facility. It is used in hospitals to check on the needs of bedridden patients and on hiking trips to link partners or team members. It is also used in industrial

yards to monitor safety around industrial equipment and in labs to check on employees working around hazardous chemicals or radiation. Many P.A. systems have a monitoring mode.

eavesdropping Audio surveillance of other people's conversations is common and some of it is illegal. It tends to occur in the context of relationship difficulties or business spying.

wiretapping Court-authorized audio surveillance of conversations is primarily used by law enforcement agencies to investigate and convict cases related to violent crimes and drug trafficking.

mobile listening/recording Gray area surveillance (an activity of questionable legality) is sometimes used to safeguard personal privacy. Hidden mobile microphones and transmitting or recording devices are sometimes used for the purpose of monitoring or saving the information and characteristics of a personal communication. This is called *wearing a wire*. An individual who has been granted a restraining order against a stalker or ex-spouse might wear a wire to alert others of violations of the restraining order or to gather evidence of those violations. Investigative journalists will often wear wires when seeking access to individuals or establishments that may be involved in alleged criminal activities, to record their responses and reactions. Employees and potential employees will sometimes wear a wire to record incidences of discrimination, sexual harassment, or workplace abuse.

Sound-Monitoring Devices

A listening device is any device which is designed to channel, focus, or amplify sounds to aid the listener in better recognizing the characteristics or content of the sounds. Sound tends to travel faster and more readily through solid objects than through air (try putting your ear to a wall or to the ground). Sound travels nearly five times as fast through water as it does through air. Thus, the context in which listening devices are used is important, as they depend not only on electronics design, but on their careful placement and alignment. For example, laser listening devices are precision instruments, requiring a steady base and the correct angles. If you don't have a solid, steady surface and a tripod for mounting the device, they're apt to record noise or unusable sounds.

Listening devices are generally designed to amplify a signal or to make it clearer (to remove static, noise, other voices, etc.). Amplification systems have been around for a long time; a stethoscope or glass can be placed against a wall, a parabolic dish can focus and thus amplify the sound from across a street, or an electronic amplifier can be embedded in a plant. These are all ways in which sounds are made louder and easier to understand.

Technologies for clarifying sound are more recent. Computer technology now makes it possible to analyze a signal and single out a particular voice, or to test it for stress levels that might be related to the truth of the information, or to fuse the tones from one 'frame' or moment in time to the next to algorithmically 'guess' at the content of a poor or faint recording. It is also possible to use computer technology to translate a conversation that is being carried out in a foreign language. Even if the translation isn't perfect, the context may be sufficient to make an educated assessment of the communication.

Tapping Devices

In most cases, phone tapping involves the installation of a device in close association with the phone being tapped. This is especially true now that electronic technologies make it harder to de-encrypt or intercept a call en route. Thus, tapping a phone usually involves gaining

access to the premises, either inside or outside, depending on the type of tapping equipment and the configuration of the phone equipment. However, there are still circumstances where a call is tapped en route, usually at the premises of a local common carrier. Authorized law enforcement taps are usually done this way.

Single-line phones are the easiest to tap, and extension lines are not especially difficult. A tap can be set up on a specific line, or on all extension phones attached to that line, depending upon the placement of the tap on the circuit. Multiline phone systems are harder to tap, and phone-bugging devices for multiline systems such as private branch exchanges (PBXs) are harder to obtain and usually more expensive.

Society has become more mobile and so the demand for mobile communications continues to increase. Wireless phone conversations used to be relatively easy to access, when a single frequency was used, but spread-spectrum technologies are being built into consumer phones, making it much more difficult to access and decrypt a wireless conversation.

Because phone tapping is typically covert, most phone tap equipment is small, and thus portable, frequently no larger than a pocket pager, and sometimes as small as a matchbox or button, depending on its capabilities.

Wireline tapping devices are usually installed in buildings or on junction boxes or lines near the premises being tapped. They may also be installed on the local phone company premises, but these taps are in the minority. Portable or stationary recorders may be used in land vehicles, marine craft, or aircraft. Mobile recorders may be attached to moving conveyances or worn on the body.

4. Origins and Evolution

The history of audio surveillance involves four major aspects, the understanding of the science of sound, the evolution of technologies to project sound over distance, the evolution of devices to record sound, and laws to regulate the use of these technologies. Much of the current legislation regarding communications, recording, and wiretapping has its roots deep in the 19th century. (The aspects of audio surveillance that apply to wireless communications are described further in the chapter on Radio Surveillance.)

Humans have been recording events for at least 20,000 years, through images and later through text, but the recording of sound is a surprisingly recent event. Both sounds and images are now frequently recorded together on the same medium.

The first visual recording devices were fingers and sticks, used by humans to draw images in dirt or sand. Later, the use of chisels, charcoal, and pigments provided a way to create a more permanent record, preserved for hundreds of thousands of years in petroglyphs and cave paintings. Thus, the earliest known efforts to record thoughts and communications were images that were carved or drawn by human hands. Later, written records on clay tablets and papyrus sheets provided a means to record histories, beliefs, people, and events. But no one had yet figured out how to record a human voice, the primary means of communication.

Replicating images was found to be easier than replicating speech. A pantograph was probably one of the earliest mechanical image-replicating devices. A pantograph is a zigzag 'arm' that holds a drawing implement in such a way that an image can be retraced with a stylus, with a drawing tool duplicating the motions, and hence the image, a few inches away. This concept of replicating an event or picture is the essence of recording technologies, whether they are audio or visual.

Music boxes are one of the oldest means of replicating sound. They existed in Europe in the Middle Ages and the idea may have originated through eastern trade with China. By the 1700s, there were many different music box mechanisms that could store and replay tunes. By placing pins in a rotating cylinder or holes in a platter or a strip of paper, a short, predetermined piece of music could be played many times.

Coding systems allows sounds to be replayed. Left: Carmen-Marsch music cylinders from a table-top music box were like cartridges, interchangeable. The pegs would hit the sound mechanism as the cylinder rotated, producing the music. Right: A flat metal cylinder punched with holes to play a tune, housed in a phonograph-style cabinet, from the Bellingham Antique Radio Museum collection. [Classic Concepts photos ©1998, used with permission.]

The printing press is one of the most significant inventions in modern history. It was the first invention to provide a practical way to replicate and inexpensively disseminate multiple copies of the same document. This had important consequences for the permanence of written records. If some copies were lost, the information still had a good chance of surviving if multiple copies had been printed. The creation and replication of information also created a new tool of accountability. It was difficult to deny libelous statements when the proof had been 'captured' in the pages of a book. Similarly, when sound-recording devices were later invented, it became difficult to deny slanderous statements that had been captured on tape or another recording medium.

In 1904, Edwin Welte and Karl Bockish used the concept of music boxes to develop the Welte-Mignon reproducing piano, leading to a craze in 'player pianos' that could play 'by themselves' from notes punched in long rolls of paper. However, even sophisticated devices that played music were not yet able to record and reproduce the sound of a natural human speaking voice.

It may seem odd, but an ancient clay pot, handmade on an old-fashioned potter's wheel, is a type of crude sound-recording device. The grooves in a pot are like the grooves in a record platter, the vibrations of the fingers of the potter create indentations in the clay pot as it spins on a potter's wheel and the hands move upward, in somewhat the same way that the vibrations of a cutting stylus create indentations on a phonograph record as it spins on a revolving base. Unfortunately, the sensitivity of the potter's fingers and the signal-to-noise ratio results in a very poor recording, so we can't get much information about the past from 'playing' a pot, but it is interesting that some of the first phonograph 'records' were shaped like narrow, cylindrical pots, with fine grooves spiraling up the outside of the cylinder. Later, flat platters, called records, were used instead.

Eavesdropping - The Famous and the Infamous

Audio recording technology is one of the closest descendants of human spying and eavesdropping. The field has developed mainly to enhance or replace the human ear. People have

rarely been able to resist the urge to eavesdrop. The impulse to listen in on other people's conversations is powerful and ubiquitous and has been around since long before the early days of the telegraph and telephone.

During the American Revolution, Lydia Barrington Darragh is reported to have eavesdropped regularly on the conversations of officers stationed at British headquarters near her home. She recorded these revelations in a simple code, hid them in large buttons on the clothing of messengers, and had them conveyed to her son, an officer in the Continental Army under the leadership of George Washington. Almost a century later, Allan Pinkerton, founder of the famous Pinkerton's Detective Agency, pointed out that many strategists had made the mistake of thinking that unenlisted women were not a serious threat to the Civil War effort.

Political acts that threaten the status quo often result in civil unrest and an increase in surveillance activities at various levels of society. The Enactment of the 1850 Fugitive Slave law drove many people underground and caused others to become 'manhunters.' Critics declared that the Slave law deprived black people of their right to due process and changed citizens into 'bloodhounds' in search of slaves. It also made Harriet Tubman a more wanted 'criminal' than ever before, with rewards for her capture reaching as high as $40,000. Left: Rush Richard Sloane (1828-1908), a judge and mayor in Ohio, helped slaves escape after their own masters had arrested them. He was prosecuted for his actions under the Fugitive Slave law. Right: A signal lantern being raised on a flagpole at the John Rankin House in Ripley, Ohio. The lantern signaled to slaves that it was safe to cross the Ohio River. [Library of Congress American Time Capsule and Wilbur H. Siebert Collection, c1850; clipping from 1915, copyrights expired by date.]

One of the most remarkable stories of secret activities during the 19th century is that of "Harriet" Tubman (1820 or 1821-1913). Tubman was born Araminta Ross, a poor black slave, in a windowless one-room shack. From the age of six, she was often taken from her family and hired out to others. In 1844, she married John Tubman, a freed slave. When she became aware that her master's property was going to be sold (which would likely include her), she

escaped, in 1849. Her indomitable character led her to take great risks and to make many trips through dangerous territory in her efforts to free more than 200 other slaves. She frequently had to hide in haystacks, barns, and churches. Tubman is credited with great strategic and organizational skills. She used some surveillance technology to achieve her goals, as well, forging passes, writing messages in code, and carefully selecting costumes for the passengers she ferried through the "Underground Railroad."

In 1850, Congress passed the Fugitive Slave act, making it a criminal offense to aid runaway slaves, but Tubman was so good at subterfuge that she was never caught, in spite of posted rewards for her apprehension. During the Civil War, in the 1860s, she worked as a nurse, a scout, and a spy, and received a number of official commendations from Union Army officers. Later in life, she produced letters from prominent dignitaries that substantiated their appreciation of her achievements.

UNVEIL "TUBMAN" MEMORIAL.

Auburn, N. Y.—Impressive ceremonies were held at the Fort Hill Cemetery by the Harriet Tubman Club of New York City, assisted by Empire State Federation of Women's Clubs at the grave of Harriet Tubman, the late famous conductor of the underground railway.

The "Civil War heroine" died last year at the age of ninety-six.

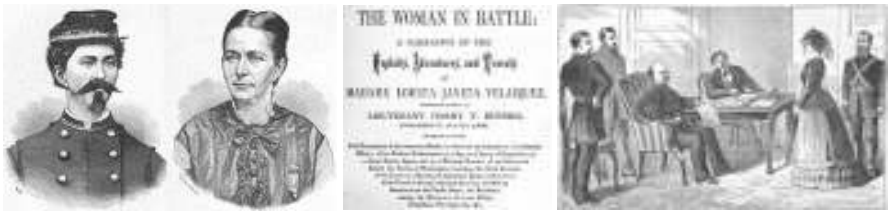
Harriet Tubman, who was born in slavery, fled to the North, and after regaining her freedom in this manner assisted 400 slaves to freedom. John

Left: Harriet Tubman successfully engaged in clandestine and covert activities for many years, freeing slaves through the Underground Railroad using codes, disguises, and forged passes. She also provided scouting and spying services for the Union Army during the Civil War. After the War, she raised money for black schools and created a home for the elderly. Right: This Cleveland Advocate newspaper clipping has some errors (e.g., age), but illustrates the respect that was held for Tubman. Bottom: William H. Seward aided Tubman in acquiring this two-story brick home near Auburn, New York, an illegal transaction at the time. Tubman's home for the elderly became known as the "Harriet Tubman Home for Aged and Indigent Colored People." Her contemporaries greatly respected her, praised her valor and heroism and buried her with Military rites at the Fort Hill Cemetery. The rebuilt Harriet Tubman Home in Auburn, New York, is now a national historic site. [Harriet Tubman historical photo c1900; New York historical photo; Library of Congress clipping, 1915, copyrights expired by date.]

Before long-distance communications, eavesdropping was an immediate and simple means of acquiring information, but only if the eavesdropper could get close to the conversation. Sometimes it was safer and more effective for an informant to enlist the talents of clothiers and chemists in creating a disguise. Sarah Emma Evelyn Edmonds (1841-1898) wrote in her memoirs that she worked as a spy for General George B. McClellan, carrying out eleven secret missions. It is difficult to substantiate these claims, due to a significant lack of corroborating evidence, but some historians have accepted that she enlisted with the army and traveled in disguise as "Frank Thompson." Indeed several women may have enlisted as 'men.'

Apparently pseudo-science accompanied technological science in the thinking of some of the military minds of the Civil War. Before being sent on a secret mission, Edmonds claims that the army gave her a *phrenological* examination. Phrenology is the association of certain mental and psychological traits with the physical characteristics of the skull. In those days it was believed that bumps on the head reflected the more developed portions of a person's brain. The phrenological examination of Edmonds revealed that she had well-developed "organs of secretiveness, combativeness, etc." Apparently these qualities, plus an oral interview, qualified her for a spying mission.

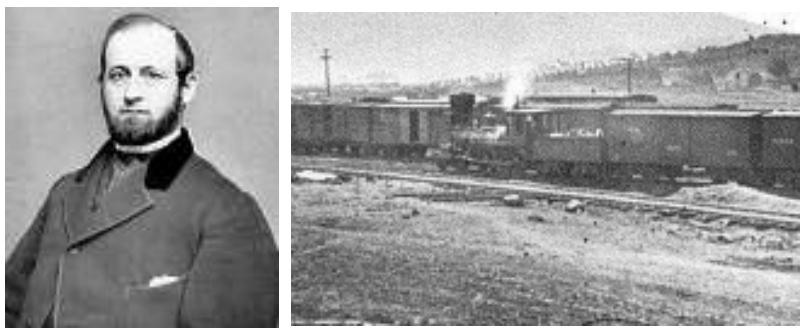
Sarah Emma Edmonds published her "Female Spy" memoirs in 1894, claiming that she participated in the Civil War as enlisted man and male nurse "Frank Thompson." Right: Edmonds is illustrated in her book in one of her costumes as a black 'contraband' working behind rebel lines. Bottom: The memoirs were reprinted in 1895 and again in 1999. Edmonds was inducted into the Military Intelligence Hall of Fame in 1988. A digitized copy of her book can be viewed online through the Making of America (MOA) site at the University of Michigan. [Images from "Nurse and Spy in the Union Army," 1865, copyrights expired by date.]



Sarah Edmonds wasn't the only woman who claims to have used the 'technology of disguise' to infiltrate the army. Loreta Janeta Velazquez has described numerous adventures in the Confederate Army as Lieut. "Harry T. Buford," and her experiences as a spy and secret service agent for General John H. Winder. In the course of her activities, she was arrested on numerous occasions and brought before General Butler (right) [Images from "The Woman in Battle," 1876, copyright expired by date.]

In her memoirs, Edmonds describes how she dressed up as a 'darky,' coloring her arms, head, face, and hands and acquiring 'a wig of real negro wool.' She then crossed through rebel lines and sought work in General Lee's camp. Edmonds recounts that she used nitrate of silver to preserve the color on her face when it began to fade. Later, she dressed as an Irish peddlar-woman. Edmonds apparently had a talent for accents, switching from 'pidjun-English' to an Irish brogue to fit her various disguises. Following the War, Edmonds received distinction and a Civil War veteran's pension.

Sometimes special 'surveillance talents' are revealed unexpectedly in emergency situations. Wiretapping without sophisticated equipment was demonstrated by an unusual traveler, not long before the Civil War. The story is told that in 1858, a Philadelphia telegraph operator named Anson Stager was taking a trip through the midwest when his train broke down. On finding out that the engine had failed, he asked the conductor if he was willing to order a replacement from the next station if Sager telegraphed the message. The conductor said yes and Stager "climbed a telegraph pole and lowered a wire to the ground. He thrust into the ground an iron poker from the coal stove in the coach, and tapped the end of the wire against it to order an engine." To receive the returning telegraph, Stager "stuck out his tongue, placed the wire upon it and received the electrical impulses." [G. Oslin, 1992.]



Left: Stager, a competent telegrapher, became an officer in the Federal Army, a member of the Telegraph Corps and eventually became a General. Right: A Chatanooga train and telegraph wires in c1864. [Library of Congress photos, copyrights expired by date.]

During the Civil War, Stager worked with the Telegraph Corps to create a wartime cypher-correspondence and set up a system of field telegraphs used during battle.

The assassination of President Abraham Lincoln brought together the Military Commis-

sion to determine the full extent and involvement of the 'conspirators' who had been captured in connection with the crime. Twenty-one-year-old Lewis Thornton Powell "Lewis Paine" or "Payne" was indicted for assaulting Secretary of State William H. Seward and his household. At the time of the trial, the Military Commission was not aware that Powell was an agent of the Confederate Secret Service at the time he attempted to murder Seward. At the trial, all were found guilty and Powell and the others were sentenced to death by hanging.

Left: Members of the 'Conspirators Court' Military Commission met for two months in spring 1865 to decide the fate of the prisoners accused of the plot that resulted in the assassination of President Lincoln. Lewis Thornton Powell (middle), a young, charismatic Secret Service agent for the Confederates, was included in the Lincoln conspiracy trial when he was apprehended for attempting to kill William H. Seward (right). Until then, he was not suspected of being a spy. [Minnesota Historical Society, 1865; National Archives photo by Alexander Gardiner, 1865; National Archives photo mid-1800s, copyrights expired by date.]

Anson Stager went on to help Gray and Barton establish the Western Union Telegraph Company. He is mentioned in connection with Western Union in some of the letters of Alexander Graham Bell's family in the late 1870s. Along with George Bliss, he paid a visit to Thomas Edison's laboratory in Menlo Park in February 1877 to discuss foreign rights to an 'electric pen' replicating system conceived by Edison in 1875. A few months after this visit, Edison was busy experimenting with an 'acoustic telegraph' system. The telephone age was imminent.

Left: The Western Union Telegraph Company grew and spread across the continent. This 1895 photograph shows the Western Union Telegraph office in Minneapolis in 1895. Middle: The Gulkana Signal Corps telegraph station in Alaska, 1910-1915. Right: A Western Union telegraph messenger, 1920. [Minnesota Historical Society photos; middle photo from the Alaska State Library, copyrights expired by date.]

General John H. Morgan, a Confederate cavalry leader was known for his ability to tap Union lines. He could apparently mimic the telegraph style of Union telegraphers (a rare talent) and send misinformation and orders, signed with the names of Northern generals. The Union responded by encrypting their messages, providing the code only to generals and the War Department. (See Cryptologic Surveillance.)

In the American Civil War, General J. Stuart is reported to have carried a telegraph tapping device to intercept military communications, a slightly more sophisticated means than Stager's method of touching the wire with his tongue.

The telegraph had a substantial impact on the stock market. People who lived far from Wall Street could now participate. They could also eavesdrop on telegraph communications containing up-to-date market-related information. By 1864, there had already been at least one prosecution for the tapping of telegraph lines to obtain stock information [Dash, Schwartz, Knowlton, 1959]. A few years later 'stock ticker' machines (specialized printing telegraph receivers) were invented.

Another historic telegrapher who became famous for his association with surveillance activities was John E. Wilkie who became chief of the U.S. Secret Service in 1898. A 1906 edition of The Railroad Man's Magazine describes Wilkie as a newshound in his youth who 'scooped' big stories by eavesdropping on the 'fire-alarm-telegraph-wire.' The Secretary of the Treasury at the time apparently solicited Wilkie for the Secret Service without application. Wilkie began to tackle crime and made a long, stealthy stalk of a bold and substantial counterfeit gang, eventually convicting the counterfeiters. One of the members of the gang was found to be a former U.S. State District Attorney.

Inventions Leading to the Telephone

Telephone technology is an evolutionary step arising from the revolutionary invention of the telegraph (both telegraph and telephone history are covered in more detail in the Radio Surveillance chapter).

The telegraph was the first technology that dramatically changed hand-to-hand physical communication, through objects and letters, to almost instantaneous communication over great distances. Even the carrier pigeon couldn't fly at the speed of sound or light. Telegraph concepts were developed in Europe in the late 1770s, and first put to practical use in England in 1836 by Wheatstone (1802-1875) and Cooke. In America, Samuel F. B. Morse (1791-1872) and his assistant Alfred Vail were developing telegraph equipment as well. In the days of telegraph systems, an eavesdropper had to learn the code to be able to listen in on messages. With the invention of the telephone in the late 1800s, eavesdropping became much easier.

In the late 1850s, Antonia Meucci, an Italian living in Cuba, attached wires to animal membranes to transfer sound through current, but due to his isolated location, news of his discoveries did not spread. In Europe and America, similar experiments were being conducted. Johann Philip Reis (1834-1874), a German inventor, demonstrated the transmission of a tone through wires in 1861. He reported in a letter that he could transmit words, but other evidence of his achievement has not survived. At about the time of his death, Elisha Gray (1835-1901), an American physicist, was experimenting with telegraphy and succeeded in transmitting tones, the basis of telephony. His inventions ran neck and neck with those of Alexander Graham Bell (1847-1922). Thus, the invention of the telephone was envisioned by a number of brilliant inventors at about the same time and it soon came to be a much-desired commodity in business and personal communications.

Now that inventors knew that wired telephony was possible, what about wireless communications? It didn't take long before they were competing to see who could develop the first wireless devices. In 1866, Mahlon Loomis (1826-1886) demonstrated that airborne kites could pass a signal from one kite to the other without a physical connection. Six years later, he applied for a patent for a wireless telegraphy system. Amos E. Dolbear, a university research

professor and writer, was awarded an 1886 patent for a wireless telegraph system based on induction. In the mid-1890s, Aleksandr Stepanowitsch Popow (1859-1906) sent a wireless shipboard message to his laboratory in St. Petersburg. While not as quick to develop as the conventional telephone, these inventions eventually led to the development of radio and cellular telephone communications.

The Early Development of Recording Devices

A punch card can be used to store a weaving pattern so that it can be repeated at a later time. Music boxes use a similar system, storing songs on punched paper or metal. These were already in use by the early 1800s. However, recording technologies that could save human speech didn't exist until a few years before the outbreak of the American Civil War and didn't get firmly established until about a decade after the end of the War.

Sound-recording devices and stock ticker devices were developed around the same time, in the mid-1800s. While they might seem to be divergent technologies, they were held together by powerful social factors–the desire to know and record business transactions. The capability to record and transmit business information, whether by telegraph signals or by voice, made a permanent change in the economic structure of the world.

In the 1860s, a new type of telegraph was devised to transmit business information. In essence, the first stock ticker machines were 'printing telegraph' machines. Since they were a valuable business commodity that not everyone could afford, there was a temptation to spy on messages or access the telegraphic signals carrying stock information.

Telegraphic stock tickers had an enormous impact on business dynamics since they made it possible to monitor and interact with the stock market from remote locations. Western Union first introduced stock tickers to brokerage firms in 1866. Left: The New York Stock Exchange building as it looked in the early 1900s. Middle and Right: Cartoon of ticker tape (a type of printed telegraphic message) being carefully studied by an investor. [Life Magazine cartoon, 1899; Library of Congress, Detroit Publishing Co., ca. 1904; copyrights expired by date.]

In 1857, Édouard-Léon Scott de Martinville developed one of the earliest known sound-recording devices, the *phonautograph.* He configured a funnel-shaped horn to channel the sound to a sensitive diaphragm which transmitted the sound vibrations to a stylus and recorded them on a rotating cylinder of blackened paper (charcoal or ink may have been used). This is the essential concept of cylinder and platter-based recording devices.

By 1877, Charles Cros in France and Thomas Edison in America had both invented devices to record sound. (Since Edison was both prolific and commercially astute, his devices are better known.) With the basic concept in hand, Edison set about trying to find a practical and readily available recording medium. He created early recordings on both waxed paper

and tinfoil. The idea of using paper was not as unusual as it might seem, since certain music boxes and looms already relied on patterns punched in paper or metal.

The success of these new sound-recording technologies meant that it was now possible to capture and replay nature sounds, music, and voices, with or without the knowledge of those being recorded.

As a surveillance technology, however, recording was still in its infancy. There were four big limitations to the early machines:

- The recorders were bulky and difficult to move around.
- It wasn't truly a re-recording medium, as the wax had to be reheated or reapplied, or the metal had to be hammered out in order to be used again.
- The recording times were very short, generally only about three minutes.
- The quality of the sound was crude and scratchy, though probably adequate for identifying voices and speech. The bigger limitation was that microphones hadn't been invented yet and the speaker had to be near the horn that funneled the sound in order for a voice to register on the recording.

In spite of the limitations of early machines, Edison recognized the potential commercial value of a device that could record voice transactions over the telephone "so as to make that instrument an auxiliary in the transmission of permanent and invaluable records, instead of being the recipient of momentary and fleeting communication."

By 1881, there were dictating machines that freed the speaker from being present at the same location and time as the person transcribing the message. Recording technologies were of particular interest to business people trying to gain mobility or a competitive advantage. They provided greater flexibility in time scheduling. A recording could be shipped to another location or recorded off-hours and transcribed during working hours.

Phonographic Recordings

People who enjoyed phonograph records from the late 1800s until the late 1900s are familiar with them as a playback medium and most listeners had never seen a 'record-pressing' device. In the early days of recording, however, there weren't thousands of companies selling records, so there was very little to play on the phonograph machines. At that time, companies were selling phonographs as recording devices in much the same way they now sell tape recorders.

One of the ways in which phonograph recorders were marketed was for "Phonograph Parties." In trying to establish a new market, vendors encouraged people to throw parties in which they surreptitiously recorded their friends. The idea was to then surprise them with the fact that they had been recorded. The market for consumer phonograph-recording machines virtually disappeared, however, when record companies started mass-marketing prerecorded discs. People who wanted to make their own individual recordings no longer had easy access to phonograph recorders.

Meanwhile, the demand for prerecorded sound was booming. The early Edison recordings were sold on cylinders, but cylinders with variable-depth grooves were hard to mass-produce. Inventors looked for other solutions.

In 1887, Emile Berliner developed an important innovation in the phonographic process in which the groove created by the recording stylus was etched side-to-side rather than up-and-down. This made it possible to mass-produce flat records by 'stamping' out platters in quantity and imprinting the grooves in a softer material. Berliner chose shellac because it was

malleable when heated and hard when cooled. The Victrola company was built upon Berliner's U.S. patents. Edison's highly competitive spirit was roused and he responded by switching to discs, but they weren't compatible with the Victrola side-to-side-groove machines.

Left: A Victrola could play but not record. Right: A phonograph and wire-recording machine could both play and record. [Classic Concepts ©1997 photos, used with permission.]

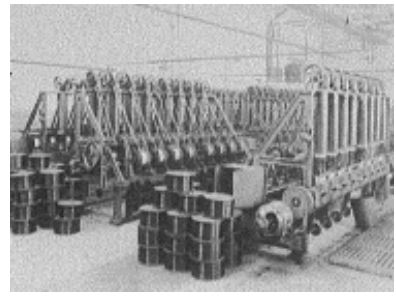
The early players were limited, so inventors looked for more practical ways to record longer sequences and perhaps re-record on the same medium.

In 1888, Oberlin Smith submitted a caveat for a patent (notice of intention to file) for a magnetic device for recording a phone conversation. But Smith never filed the actual patent, choosing instead to publish his ideas in the September issue of "The Electrical World." Smith suggested recording on a metal-impregnated thread, an idea that led other inventors to experiment with wire.

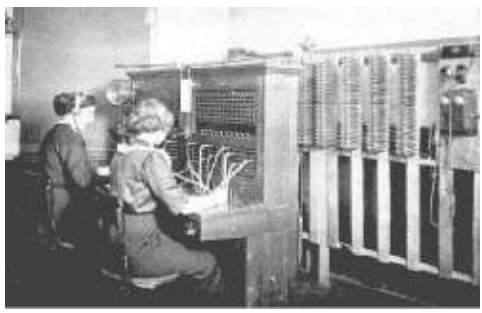
By 1898, a Danish inventor, Valdemar Poulsen, had figured out a way to coil wire so that it could be rotated and passed under a magnetic pickup, thus creating a device that could record on fine wire. He demonstrated his invention at the international exposition in Paris, in 1900. Unfortunately, long spools of wire were awkward to handle and not ideal in terms of sound quality. Nevertheless, it was a breakthrough, and Poulsen patented his 'Telegraphone,' suggesting that it could be used for the unattended recording of phone messages. When he later added an automatic-answer feature; he had essentially developed the telephone-answering machine.

These basic recording technologies were improved over the next two decades by various inventors, to include amplification, better fidelity, a variety of recording media, and various mechanisms to turn the machines on and off. During this same time period, telegraph lines continued to reach out to the more remote areas of the continent and telephone switchboards were appearing almost everywhere. Business telegraphy, voice communications, and sound recording technologies were becoming well-established fixtures of society.

The basic aspects of sound recording were firmly in place by the 1910s, a fact that caused a stir in the motion picture industry. Up to now people had been getting their movie entertainment from 'silent pictures,' moving films without sound. By 1911, inventors were creating ways to synchronize sound with the pictures, creating a whole new genre called 'talkies' and putting a lot of the silent film stars out of work. This was an important development because, from this time on, many important technologies were able to simultaneously record images and sound. (See the Visual Surveillance chapter for further information on the recording of images.)

Left: Bales of wire blanket the rough terrain where the telegraph line crossed the Stikine River in B.C. at the turn of the century. Right: Bales of copper wire. Copper wire was used for almost every type of electrical installation from office buildings, to phone and telegraph wires, to wiring in automobiles. Most early telegraph and phone taps were set on copper wires. [B.C. Archives c1900 historical photo; Library of Congress 1925 Detroit Publishing Co. photo, copyrights expired by date.]




Telephone services expanded across North America in the early part of the century, staffed by female operators. Left: Switchboard operators at work in Port Alberni, B.C. Right: Telephone operators in the Vancouver Hotel, B.C. [B.C. Archives c1910s and 1916 historical photos, copyrights expired by date.]

There followed a period of refinement in sound technologies. Optical sound tracks were added to films, broadcast sound fidelity was improved by modulation, and, in 1917, E. C. Wente invented a condenser microphone to record clearer, more uniform sound. Edward Howard Armstrong developed the superheterodyne circuit, which improved the sensitivity and selectivity of radio receivers, so that amplifier tuning was no longer necessary. Technology was becoming more sophisticated and people were devising new ways to use it.

Regulation of Communications Technologies

In the latter half of the 19th century, developed nations began to organize their political economies around the new technologies. As telegraph systems unified nations, nations established regulations to control their use.

In 1835, in Britain, the Municipal Corporations Act called for individual regions to set up police forces overseen by local watch committees. In 1842, a Criminal Investigation Department was established. By 1849, the various district police stations were being interlinked and connected to Scotland Yard by telegraph lines.

America followed a similar path. The Boston and New York Police departments were established in 1838 and 1844, respectively. Within a year, the precincts in New York were

interconnected by a police telegraph system. Due to political wrangling, the New York Metropolitan Police was created in 1857, with broader jurisdiction over New York City, Brooklyn, and Westchester County (coexisting with the New York Municipal police until 1870). By 1878, police telegraph boxes were being installed in the large cities of America.

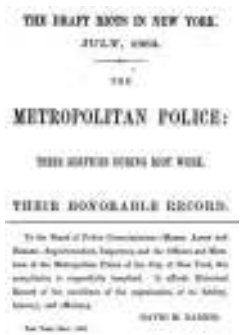
At the federal level, changes were also occurring. The Internal Revenue Service was put in place in 1862. Then, in 1866, regulation of the telecommunications industry was initiated with the *Post Roads Act*, which granted the Postmaster General the authority to oversee rates for government telegrams and to assign rights of way through public lands.*

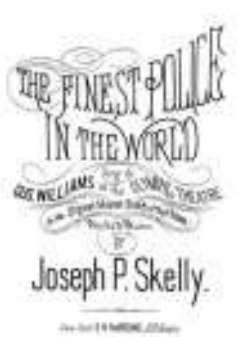
Public Officials and Charges of Wiretapping

While phone 'tapping' implies some electrical or mechanical connection to a phone line, in this historical section it will be used in its broadest context as meaning any persons or any recording devices 'listening in' on a wired or wireless phone conversation with whatever means are at their disposal. In other words, it encompasses most types of telephone eavesdropping.

In 1863, a 'draft riot' galvanized the New York Metropolitan Police to quell the disturbances. The police were publicly commended:

> "The services of the Metropolitan Police, officers and men, during Riot Week, won for them the admiration and confidence of the community. Never did men meet an emergency so fearful with more promptness, unanimity, and courage, and never was hazardous and prolonged duty discharged with more willingness and fidelity."
>
> [David M. Barnes, "The Metropolitan Police: Their Services During Riot Week. Their Honorable Record," New York: Baker & Godwin, 1863.]


THE DRAFT RIOTS IN NEW YORK.
JULY, 1863.
THE
METROPOLITAN POLICE:
THEIR HONORABLE RECORD.


THE FINEST POLICE IN THE WORLD
Joseph P. Skelly.

Prior to the investigation of the New York Police in the early 1890s, the actions and reputation of the Metropolitan Police were a source of pride for the city. Left: David M. Barnes authored "The Metropolitan Police: Their Services During Riot Week. Their Honorable Record" in 1863, commending police actions. Middle: Sheet music by Joseph P. Skelly exemplified the public perception of the Police force in 1875, prior to the Lexow Commission Report. Right: Theodore Roosevelt instituted reforms as a member of the Police Board from 1895 to 1897 (shown here as Governor in 1910). [Baker & Godwin, 1863; E.H. Harding sheet music, 1875; Library of Congress, Detroit Publishing Co., 1899, copyrights expired by date.]

New York enacted statutes to prohibit eavesdropping in 1892. Yet, to the astonished alarm of the residents of America's mightiest city, the first celebrated case of wiretapping involved

*The telephone was not yet on the scene. The regulatory responsibility of the Post Roads Act eventually came under the jurisdiction of the Federal Radio Commission (through the RadioAct of 1927). Then, through the Communications Act of 1934, it became the Federal Communications Commission (FCC) which is still the main regulatory body.

the New York Police. They were charged with eavesdropping on sensitive communications and continued to tap as though they were exempt from the law. In 1894, a committee headed by State Senator Clarence Lexow released damning revelations of New York Police corruption, extortion, and wiretapping.

Reports of abuse in New York and elsewhere increased the population's awareness of wiretapping and made people more sensitive to the vulnerability of trusted officials and of conversations over public communications systems. In 1862, California enacted a law prohibiting the tapping of telegraph wires. In 1893, the police community at large founded the International Association of Chiefs of Police (IACP) to create a national forum for police organization, codes of conduct, and record-keeping. In 1899, the San Francisco Call accused the San Francisco Examiner of wiretapping reporters' communications and stealing exclusive stories, while thousands of miles away, the state of Connecticut enacted an electronic eavesdropping law that made it a state crime to listen to "the transmission of telegraphic dispatches or telephone messages to which he is not entitled." The California legislature responded, in 1905, to complaints of intrusions by extending the 1892 telegraph law to restrict wiretapping of telephone communications [Dash, Schwartz, Knowlton, 1959].

In 1895, Theodore Roosevelt was appointed to the New York Police Board and initiated changes that helped restore public confidence in the force that was lauded as "New York's Finest" before the scandal. He reformed hiring practices, record-keeping, and identification procedures. The New York force had a small number of women 'matrons' but none had yet been hired to work at Police Headquarters. Roosevelt appointed Minnie Gertrude Kelly to a post in 1896. He also adopted the Bertillon system, a biometric bone-measuring identification system that predated fingerprinting. Roosevelt further reorganized the Detective Bureau and appointed Isabell Goodwin, who became a police matron in 1896 and went on to become an undercover agent. She was promoted to first grade detective in 1912.

Left: Thomas Edison's company recorded this film of the June 1899 Policeman's Parade in New York City. When Edison's company shot the film, the New York Police Department was still recovering from the corruption scandals that had surfaced in the early 1890s. The Lexow Committee, which investigated the Department, described serious criminal activity within the force which included wiretapping abuses. Right: The Policemen's Parade on Fifth Avenue, ca. 1903. The annual Police Parade was cancelled in 1895 due to the drop in public opinion but later restored with reforms spearheaded by Theodore Roosevelt. [Library of Congress, Thomas A. Edison, Inc.; Detroit Publishing Co., copyrights expired by date.]

The telegraph had a major impact on unifying the vast North American wilderness, yet the telephone patents of Alexander Graham Bell were a potential goldmine to any company who could use them to establish a commercial system to augment telegraph systems with something more natural. The Bell system was incorporated in 1878, based on Alexander Graham Bell's patents, less than 15 years after the telephone was first introduced in America. A telephone was quickly installed in the White House and President Hayes placed a call to the Bell company a few miles away. A telephone was also installed in the Washington, D.C. police station. By the early 1900s, the police departments in major cities had installed telephone

systems that would eventually displace the telegraph lines.

The quick installation of phones in the White House and the police station may, in part, have been a marketing/networking coup on the part of the Bell company. Under the astute business management of Theodore Vail, the Bell system did very well, so well, in fact, that much of the early legislation related to communications was in response to the activities of the Bell system and, later, AT&T.

Entrepreneurs wanted in on the growing communications profits. In the early 1890s, when the original Bell patents expired, thousands of independent telephone companies sprang up throughout the country. The Bell system responded by buying out, forcing out, and consolidating the independents. It regained its dominant position in just a few years. This situation had advantages and disadvantages. While innovation and local community-owned businesses were suppressed, consistency and stability were maintained under the direction of the corporate giant. This uniformity of hardware and services had a substantial impact on phone surveillance. A consistent national telephone infrastructure made it very easy to eavesdrop on telephone communications, especially before there were statutes in the United States to regulate wiretapping.

Other technological inventions were changing the country and the strategies of the people who were maintaining law and order. The invention of the automobile and the radio forever changed the way local law enforcement officers patrolled their beats and communicated with one another and with other precincts. It was a new age of transportation and communications. The concept of distance was to dramatically change over the next few years as automobiles and motorcycles superseded horses and bicycles.

Motorcycles and automobiles were adopted for police work all over the country at about the same time that telephones were superseding telegraphs and radio communications were being established. Top: The Police Department of the City of Bridgeport, Connecticut displaying motorcycles in October 1914. Bottom: Military police with motorcycles at division headquarters in Camp Zachary Taylor, Kentucky in front of the Western Union Telegraph Company building (center). [Library of Congress, Henry J. Seeley collection, 1914; Library of Congress, Caufield & Shook collection, ca.1918, copyrights expired by date.]

Problems were still occurring in New York, however. In 1916, a New York mayor authorized wiretapping of Catholic priests in a charity-fraud investigation, without demonstrating that there was sufficient cause to initiate the action. In the course of investigating these police actions, the legislature discovered the police could tap any line in the New York Telephone Company and had listened to many confidential conversations. These continued accusations of wiretapping abuse brought more public and Senate attention to the issue.

Global Developments

Improvements in long-distance travel and communications allowed geographically diverse organizations to cooperate internationally. It now became possible to monitor criminals who

fled to other countries. Up to this point, it was very difficult to capture a felon who melted anonymously into a foreign nation. In 1914, the first International Congress of Criminal Police came together in the Principality of Monaco to discuss global issues in policing including cooperative record-keeping and identification measures.

In 1923, at a meeting of the International Congress of Criminal Police, the International Criminal Police Commission was formed, where it gradually evolved into INTERPOL, an international data-collection agency that would assist with international investigations within certain guidelines.

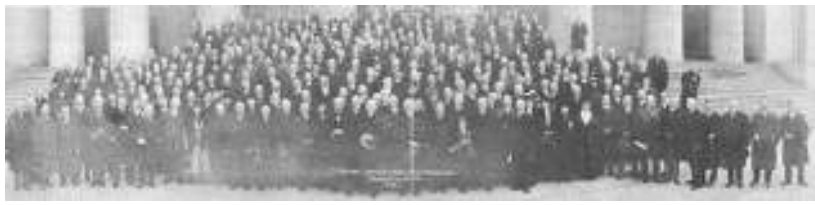
Wiretapping Legislation in America

In America, it appeared as though wiretapping might eventually be outlawed altogether but for two strong social factors that caused the government to reconsider its use. The first was the outbreak of World War I and the fear of foreign infiltration. The second was Prohibition and the fear of gangsterism and general public opposition to some of the strictest prohibitions. Both of these events increased the prevalence of surveillance activities in general.

With the outbreak of World War I, the fear of foreign agents operating in America led to many acts intended to deal with foreign infiltration, including *The Act of October 29, 1918* in which Chapter 197, 40 Statute 1017 says in part that:

> "... whoever during the period of governmental operation of the telephone and telegraph systems of the United States shall, without authority and without the knowledge and consent of the other users thereof, except as may be necessary to operation of the service, tap any telegraph or telephone line, or wilfully interfere with the operation of such telephone and telegraph systems or with the transmission of any telephone or telegraph message, or with the delivery of any such message, or whoever being employed in any such telephone or telegraph service shall divulge the contents of any such telephone or telegraph message to any person not duly authorized or entitled to receive the same, shall be fined ... or imprisoned for not more than one year, or both."

This Act established that tapping was to be used for counterespionage purposes only. It was not intended to endorse wiretapping of "U.S. Persons."



Delegates and speakers at the "National Conference on World Wide Prohibition" held in Columbus, Ohio, in November 1918. [Library of Congress Panoramic Photographs Collection, 1918, copyright expired by date.]

On 11 November 1918, the Germans signed the Armistice, ending World War I. From 19-22 November 1918, the "National Conference on World Wide Prohibition" was held in Columbus, Ohio with some significant consequences.

In 1919, the *18th Amendment* to the Constitution was ratified, prohibiting the "manufacture, sale, or transportation of intoxicating liquors within, the importation thereof into, or the exportation thereof from the Unites States and all territory subject to the jurisdiction thereof for beverage purposes ..." Enforcement of the measures was defined in the *Volstead Enforcement Act*.

SUPREME COURT DECISION ON THE PROHIBITION AMENDMENT AND THE VOLSTEAD ENFORCEMENT ACT ANXIOUSLY AWAITED

How the Supreme Court will pass upon the prohibition issues now before it, is a matter of daily concern. What the court will have to say on this vital issue is a matter of current interest to those for and against the liquor business. That a favorable decision in the interest of a better citizenship will be rendered, is

Left: Announcement of the Supreme Court Decision on the 18th Amendment and the Volstead Enforcement Act on alcohol prohibition, June 1920. Right: U.S. officials enforcing alcohol prohibition laws at the Brownsville Custom House in Texas, in Dec. 1920. [Ohio Historical Center Archives Library, 1920; Library of Congress South Texas Border Collection, 1920, copyrights expired by date.]

In 1927, Congress passed the *Radio Act of 1927*, Public Law 632. This important act established the Federal Radio Commission (FRC) to regulate use of the airwaves. Further, Section 27 stipulated that:

> "No person receiving or assisting in receiving any radio communication shall divulge or publish the contents, substance, purport, effect, or meaning thereof except through authorized channels of transmission or reception to any person other than the addressee ....
>
> and no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purport, effect, or meaning of such intercepted message to any person; and no person not being entitled thereto shall receive or assist in receiving any radio communication and use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto ...."

In 1927, wiretapping was outlawed in Illinois but, as had happened in New York, the police illegally continued the practice.

Constitution Issues and Wiretapping

The enactment of Prohibition brought many new cases into courts, some of which strongly challenged constitutional issues and the ability of the legal system to sort them out. Wiretapping featured prominently in one of these cases.

Wiretapping was used to catch liquor offenders during Prohibition. In a now-famous case, Roy Olmstead was caught running a $2 million a year smuggling operation out of the Pacific Northwest. Information about the illegal operation was largely obtained by four Prohibition Agents tapping through wires that were inserted by a lineman into the normal telephone lines outside the premises. The tapped dialog was transcribed into almost 800 typed pages that detailed illegal operations including the smuggling and sale of liquor, tax evasion, and bribes offered to local police officers. Olmstead and others were convicted of conspiracy to violate the National Prohibition Act, based partly on the wiretap evidence. Olmstead appealed. It went to the Supreme Court, but since no physical trespass had occurred, the Justices agreed

that conversation was an intangible and thus did not constitute illegal search and seizure.*

In association with this string of events, Justice Louis Brandeis offered the following dissenting point of view:

> "The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping."
>
> [Justice Louis Brandeis, *Olmstead v. United States*, 1928.]

In spite of this eloquent and impassioned plea, the U.S. Congress did not make wiretapping illegal, but neither was the matter permanently resolved. Brandeis' words would echo many times in cases through subsequent decades.

Audio-Visual Developments

These days people typically own their own phones and are responsible for their phone lines from the junction box to the interior of the house or office. In the 1920s, however, except for a few communities or large corporations with independent phone systems, AT&T was in control of everything from the local office to the phone inside the house (which was leased to the customer). As the 1920s progressed, AT&T grew, technology improved, and recording technologies became more sophisticated and practical to use, but they weren't permitted on Bell system phones.

The telephone changed the way public service industries and businesses conducted their activities. Left: Forest-fire-reporting telephone lines provided a new way to report and track the progress of fires (Florida, 1937). Middle: A phone system provided a way for logging crews in different areas of the forests to intercommunicate (1941). Right: Telephones could now be used to direct construction crews from a good vantage point of a distance. Here a signal man instructs crews working at the Shasta Dam in California, in 1941. [Library of Congress FSA-OWI Collection photos by Arthur Rothstein and Russell Lee, public domain.]

AT&T had a virtual monopoly on telephone service in the 1920s and held jurisdiction over the phone lines and the phones they installed on customers' premises. They responded

*Reference *Olmstead v. United States*, 277 U.S. 438, 462 (1928). Chief Justice Taft ascribed the rule to both the Fourth and Fifth Constitutional Amendments. Justice Brandeis and Justice Holmes dissented, offering the opinion that evidence admitted through violation of the Fourth Amendment in turned violated the Fifth Amendment.

to developments in technology by banning the use of answering machines on the public networks. Thus, in America, recorders could only be used on private systems or those belonging to independent systems that permitted them.

By 1926, Dictaphone was selling the Telecord machine, an electronic telephone recorder that used wax cylinders. Synchronized sound movies, video technologies, and the earliest tape players were in development by the late 1920s.

The pressure on AT&T to permit telephone-answering machines increased. AT&T relented somewhat in 1930, allowing Dictaphone's Telecord machine to be used on private branch exchanges (PBXs). The machines caught on in America, in spite of the restrictions. People wanted the capability to monitor phone calls while they were away and to record conversations. Small businesses were eager for the machines, especially those that couldn't afford to hire a receptionist or who wanted to offer 24-hour telephone information. Europeans began using answering machines and the variety of types of recording media grew. In 1932, Loftin-White labs in New York announced a disc-based answering machine.

AT&T was concerned about how to maintain control and still meet public demand for answering machines and began to provide call-forwarding services so subscribers could arrange calls to be forwarded to live answering services.

As telephone service spread and improved, consumer magnetic-tape machines were soon to appear. In 1935, at the Radio Exhibition in Berlin, the *Magnetophon* was demonstrated, becoming available to the public in 1936. The Magnetophon provided a means to record on tape. A Swiss answering machine called the *Ipsophon* recorded on steel tape. You could even dial the fully automated Swiss machine to remotely retrieve phone messages. Semi J. Begun, a German immigrant working at the Brush Development Company in America, developed both steel tape and coated-paper tape recorders and sold the devices to the military. The machines could record on a variety of types of media including tapes, discs, and wire. Wire recorders of various types were being marketed in competition with the other formats and reached their peak in the late 1930s and early 1940s. Thus, there were now a number of practical formats to meet the growing demand for telephone call recording.

These photos illustrate the manual telephone systems still in use in the 1930s and 1940s. Their simple electrical/mechanical connections and uniformity made them easy to wiretap. Less scrupulous operators were also known to eavesdrop on calls, directly motivating the invention of automatic switching systems and phones with dials. Left: Switchboard operator at Littlefork, Minnesota in 1937. The phone jacks had to be manually plugged into the appropriate holes by a human operator to make a connection. Middle: Old-style home telephone with a hand crank, in Martin County, Indiana. Right: A telephone lineman using boot spurs to scale a pole to do maintenance on a line in 1940. Linemen's telephone sets were designed with alligator clips to hook temporarily to a line for testing. These were sometimes also used to tap lines. [Library of Congress photos by Roy Stryker, Arthur Rothstein, and Lee Russell. FSA-OWI collection, public domain.]

Further Legislation Related to Wiretapping

In 1934, the *Federal Communications Act* (FCA) prohibited the interception and divulgence of wire or radio communications; 47 U.S. Code, Section 605 reads:

> "No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person...."

Even though the Federal Communications Act was aimed more at radio communications than wireline telephone communications, the Supreme Court interpreted the Act broadly. Thus, in a significant move, the FCA ruling was instrumental in reversing the famous *Olmstead* decision. On the basis of the new FCA law, the Court held in *Nardone v. United States* that wiretap information acquired by federal agents was not admissible as evidence. It further ruled in 1939, in *Weiss v. United States,* that this applied to federal tapping of intrastate as well as interstate communications. As a consequence of the various rulings, the Attorney General ordered a halt to FBI wiretapping. Ten years later, the pressure of World War II would cause the tide to turn once again.

The social and economic instability caused by the War rekindled the debate about wiretapping. America was emerging as a multicultural country such as had never existed before. Over the last half century, people from nations around the world, in numbers equal to Canada's entire population at the time, had immigrated to the United States. A large proportion of the population consisted of first generation Americans, with languages and cultural habits drawn from a wide spectrum. National security and local law enforcement agents felt that it might be relatively easy for a foreign spy to 'blend in' to this melting-pot landscape.

Since the *Nardone* case, wiretapping had been suppressed. Then, in 1940, J. Edgar Hoover, Director of the FBI, argued that the bureau needed broader wiretapping powers to detect and convict spies and subversives. Attorney General Robert H. Jackson decided that intercepting the communications would be permissible under the *Nardone* decision if the information accessed was not divulged, but kept within the federal government. President Roosevelt subsequently authorized the wiretapping of foreign agents for national security. He did, however, restrict approval to:

> "... persons suspected of subversive activities against the government of the United States, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens."

In response to the President's approval, in 1941, Attorney General Jackson instructed the Director of the FBI to maintain records of wiretapping, including cases, times, and places. While the requirement to keep a log might seem to establish accountability, the opposite may also be true. Jackson may, in essence, have asked the foxes to guard the henhouse, by not appointing an external, independent party to monitor the wiretaps.

Hoover continued his lobby for broader powers by opposing legislation requiring warrants for wiretapping.

In 1942, President Roosevelt established the Office of War Information to control news and propaganda which, among other things, generated a remarkable legacy of photographs detailing life (as they wanted it to be seen) in America.

Challenging the Olmstead Decision

The courts were busy, too, as another important case related to eavesdropping was debated that year.

In 1942, in *Goldman v. United States*, the plaintiff charged that law enforcement officers had violated the Fourth Amendment. They had bugged a wall adjacent to the plaintiff with a Detectaphone which could amplify and record the sounds in the next room. As there was no physical trespass of the bugged suite, the Court decided against the plaintiff, stating that the Fourth Amendment had not been violated. Justice Roberts voiced his opinion that there was no violation because there was no illegal search and seizure and the evidence obtained in this way was admissible in a federal court. This decision is important in another respect because it suggested a legal distinction might be made between bugs and wiretaps.

In 1943, a secret project, code-named VENONA, was quietly initiated within the U.S. Army Signal Intelligence Service (forerunner of the NSA) to monitor foreign communications.

Another prominent court case related to wiretapping occurred in 1945, in *Bridges v. Wixon, District Director, Immigration and Naturalization Service*. In its findings, the Court strongly denounced the Immigration and Naturalization Service (INS) and others for persistent hounding and attempts to deport Harry Bridges. Bridges was an Australian who had immigrated to America in 1920. Deportation proceedings were instituted against him on the grounds that he was affiliated with the Communist Party which, in turn, was allegedly seeking to overthrow the U.S. government. Statements in the case were passionate and direct, in part stating that:

> ".... The record in this case will stand forever as a monument to man's intolerance of man. Seldom if ever in the history of this nation has there been such a concentrated and relentless crusade to deport an individual because he dared to exercise the freedom that belongs to him as a human being and that is guaranteed to him by the Constitution...."

Later in the statement, it comments on wiretapping of communications connected with Bridges:

> "Industrial and farming organizations, veterans' groups, city police departments and private undercover agents all joined in an unremitting effort to deport him on the ground that he was connected with organizations dedicated to the overthrow of the Government of the United States by force and violence. Wiretapping, searches and seizures without warrants and other forms of invasion of the right of privacy have been widely employed in this deportation drive.... The Immigration and Naturalization Service, after a thorough investigation of the original charges in 1934 and 1935, was unable to find even a 'shred of evidence' warranting his deportation and the matter officially was dropped...."

At the federal level, eavesdropping was being employed on an international scale. A secret operation called SHAMROCK was initiated around the time of World War II. SHAMROCK was a telegraph-message-collection program in which three prominent international telegraph companies agreed to requests from the Government for access to certain international telegraph messages. The program was originally intended to extract telegrams relating to the communications of *foreign* targets (in compliance with national security guidelines), but later investigations indicate that the program gradually changed to include the communications of U.S. citizens and organizations, as well.

> "During World War II, all international telegraph traffic was screened by military censors, located at the companies, as part of the wartime censorship program. During this period, messages of foreign intelligence targets were turned over to military intelligence....

> The Army Security Agency (ASA) was the first Government agency which had operational responsibility for SHAMROCK. When the Armed Forces Security Agency was created in 1949, however, it inherited the program; and, similarly, when NSA was created in 1952, it assumed operational control."
>
> [U.S. Senate Select Committee reporting in "Intelligence Activities–The National Security Agency and Fourth Amendment Rights," 6 November 1975.]

Some people would argue that Operation SHAMROCK was a necessary wartime security measure. Others would oppose it on even those grounds. Most people, however, would agree that SHAMROCK should not have monitored the communications of U.S. citizens and should never have continued, as it did in various forms, for almost 30 more years. At the present time, it is difficult to reconstruct and study the operation because neither the Government nor the three companies kept a paper trail of these arrangements.

Until now, significant issues related to wiretapping had been decided in the courts, but Hoover saw an opportunity to repeat a wiretapping-related request to President Truman and the President signed it, perhaps not realizing its full implications. In 1950, George M. Elsey, the Assistant Counsel, expressed his concerns to President Truman that the wording of the Hoover memo was very broad, but Truman took no steps to reverse his approval. As far as the White House and the FBI were concerned, wiretapping could now be used in situations other than national security investigations of foreign agents.

Post-War Developments in Technology

World War II was winding down, families were reunited, the economy adjusted to Cold War and peacetime activities and the Korean conflict was stirring up in southeast Asia.

The end of the Second World War provided an opportunity for American and British technical investigators to 'discover' foreign technologies, including the Magnetophon recorder that was in use in German-occupied nations. The U.S. Alien Property Custodian seized the patent rights. Based on technological devices found overseas, the U.S. Department of Commerce published technical information about tape recording. John T. Mullin demonstrated a Magnetophon machine to the Institute of Radio Engineers in America. Magnetic tape recorders were poised to supersede the steel tape, 45 rpm, and wire recorders that had shared the market for the last several years.

By the late 1940s, tape recorders were beginning to win the 'format wars.' Even movie reels were changing from optical to magnetic sound. Meanwhile, 'Ma Bell' continued to face pressures from people who wanted to use telephone-answering machines. AT&T began leasing the machines to their customers.

In 1947, inventors at the Bell research labs invented the transistor, a development that was to have a stunning impact on the development of electronics devices from that point on.

Two things happened to dramatically affect AT&T's business practices in 1949. The Federal Communications Commission (FCC) had taken steps to relax regulations against the use of answering machines culminating in a landmark ruling in 1949, permitting consumers to use telephone-answering machines. The Department of Justice (DoJ), in turn, sued AT&T for antitrust violations (the second effort since 1913) to promote competition in the communications industry.

By 1950, AT&T was providing microwave relays in the east. Direct Distance Dialing was available by 1951; a human operator was no longer needed to connect long-distance calls.

While prosecuting AT&T, the DoJ had to cope with a scandal of its own. In March 1949, Judith Conlon, a DoJ employee, was caught ready to hand over confidential FBI documents

to a United Nations employee from the Soviet Union. Conlon was arrested and charged with theft and later with conspiracy for the distribution of secret Department documents. The convictions were subsequently overturned, but the events brought internal security to the attention of outsiders, including Hoover's efforts to have the charges against Conlon dropped, presumably to prevent disclosure of FBI activities. Hoover is said to have instituted new filing procedures, placing FBI reports in separate files, depending on their content and sensitivity.

By 1950, the forest service and certain other emergency and search and rescue operations were beginning to use radio phones on a regular basis.

Continued Controversy Over Government Wiretapping

Left: The Truman Cabinet members and various officials in 1950. President Truman is shown fourth from the right, with Attorney General J. Howard McGrath second from the right and Chairman of the National Security Resources Board, Stuart Symington, sixth from the left around the table. Right: Attorney General McGrath, President Truman, and Defense Secretary Louis Johnson in 1950. McGrath was in favor of strict approval procedures for authorized wiretaps and opposed the practice of wartime interment of immigrant Americans on the basis of race alone. [U.S. Dept. of Education archives (from NARA), public domain, photo on the left by Abbe Rowe.]

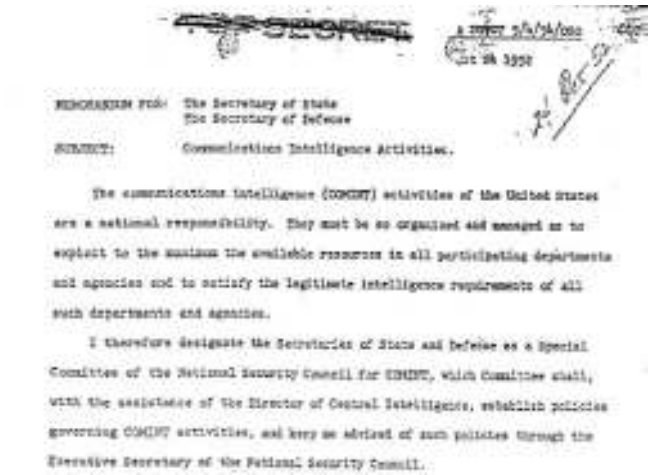
The early 1950s were years of nervous Cold War instability and conflicts in Korea. Public Law 513 was enacted, making it a crime to disclose classified information about American or foreign cryptography systems.

A secret operation called SOLO was initiated by the FBI, in the early 1950s, to monitor CPUSA, the Communist Party of the United States of America. SOLO amassed a large body of sensitive information through several presidential administrations over the next three decades.

Government wiretapping and issues of domestic versus national security continued to be controversial over the next few years.

- In 1950-1951, a Subcommittee on the Investigation of Wiretapping reported to Congress, generating four linear feet of records, now stored in the National Archives.
- In 1950, Presidential Directives authorized the FBI to investigate subversive activity but were not explicit as to how investigations were to be conducted. Government memos from the late 1940s to the late 1950s indicate an internal debate over whether the FBI should be limited to domestic national law enforcement or should be funded for "secret activities abroad."
- Attorney General Francis Biddle turned down applications he felt were not justified. This approval process was made explicit by Howard McGrath, the Attorney General in 1952 [Diffie and Landau, 1998].

- Wiretapping and internal security matters came up again at the December 1953 Legislative Leadership Conference.



MEMORANDUM FOR: The Secretary of State
The Secretary of Defense

SUBJECT: Communications Intelligence Activities.

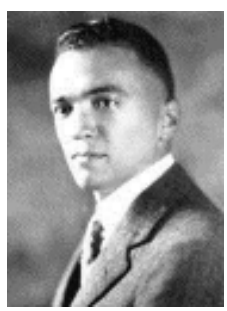
The communications intelligence (COMINT) activities of the United States are a national responsibility. They must be so organized and managed as to exploit to the maximum the available resources in all participating departments and agencies and to satisfy the legitimate intelligence requirements of all such departments and agencies.

I therefore designate the Secretaries of State and Defense as a Special Committee of the National Security Council for COMINT, which Committee shall, with the assistance of the Director of Central Intelligence, establish policies governing COMINT activities, and keep me advised of such policies through the Executive Secretary of the National Security Council.

On 24 October 1952, President Truman issued a Top Secret memorandum to the Secretary of State and the Secretary of Defense establishing a Special Committee of the National Security Council to handle COMINT (communications intelligence), to establish policies and provide advisement to the President. The resulting Directive was to replace NSCID No. 9. (Chapter 1 provides background information on NSCIDs, COMINT, and the NSA.) [NSA eight-page Top Secret, distribution status downgraded per NSC 28 Jan 1981.]

Another important legal case was tried in 1954 in *Irvine v. California*. The case discussed the concealment of listening devices in the walls of a residence. The Court upheld the bugging activities, but the Justices expressed "outrage[d]" at the "indecency of installing a microphone in the bedroom."

In 1954, Attorney General Brownell pressed for warrantless wiretapping to prosecute alleged Communists. The House Judiciary Committee accepted his argument, but the House of Representatives disagreed and no consensus was reached.



Left: In 1917, J. Edgar Hoover became a member of the legal staff with the Department of Justice. In 1924, he became Director of the Bureau of Investigation, retaining the position for almost 48 years. Hoover overhauled the Bureau in its early years and became extraordinarily influential in later years. Right: President Eisenhower decorated J. Edgar Hoover in 1955. Richard M. Nixon, later connected with illegal eavesdropping in Watergate, can be seen standing behind the President to the right. [Hoover portrait copyright expired by date; FBI Web site historical timeline news photos, released.]

In 1956, Hoover briefed the cabinet about Communist efforts to influence civil rights movements. Some of the taps lasted for years, without specific prosecutions associated with the taps. Information that did not contain evidence of criminal activity was retained in files. It has been asserted that Hoover may have wiretapped prominent political figures and several Supreme Court Justices with little oversight of the tapping activities.

In the world of technology in 1956, the U.S. Government and AT&T signed a consent decree that AT&T could only engage in common carrier communications services, excluding them from the computer industry so that competition could be maintained in the emerging industries. AT&T was further required to license the Bell patents on a royalty basis to independents.

Leasing an answering machine from AT&T in the mid-1950s was not inexpensive. It cost the equivalent of about twelve hours' clerical wages per month. In other words, in today's dollars, about $150 per month. That was far too high for the typical home user, but well worth it for a business that was looking for an option to paying secretarial wages. By 1957, AT&T had about 40,000 answering machine subscribers.

In 1957, the Wright Commission recommended federal legislation to support limited and authorized wiretapping that:

> "... would make admissible in a court of law evidence of subversion obtained by wiretapping by authorized Government investigative agencies. Wiretapping would be permissible only by specific authorization of the Attorney General, and only in investigations of particular crimes affecting the security of the Nation."
>
> [Commission on Government Security, "Report of the Commission on Government Security," Washington, D.C., 1957.]

Thomas F. Eagleton presented a report before the Subcommittee on Constitutional Rights opposing legal wiretapping, with records from between 1958 and 1960. His opposition was based largely on constitutional issues of privacy.*

Miniaturization and Emerging Wireless Systems

While American society was sorting out the legal implications of wiretapping, technology was changing dramatically, due to the development of transistor technologies. Small, light electronic parts could now be used to build portable radios, microphones, cheaper mainframe computers, and tiny surveillance devices. At the same time, wireless technologies continued to improve and business owners wanted to build private systems so they wouldn't have to rely on AT&T.

In 1959, private business owners applied to the FCC for permission to build their own private microwave systems. In the *Above 890* decision, the FCC ruled that there was sufficient bandwidth above 890 KHz to serve both private customers and AT&T. This challenge to its monopoly caused AT&T to step up development on its microwave communications systems. Above 890 also opened a crack in the door for entrepreneurs to develop new wireless technologies.

Seeing an opportunity, based on the Above 890 decision, Microwave Communications, Inc. (later MCI) applied to the FCC, in 1963, to build a microwave system between Chicago and St. Louis. They felt they could offer cheaper, better private service than what was available from AT&T. It took six years for the application to be approved, but this was a signifi-

*Papers with respect to this were collected as part of his correspondence between 1957 and 1964 and are housed in the Western Historical Manuscript Collection, Missouri.

cant turning point in the communications industry, introducing competition that would eventually change the position of AT&T and the national telephony infrastructure.

Opposition to Listening Devices

The mid-1960s was a time of opposition to listening devices and an increased scrutiny of FBI wiretapping activities.

Listening devices were becoming smaller and more sophisticated. 'Bugs' were showing up everywhere. Laser listening devices were being prototyped and tested. In one significant case, law enforcement agents had driven a 'spike mike' into a wall under the apartment of a suspect. The wall wasn't punctured, but the vibrations through the building structure provided a good channel for sounds from the rooms that were being monitored. In spite of previous court decisions, in *Silverman v. United States*, the Court ruled in 1961, that the evidence obtained by bugging was inadmissable because it constituted a 'search' that had been carried out without a warrant. This was in spite of the fact that the wall wasn't punctured and no physical trespass had occurred. Thus, the Court took a stronger stand against unauthorized 'search and seizure' and provided a precedent for the protection of privacy.

In 1965, a Senate subcommittee studied electronic surveillance and the photographing of mail covers (envelopes), focusing a major part of their attention on the activities of the FBI. IRS activities were also scrutinized. The FBI was later accused of tapping the members of the subcommittee who were engaged in reviewing the FBI. Senator Edward V. Long was identified by the Bureau as unsympathetic. Not long after, Long was smeared in an article in a prominent magazine, linking him to a gangster. It is said he was pressured into signing a press release written by the FBI asserting that the FBI hadn't participated in uncontrolled tapping or eavesdropping. Long was subsequently defeated by Thomas Eagleton and retired.*

In 1965, Chief Judge Campbell reported to Congress that:

> "My experiences have produced in me a complete repugnance, opposition, and disapproval of wiretapping, regardless of circumstances.... Wiretapping in my opinion is mainly a crutch or shortcut used by inefficient or lazy investigators."

In 1965, Attorney General Katzenbach, under a directive from President Johnson, tightened tapping requirements, imposing time limits on tap authorizations, stating:

> "... the record ought to show that when you talk national security cases, they are not really cases, because as I have said repeatedly, once you put a wiretap on or an illegal device of any kind, the possibilities of prosecution are gone. It is just like a grant of immunity.... I have dismissed cases or failed to bring cases within that area because some of the information did come from wiretaps. But here we feel that the intelligence and the preventive aspect outweigh the desirability of prosecution in rare and exceptional circumstances."

In 1967, a number of bills related to crime syndicates, admissibility in evidence of confessions, and wiretapping were submitted to the U.S. Senate. The President's Commission on Law Enforcement members claimed that a majority supported the authorization of law enforcement agents to use electronic surveillance.

By 1967, the distinction between wiretaps and bugs was disappearing, partly through improvements in technology and partly through subsequent legal decisions. In *Katz v. United States*, it was ruled that people have a reasonable "expectation of privacy" in using a public

*Long responded to the chain of events by telling the story from his perspective in "The Intruders, the Invasion of Privacy by Government and Industry," 1967.

phone booth and a search warrant based on probable cause was required, "...a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." The constitutional basis of the various privacy decisions was being strongly formulated by the growing number of cases related to listening devices.

Shifting the Focus to Law Enforcement

Numerous hearings that were critical of wiretapping were held around this time. Attorney General Ramsey Clark spoke against wiretapping, reflecting the public outcry, except for cases involving national security. He stated "I also think that we make cases effectively without wiretapping or electronic surveillance. I think it may well be that with the commitment of the same manpower to other techniques, even more convictions could be secured, because in terms of manpower, wiretapping, and electronic surveillance is very expensive."

If you have read Chapter 1, you will be aware that national security bodies were not authorized to focus surveillance on 'U.S. Persons,' and that hounding the citizenry was not to be a goal of government intelligence-gathering. However, the FBI and the Department of Justice were concerned with domestic law enforcement and justice, as opposed to national security (the jurisdiction of the NSA), and thus considered intelligence-gathering of domestic activities to be within their mandate. Following this line of reasoning, in 1968, the *Interdivisional Information Unit* (IDIU) was consolidated under the administration of Attorney General Clark. This computerized system included files on organizations and individuals playing a role "purposefully or not, either in instigating or spreading civil disorders, or in preventing our checking them."

In 1968, organized crime was considered a serious problem and a number of studies concluded that the impenetrability of criminal groups justified wiretapping and bugs in law enforcement. The logic was that no specific victim was necessarily involved in these types of cases and that victims might be subject to threats, if they acted as 'stool pigeons' (informants), thus making apprehension and prosecution more difficult than in other types of crimes.

In 1968, the *Omnibus Crime Control and Safe Streets Act* was passed, establishing basic law for criminal investigation interceptions, generally in the cases of violent crimes, gambling, counterfeiting, and the sale of marijuana. It further set out requirements for telecommunications carriers to provide technical assistance and hardware adjustments to their equipment to aid law enforcement agencies in carrying out electronic surveillance, a move that provoked strong opposition that continues today (Title III was amended in 1970). The Act also created the National Institute for Justice, the research and technological development arm of the Department of Justice.

Watergate and The Computer Age

In the early 1970s, Government and press disclosures made it seem as though everyone was bugging everyone and this may have been true. IBM discovered that they had been bugged by Soviet agents. Attorney General Clark discovered, after denying the fact to a judge, that the FBI had been using electronic surveillance. News agencies found out they were being bugged. As soon as the miniature technology became widely available, it appears to have become widely used.

The 1970s are characterized by three important chains of events, one in communications delivery, one in national government, and one in technological development. These were

- the imminent breakup of AT&T,
- the loss of public trust of public officials with the Watergate Scandal, and
- advancing wireless telephony and emerging personal computers.

In 1974, the Department of Justice filed a comprehensive antitrust suit against AT&T, citing illegal actions in perpetuating its monopolistic business practices. The suit called for divestiture of some or all of the Bell Operating Companies and the further divestiture of Western Electric.

In 1974, in connection with the Watergate breakins, Judge John J. Sirica appointed six experts in audio technology to study one of the tapes made by President Richard M. Nixon in 1972. The June recording between H. R. Haldeman and Richard Nixon was obscured at a key point with a buzzing noise for about 18.5 minutes. The erasure appeared to be from a machine other than that on which the tape had been recorded. Investigators concluded that it was probably deliberate erasure produced on a Sony model 800B. By studying the magnetic signature, it was surmised that the erasure was caused by a machine normally operated in Nixon's secretary's office. This is one of the more interesting stories in forensic investigation, as the experts associated with IEEE, a respected electrical engineering organization, used spectrum analysis, waveform analysis, and digital signal-processing equipment to study the magnetic patterns on the tape. They prepared the medium by washing the tape in a fluid containing ferrite particles (which align to the patterns). The IEEE panel findings were presented and subsequently described in the April 1974 issue of *IEEE Spectrum*. The mystery of the content of the tapes was not solved, however.

After a series of laws and amendments, in December 1975, Public Law 94-176 (89 Stat. 1031) established a *National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance* to study and review the operation and provisions of the chapter to determine their effectiveness. This Commission, comprising "competent social scientists, lawyers, and law enforcement officers" was to report to the President and Congress by April 1976.

As far as the communications infrastructure was concerned, AT&T was still fighting hard to maintain its control and market share of the telephone market. In the 1976 *Resale and Shared Use* decision, the FCC permitted unlimited resale and shared use of private line services and facilities. Interstate communication was more closely regulated, however. AT&T entreated Congress and the *Consumer Communications Reform Act* (the "Bell Bill") was enacted. This was possibly the most significant general communications regulation since the Communications Act of 1934 and would have favored AT&T. The issue wasn't fully settled, however, and aspects of the bill continued to be debated well into the 1990s. In a series of decisions called *Execunet*, the U.S. courts opened up the long-distance markets.

New Technologies and Common Carrier Obligations

An important characteristic of the late 1970s and early 1980s was the increasing sophistication and variety of communications and surveillance devices. Wiretapping was no longer the sole issue in the courts. Bugs, pen registers, surveillance cameras, and other devices were filtering out into the marketplace and being adopted by law enforcement agencies.

With technology changing so fast, investigators found themselves at a loss as to how to apply the old laws and procedures to new devices and systems. They entreated Congress and the courts to help.

In *United States v. New York Telephone Co.,* in 1977, the Supreme Court found that telecommunications carriers were responsible for providing assistance to law enforcement agents "to accomplish an electronic interception." The technological details about how this should be achieved were not stipulated at the time. However, continuing improvements in computer technology made it clear that this issue would soon have to be addressed.

Until the age of modern electronics, wiretapping was easy. You chose a phone line, attached a device, and listened. Now it was getting complicated. A person could have more than one phone number; the phones could include a wireline phone, a cordless phone, a traditional cellular phone, or a PCS phone (or all four). The calls could be encrypted or sent over spread-spectrum frequencies to ensure privacy. The phone service might be accessed through several vendors at various times of the week or times of the day. Did the existing laws broadly apply to the new modes of communication?

Privacy advocates, in turn, were concerned that law enforcement agents were using the changes in technology to lobby for increased powers. If wiretapping powers were to be applied to new systems, there was going to be a stronger need than ever before for the communications providers to assist law enforcement officials in carrying out the tapping. Some of these providers had strong moral and financial reasons for opposing this requirement.

Bugs, Wiretapping, and Issues of Entrapment

It is worth pointing out that up to now, the regulations related to bugging and those related to wiretapping, while closely related, are not synonymous. Bugging appears to have been tolerated in some circumstances where wiretapping was not. In spite of this, they yield similar information and are often discussed together.

There have been some arguments as to whether the information obtained by wiretaps can be obtained by other less 'intrusive' methods and counter-arguments (e.g., by Louis Freeh, Director of the FBI) that important information is obtained by taps that can't be obtained any other way. The strongest argument in favor of taps is that the recordings provide strong evidence that is accepted more readily as 'truth' than the remembrances or hearsay of a human eavesdropper. It has also been argued that an electronic device might be less liable to entrap a suspect.

> "But wiretaps and bugs enjoy two advantages over secret informants. First, the evidence they report as to what the defendant did or did not say is trustworthy. Second, and perhaps more important, a bug cannot encourage lawbreaking: It can neither advocate nor condone such conduct....
>
> In any event, for the purpose of my more general argument, it is enough to acknowledge that both legal tests of entrapment–objective and subjective–permit police to employ an enormous amount of routine deception, although the prevailing subjective test permits even more."
>
> [Jerome H. Skolnick, "Deception by Police," *Criminal Justice Ethics,* 1982, Volume 1.]

Skolnick makes an interesting observation here, noting that a bug or wiretap cannot be used to entrap in the same way that a physically present undercover agent might entrap. In the context of Skolnick's argument, this is a good point. In the larger picture, outside of Skolnick's central theme, it would not be an appropriate argument for someone to use to justify the substitution of wiretapping information for that which might be obtained by undercover agents. After all, if entrapment is an issue, a law enforcement agent could use information obtained from a wiretap or bug *to enact a future entrapment* that might not have been possible without the information obtained from the tapping operation in the first place.

In other words, it should be remembered that surveillance techniques are not used in isolation and information obtained from one source is generally combined in a larger body of intelligence with information obtained from other sources.

Surveillance and Civil Rights

A lot of attention was focused on surveillance and information obtained from wiretaps in the late 1970s and early 1980s. This was in part a leftover from the Watergate investigations and in part a consequence of the increasing availability of surveillance devices. It was also a lingering legacy of the Cold War.

At this time, the Soviet Union was undergoing major changes, global commerce was opening up, and the Cold War was winding down. In 1980, Operation SOLO, a long-standing FBI surveillance operation, was terminated. In spite of global changes, Communist fears and general social intolerance were still evident in many of the public statements of Government officials which, in turn, were reflected in decisions about who or what the Government had a responsibility or right to surveil.

Dr. Martin Luther King, Jr. had been assassinated on 4 April 1968, but his name continued to come up again and again in the 1970s and 1980s, in part because of the extensive surveillance and wiretapping of his activities that had occurred while he was alive.

In January 1977, District Justice John Lewis Smith, Jr. ordered the FBI to purge its files of:

> "... all known copies of the recorded tapes, and transcripts thereof, resulting from the FBI's microphonic surveillance, between 1963 and 1968, of the plaintiffs' former president, Martin Luther King, Jr.; and all known copies of the tapes, transcripts and logs resulting from the FBI's telephone wiretapping, between 1963 and 1968, of the plaintiffs' office in Atlanta, Georgia and New York, New York, the home of Martin Luther King, Jr., and places of accommodation occupied by Martin Luther King, Jr....
>
> ... at the expiration of the said ninety (90) day period, the Federal Bureau of Investigation shall deliver to this Court under seal an inventory of said tapes and documents and shall deliver said tapes and documents to the custody of the National Archives and Records Service, to be maintained by the Archivist of the United States under seal for a period of fifty (50) years; and it is further ORDERED that the Archivist of the United States shall take such actions as are necessary to the preservation of said tapes and documents but shall not disclose the tapes or documents, or their contents, except pursuant to a specific Order from a court of competent jurisdiction requiring disclosure."

In 1983, Senator Jesse Helms made a series of inflammatory justifications to Congress regarding Dr. Martin Luther King, Jr., who had now been dead for 15 years. (The following quotes are brief so you are encouraged to read the full Congressional Record and form your own opinions.) In his statements, Helms remarked:

> "Mr. President ... it is important that there be such an examination of the political activities and associations of Dr. Martin Luther King, Jr.... King associated with identified members of the Communist Party of the United States (CPUSA)....
>
> There is no evidence that King himself was a member of the CPUSA or that he was a rigorous adherent of Marxist idealogy or of the Communist Party line...."
>
> [Jesse Helms, 3 October 1983 Congressional Record, Vol. 129, No. 130.]

In his statement, Helms asserted that King was vigorously entreated, by members of the Government, to sever all ties with the Communist sympathizers, which King did not do. He

described how King continued to "address their organizations" and "invite them to his own organizational activities." Since Helms openly stated that King was not campaigning for Communism and was not a "rigorous adherent of Marxist idealogy or of the Communist Party line," it seems that the chief complaint against King was that "he had no strong objection to Communism" and, by implication, could be under their influence.

In public statements, King promoted a global humanity and a free country in which people were entitled to equality and a diversity of opinions, so it's not really surprising that King expressed a liberal view with "no strong objection to Communism." Helms asserted, for this reason, that he was a threat to be monitored and suppressed, and he and other detractors feared that "the Communist Party [would] infiltrate and manipulate King and the civil rights movement."

Those who oppose King's views have drawn parallels between his statements on eliminating racism and inequality with the Communist philosophy. They have generally failed to point out, however, that Communist philosophy and the militaristic Soviet implementation of that philosophy are fundamentally at odds with one another, with a repressive, coercive element that is anathema to most members of our free society, including those involved in civil rights movements. In retrospect, some might argue that criticisms of King were motivated not purely by fears of Communism but also by fears that his philosophy of a "new world order" would upset the traditional lines of power referred to as the 'old boys network' in our own political structure. Either way, it's difficult to assess the full facts in the case if the records are sealed until at least the year 2027, according to the Judicial decree.

Issues of Privacy and Constitutional Rights

By this time, wiretapping was outlawed in most states, but electronic eavesdropping, a more recent technology, was still largely permissible. Before this was sorted out, yet another class of devices was becoming available in the form of portable, wearable transmitters.

In 1963, the Chief Justice of the Supreme Court set the tone for many court decisions of the 'flower power' decade by noting that "... the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; [and] that indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments ...." In *Lopez v. United States* (1963) the entrapment issues inherent in 'wearing a wire' were tested when an IRS agent used a pocket recorder to gather evidence. Since the wire was used in conjunction with the agent's activities, it was held that it was not listening in on conversations that could not otherwise have been heard and since there was no unlawful trespass, there was no instance of unconstitutional eavesdropping.

In 1967, in *Berger v. New York*, in which the plaintiff had been convicted of conspiracy based on eavesdropping evidence obtained from a recording device in an attorney's office, strong arguments were made both for and against the plaintiff. Justice Black offered a dissenting view that in part expressed sympathy for the position of law enforcement officials:

> "Today this country is painfully realizing that evidence of crime is difficult for government to secure. Criminals are shrewd and constantly seek, too often successfully, to conceal their tracks and their outlawry from officers.... In this situation, 'Eavesdroppers,' 'Informers,' and 'Squealers' as they are variously called, are helpful, even though unpopular, agents of law enforcement....
>
> Since eavesdrop evidence obtained by individuals is admissible and helpful, I can perceive no permissible reason for courts to reject it, even when obtained surreptitiously by machines, electronic or otherwise. Certainly evidence picked up and recorded on a

machine is not less trustworthy. In both perception and retention, a machine is more accurate than a human listener....

The superior quality of evidence recorded and transcribed in an electronic device is, of course, no excuse for using it against a defendant if, as the Court, holds, its use violates the Fourth Amendment. If that is true, no amount of common law tradition nor anything else can justify admitting such evidence. But I do not believe the Fourth Amendment, or any other, bans the use of evidence obtained by eavesdropping."

Justice Clark's opinion, on the other hand, was that:

"The claim is that the statute sets up a system of surveillance which involves trespassory intrusion into private, constitutionally protected premises, authorizes 'general searches' for 'more evidence,' and is an invasion of the privilege against self-incrimination.... We have concluded that the language of New York's statute is too broad in its sweep, resulting in a trespassory intrusion into a constitutionally protected area, and is, therefore, violative of the Fourth and Fourteenth Amendments...."

In this ruling, Justice Clark made a distinction between bugs and wiretaps. Justice Douglas concurred with Justice Clark's opinion, stating that:

"... at long last, it overrules *sub silentio Olmstead v. United States,* 277 U.S. 438, and its offspring, and brings wiretapping and other electronic eavesdropping fully within the purview of the Fourth Amendment. I also join the opinion because it condemns electronic surveillance, for its similarity to the general warrants out of which our Revolution sprang and allows a discreet surveillance only on a showing of 'probable cause.' These safeguards are minimal if we are to live under a regime of wiretapping and other electronic surveillance.

Yet there persists my overriding objection to electronic surveillance *viz.,* that it is a search for 'mere evidence' which, as I have maintained on other occasions ... is a violation of the Fourth and Fifth Amendments, no matter with what nicety and precision a warrant may be drawn....

A discreet selective wiretap or electronic 'bugging' is, of course, not rummaging around collecting everything in the particular time and space zone. But even though it is limited in time, it is the greatest of all invasions of privacy. It places a government agent in the bedroom, in the business conference, in the social hour, in the lawyer's office–everywhere and anywhere a 'bug' can be placed.

If a statute were to authorize placing a policeman in every home or office where it was shown that there was probable cause to believe that evidence of crime would be obtained, there is little doubt that it would be struck down as a bald invasion of privacy, far worse than the general warrants prohibited by the Fourth Amendment. I can see no difference between such a statute and one authorizing electronic surveillance which, in effect, places an invisible policeman in the home. If anything, the latter is more offensive because the homeowner is completely unaware of the invasion of privacy.

The traditional wiretap or electronic eavesdropping device constitutes a dragnet, sweeping in all conversations within its scope–without regard of the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime, and intercepts the most intimate of conversations...."

Justice Clark's opinion included

"I would hold that the affidavits on which the judicial order issued in this case did not

constitute a showing of probable cause adequate to justify the authorizing order. The need for particularity and evidence of reliability in the showing required when judicial authorization is sought for the kind of electronic eavesdropping involved in this case is especially great...."

This case has lengthy arguments for and against the constitutionality of eavesdropping and evidence obtained by eavesdropping. The short quotes included here cannot fully convey its import and the judgment is worth reading in its entirety (it can be searched on the Web through http://www.findlaw.com/ and is on file online at Cornell University).

Telephony had continued to spread and evolve. Since the introduction of the Communications Act of 1934, legal interpretations of the regulations varied over the years with regard to wiretapping and related enforcement issues. Law enforcement activities were more specifically set out under the *Omnibus Crime Control and Safe Streets Act of 1968*, Title III. This Act defines the authority and specifies conduct and procedures of wiretaps by federal law enforcement agencies. Most of the states have enacted similar statutes supporting these restrictions. In 1970, the Act was amended to clarify the position and responsibilities of communications service providers for assisting law enforcement agents.

Public Disclosure of SHAMROCK

In November 1975, the *U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities* submitted "Intelligence Activities–The National Security Agency and Fourth Amendment Rights" which discussed an operation called "SHAMROCK" in which communications carriers were persuaded to work in conjunction with government officials. The report says in part:

"SHAMROCK was the cover name given to a message-collection program in which the Government persuaded three international telegraph companies, RCA Global, ITT World Communications, and Western Union International, to make available in various ways certain of their international telegraph traffic to the U.S. Government. For almost 30 years copies of most international telegrams originating in or forwarded through the United States were turned over to the National Security Agency and its predecessor agencies.

As we discuss more fully below, the evidence appears to be that in the midst of the program, the Government's use of the material turned over by the companies changed. At the outset, the purpose apparently was only to extract international telegrams relating to certain foreign targets. Later the Government began to extract the telegrams of certain U.S. citizens.... There is no evidence to suggest that they ever asked what the Government was doing with that material or took steps to make sure the Government did not read the private communications of Americans."

In 1980, operation SOLO, the secret FBI operation that had been initiated in the early 1950s, was publicly disclosed and officially brought to an end.

Techies and Techie Toys

The late 1970s and beyond belonged to a new breed of technologically astute, intelligent, playful software programmers and electronics wizards. Fortunes were made by entrepreneurs, technologists began creating new communications channels, and subtle but significant changes in the fabric of the communications infrastructure were beginning to manifest through computers and computer networks.

In the late 1970s and early 1980s, it became a popular pastime for computer techies to

build 'blue boxes,' handheld devices that could control a touchtone phone (usually a payphone) through tones. Blue boxes were designed to manipulate the phone line electronics to do mischief and make 'free' long-distance calls. Electronics buffs began to build and sell these illegal devices through the computer underground. Blue boxes became popular and the media began to release stories about the devices. It was assumed by the general public that most of the calls placed with blue boxes were made by university students and computer geeks, which was somewhat true, but investigators discovered that a large proportion of blue box thieves were well-paid professionals, including doctors and businessmen.

The significance of blue boxes was three-fold:

- the people who designed them were technologically capable of building various surveillance devices and marketing them as they had the blue boxes,
- the touchtone system through which they operated was shown to be easy to manipulate, and
- the concept of 'hacking' into the phone system could be applied to hacking into the new computer bulletin-board systems (BBSs) that were appearing in communities throughout the developed world.

Blue boxes made communications carriers and electronics designers more acutely aware of the security weaknesses of the existing phone system. Engineers were in the process of incorporating new computer technologies into many types of communications infrastructure systems at the time, including telephone signaling systems, with the result that Signaling System No. 7 (SS7) was introduced in the early 1980s. One difference between earlier systems and SS7 systems was that earlier systems carried the call control (signaling) information and the conversation (or computer data) on the same line. This is called an *in-band* system. SS7, on the other hand, carried the signaling information on a different line from the conversation or other data. This is called an *out-band* or *out-of-band* system. Not only was SS7 designed to be more flexible and powerful than earlier telecommunications systems, but as an out-band system, it was inherently more secure and less vulnerable to manipulation and unauthorized surveillance. In other words, blue boxes don't work on SS7 systems as they did on the older systems and neither do a number of other surveillance devices.

The early 1980s was also the time when many police departments began routinely taping all telephone conversations made on their lines, presumably with notice given to employees. Some departments provided an untapped line for the use of employees for personal calls, though there has been at least one incident [*Amati v. Woodstock* appeal, 1999] in which an untapped line was changed to a tapped line and the employees claimed they were not notified of the change.

By the 1980s, private branch exchange (PBX) phone systems were being equipped with 'back doors' that allowed phone service companies to access the equipment for service or maintenance, a concept that was adapted to software by computer programmers. In some phone systems, this access capability is provided through a DISA port. An external access port could also be used by off-site employees to dial into the system to make outgoing calls through the PBX for work-related communications. Understandably, such a system could be abused by employees committing fraud, or anyone wanting to place long-distance calls without paying the charges.

In the 1980s and 1990s, the digital switching systems began to supersede analog systems in most of the developed nations, and in the mid-1990s consumer 'Internet phones' with a telephone-style handset were able to interface with a computer keyboard to make interna-

tional calls over the Internet for about $.05/minute, probably foreshadowing the next significant change in telephone dynamics, economics, and phone 'tapping.'

The Breakup of AT&T and Implementation of the ECPA

In 1984, Judge Harold Greene divested AT&T of its Bell System regional operating companies. This has become known as the Modified Final Judgment (MFJ). Thus, with the breakup of AT&T and the growth of various independents, the uniformity of services and hardware changed to a proliferation of new technologies and means of providing services. At the same time that this important decision took place, analog technology was gradually changing to digital and wireless communications were beginning to increase in distribution. All of these factors greatly increased the technical expertise needed to surveil audio communications.

In 1986, Congress enacted the *Electronic Communications Privacy Act of 1986* (ECPA) and further amended the Omnibus Crime Control and Safe Streets Act, broadening the terms of the Omnibus Act to include electronic communications.

In the ECPA, Congress acknowledged the capability of technology to intrude on personal privacy. The ECPA extended jurisdiction to wireless and non-voice communications and established rules for the use of pen registers and trap and trace devices in law enforcement. Freedom supporters followed the changes.

> "Most importantly, the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances."

Evolution in Phone Technologies and Call Security

With the growth of computer electronics, voice surveillance became more complex. As technologies evolved and diversified, it became necessary to first determine how the call was being placed (cell phone, PCS, cordless, Internet phone, etc.), and then to find out if the technology chosen was analog or digital (both were now common), and then to further determine whether the communication was being routed, spread, or encrypted, and finally to find an appropriate technology to intercept, decode, or record the conversation. Greater technological complexity sometimes confers greater security. Individuals using newer products do have a greater degree of privacy if the communications are encrypted. Source- or destination-level surveillance, however, is no more secure than before. In other words, fancy routing and decryption don't make the call secure if there's a bug in the pencil sharpener next to the phone or a spy with an ear to the wall.

Challenges for Law Enforcement

In terms of law enforcement, the technological revolution has greatly complicated the process of tapping conversations. Since there are more ways to place a call, there have to be more ways to access the calls. And since there are more ways to encrypt a call, it's more difficult to make 'en route' intercepts and to make any sense of the content of the calls. Phone numbers don't have to be tied to a specific physical address. Greater technical complexity usually results in higher costs for trained personnel and for the appropriate equipment. By the early 1990s, local and federal agencies were finding it hard to keep up with the pace of change and began to lobby for assistance from Congress.

Many users of the new cordless phone technologies assumed that existing wiretapping laws protected cordless conversations. The courts ruled otherwise, however, in 1992 in *United States v. David Lee Smith* by upholding the right of law enforcement to tap a cordless phone without a warrant. This situation was changed two years later when the *Communications*

Assistance for Law Enforcement Act of 1994 (CALEA), Public Law 103-414, required that the warrant requirements of earlier wiretap laws cover cordless phones as well, except in some instances of employers monitoring employee business communications.

The Communications Assistance for Law Enforcement Act (CALEA) was passed by the U.S. Congress in October 1994. This Act required telecommunications providers to assist law enforcement agencies, which meant providers would have to make changes to existing equipment to meet the call taps and trace needs of law enforcement agencies. This reinforced the 1970 Omnibus Crime Control and Safe Streets Act Amendment of 1970 common carrier obligation with the further responsibility to *modify equipment* to fulfill the terms of the Act. The Communications Assistance Act also authorized funds to reimburse direct costs to providers complying with the terms of the Act.

CALEA was an important piece of legislation. In its more specific terms, it required telecommunications providers to have the technical capability to isolate and access realtime calls and call identification information as well as the ability to provide this to law enforcement agencies offsite. However, the Act did not require that the carriers handle decryption except in cases where the target of the call had been provided with an encryption service.

The Recording of Personal Calls

In spite of attempts by developed nations to regulate and address the intricacies of wiretapping and decide who may or may not record conversations, the 'letter of the law' with regard to private citizens recording calls (especially their own) still remains somewhat subject to interpretation. In the U.K., the best answer is that both parties need to be informed of the action. In the U.S., state-by-state statutes differ as to whether one or both parties need to be informed. Clarification often does not come until a case is adjudicated through the court system and, even then, it may require a body of cases to establish the weight of priorities in one direction or another.

In August 1990, Senator Patrick J. Leahy, Chairman of the Senate Judiciary Subcommittee on Technology and the Law hosted a hearing that discussed Caller ID technology. He concluded the ECPA needed to be reviewed due to developments in communications technologies. He appointed a private sector task force which concluded that the new technologies were "challenging the existing statutory scheme for communications privacy."

The 1990s - Changeover to New Technologies

The early 1990s saw another change in hardware that was used to carry wired communications. For decades, copper wire was the medium of choice. By the early 1990s, however, substantial amounts of high-bandwidth optical fiber were beginning to coexist and, in some cases, replace copper wire. The volume and type of communications that were carried over fiber varied somewhat from what was being carried over copper wires and the means by which cable is 'tapped' differs from the tapping of copper wires.

In the mid-1990s, wireless communications and Internet voice capabilities were beginning to come of age. By this time, there were more than a thousand cellular switching networks in the U.S. alone and people were starting to use Internet phone systems to digitally place long-distance calls.

Another concept that began to take hold in the mid-1990s was the idea of 'number portability.' In the past, a phone number was associated with a physical location, just as a house number was associated with the physical location of the land on which the building was situated. With the increase in wireless communications and diversification of the industry, the idea of associating a number with a person rather than with an address, so that person could

receive calls no matter where he or she might be located, began to appear technologically practical. While this would take years to fully implement, it would change audio surveillance technologies in a number of significant ways:

- A phone number would be tied to a person, like a social security number, rather than to an address.
- It might remain the same for the person's lifetime, rather than changing each time he or she moved.
- If people started to wear inexpensive wristwatch-sized wireless phones, the current system of phones might disappear, changing the way phones are tapped and tracked.
- If Global Positioning Systems (GPSs) were built into the tiny phones, the exact location of the person, to within about 60 feet, could be determined.

On the other hand, encryption techniques might become so sophisticated that tapping becomes impossible. That doesn't mean conversations will automatically be as safe as the communications media that carry them; there is still the potential for a conversation to be heard or recorded with tiny bugs. These could be designed to adhere innocuously to the bottom of a shoe, or the back of a lapel or could masquerade as a bird and fly along near a person to amplify and transmit a conversation to someone up to five miles away. Given the increasing sophistication of tiny remote technologies, such devices are now more real than science fiction.

Common Carrier Assistance Obligations

By October 1994, the *Wiretap Access Bill* had passed and was awaiting Presidential approval. This was originally proposed as the *Digital Telephony and Privacy Improvement Act of 1994*. It would legalize authorized surveillance of telecommunications systems and it stirred fears that law enforcement officials might require the common carriers to install systems that could be remotely monitored by law enforcement in a hands-off mode that would reduce the physical presence, and hence the accountability, of officials intercepting the conversations. In other words, in the past, a live phone carrier employee would be somewhat aware of who was tapping what, because they were involved in the activities, and could report anything that seemed out of the ordinary. With remote electronic boxes associated with the system, it would be difficult to establish the same checks and balances.

By 1994, bills were being proposed that would enable law enforcement agents to tap into the new digital communications technologies. On the one had, law enforcement officers argued this wasn't extending their jurisdiction, but rather continuing it in the face of new technologies. On the other hand, a gun-shy public, still sensitized to prior abuses on the part of trusted officials were opposing it. If communications carriers must have systems with tapping capabilities built in, engineers have to design them that way. But obsolescence and unsold goods are a commercial nightmare. Timothy Haight summed the situation up this way:

> "... it's expensive. The Feds have authorized 1/2 a billion dollars to pay for this, but the phone companies say it will cost a lot more... In the future, to avoid expensive retrofits, we can expect phone carriers to build in easy access at the outset. Allowing for wiretapping will become a design principle.
>
> These bills have a chilling effect on designers of technology. Design in security at your own risk. Next year it may be outlawed and you won't be able to sell it...."
>
> [Timothy Haight, "The Punishment of the Wise," *Network Computing*, November, 1994.]

In 1996, the first major overhaul of the Telecommunications Act of 1934 occurred with the *Telecommunications Act of 1996*. This act essentially opened the doors to access and competition within the communications services industry.

Disrobing the Machine - Security Weaknesses

The FCC cited losses of over $400 million to fraud and security problems in 1996. Later that year, prohibitions against eavesdropping on wireless phone transmissions were tested in court in a politically sensitive headline case.

Around December 1996, a couple eavesdropped with a radio scanner on a cellular conference call between John Boehner, Newt Gingrich, and other Republicans discussing a House Ethics Committee investigation. They recorded the wireless call and subsequently turned it over to a Democratic Representative who released it to the media. It was then published in the New York Times. In April 1997, the eavesdroppers were fined $1,010 for violating FCC prohibitions.

In March 1997, Counterpane Systems and U.C. Berkeley jointly announced that their researchers had found a flaw in the privacy protection used in the most advanced digital cellular phones. The group described how an intrusion could be carried out in minutes using a personal computer. A digital scanner could pick up the numbers dialed on the key pad which might include PINs or credit card numbers. Ironically, the announcement came at the same time that legislators were scheduled to hold hearings on the *Security and Freedom Through Encryption* (SAFE) bill. The group criticized the 'closed door' design process as contributing to weaknesses in the resulting security systems associated with cell phones.

Wiretapping in Foreign Nations

Unfortunately, because of the complex legal and social issues associated with communications technology, there is not enough space in this volume to discuss international developments, but it is worth mentioning that not all countries permit wiretapping.

> "Here in Japan, there is no crime problem that would seem to justify wiretapping. Nevertheless, the legalization of wiretapping is being proposed by the Ministry of Justice.... In this context, increased electronic surveillance reveals the state tendency to try to suppress autonomous people's movements by utilizing its police apparatus."
>
> [Toshimaru Ogura, "Japan's Big Brother, The Wiretapping Bill and the Threat to Privacy," *Japan-Asia Quarterly Review,* V.28(1), 1997.]

The Ministry of Justice of Japan was considering permitting very broad wiretapping of telephones, cell phones, fax machines, and computers, upon issuance of a warrant. So it appears that the for-and-against debate is not restricted to the United States.

The Late 1990s - Variation and Sophistication

It hardly seemed possible that electronics evolution could go any faster, but by the late 1990s, the pace was still increasing, and new technologies were entering and exiting the market faster than consumers could figure out their practical applications.

By 1999, the cell phone industry was booming. Eager to provide value-added services in the competition for cell phone subscribers, hardware vendors requested authorization from the FCC to add global positioning system (GPS) capabilities to cell phone handsets. This was seen as a selling point, since the origin of a call could be used to deploy emergency services or to aid a lost caller in getting back on the right track. It could potentially also be interfaced with automobile computer-mapping systems to display local services and phone numbers.

In September 1999, the FCC agreed to allow the cell phone/GPS technology. GPS tech-

nology effectively turns a cell phone into a tracking device. Up to this point, the common way to locate the user of a cell phone was to ask him or her his location or to triangulate the position from the strength of signals reaching cell transceiver stations in the vicinity. Even then, it was only an approximation.

With integrated cell phone/GPS capabilities, not only could a person's location be known, but it could be followed continuously and logged to an accuracy of between 20 and 100 feet, depending on the terrain and speed of movement. While private individuals would probably object to such monitoring, employees using company cell phones might not have a choice and law enforcement officials could theoretically obtain warrants to access tracking information by providing 'just cause' for such an investigation. Even before the ethical aspects were resolved, commercial systems began to sell in mid-2000.

By June 2000, designers, vendors, and telecommunications carriers were required by the terms of the Communications Assistance for Law Enforcement Act (CALEA) to implement systems that would enable law enforcement officials to conduct approved wiretap operations. Implementation since 1994 had been slowed by a variety of technical factors including concerns by the communications carriers that the modifications were too costly and difficult (in spite of government funds allocations). The modifications were further hampered by the concerns of privacy rights activists who argued that FBI jurisdiction was being broadened rather than just maintained with regard to new technologies. In August 1999, the FCC issued a series of technical standards to facilitate the implementation of CALEA.

Increase in Wireless Telephony

By the turn of the century, the number of cellular subscribers exceeded the entire population of Canada. By 2000, AT&T was marketing wireless phone services that functioned in much the same way as regular wired telephone services, without roaming charges or complicated service agreements.

In the mid-1990s, Harris Communications began marketing "Triggerfish," a briefcase-sized device with a headphone jack designed to continuously monitor cellular phones and provide pen register numbers and "intercept documentation" for wiretapping.

With this type of technology proliferating and GPS capabilities being built into newer cellular phones, friends, enemies, competitors, stalkers, and law enforcement officials could listen to your calls, track you, or theoretically pinpoint your location in relation to the scene of a crime. Unlike traditional tapping equipment in which a physical connection may betray the presence of a tap or for which a court authorization is required before physical connections are made, a tapping system for wireless communications is 'invisible' and difficult to detect or monitor, especially after the fact.

Because it was known that scanners could be used to listen to wireless phone calls, the Electronic Communications Privacy Act of 1986 (ECPA) prohibited the monitoring of cell phone communications except for system administration and maintenance and authorized 'wiretapping.' The Triggerfish was thus marketed specifically to law enforcement agents, but that didn't mean there wouldn't be copycat vendors developing similar systems and selling them through the same underground that blue boxes were sold through a few years earlier.

Experts have argued that the best way to secure the privacy of vulnerable communications is through encryption. Spread-spectrum technologies, which move the conversation around through different frequencies, provide an added measure of security. Secure communications that protect the populace pose a continuing dilemma for law enforcement agents, so the debate hasn't ended yet.

Wiretapping, Implementation, and Opposition

In July 1998, the New York Times reported that Louis Freeh, Director of the FBI, had approached members of the Senate Appropriations Committee, asking them to approve an amendment that would

> "... provide police agencies with the precise location of cellular phone users, in some cases without a court order."

Attorney General Reno and the Federal Communications Commission then scheduled a meeting to discuss the FBI's case that "such legislation is needed if the agency is to stay current with an evolving technology that enables criminals to use mobile phones to avoid detection." The technology being proposed was similar to 911 emergency services that could use triangulation to track the location of a cell phone caller. Several privacy groups responded to this announcement by writing to the Senate Appropriations Chair, entreating him to reject the amendment.

Meanwhile, communications carriers were voicing serious concerns about modifying their equipment to comply with law enforcement wiretapping needs. The objections were raised for various reasons, including technological feasibility, cost, obsolescence, timeline and, in some cases, moral grounds related to privacy or law enforcement accountability. The result, in August 1998, was that a suit was filed in District Court by the United States Telephone Association (USTA) on behalf of about 1200 small, medium, and large providers of local telecommunications exchange and access services throughout the country (predominantly wireline). These companies represented over 95% of the nation's local access lines. The suit named the FBI and the Department of Justice (DoJ) as defendants and challenged the regulations requested by the FBI under CALEA. The suit cited problems with the cost-recovery regulations which were supposed to reimburse carriers for the required modifications. The implementation guidelines were described by the claimants as being "arbitrary, capricious ... contrary to law" and in excess of "the FBI's statutory authority."

The implementation deadline was originally set for 25 October 1998. In September, 1998, prominent communications carriers, including AT&T Wireless Services, Inc., Lucent Technologies, Inc., et al., filed a memorandum opinion and order before the FCC and were granted an extension until 30 June 2000 for complying with CALEA.

On 27 August 1999, the Federal Communications Commission (FCC) issued a news release regarding the adoption of technical requirements for wireline, cellular, and broadband Personal Communications Services (PCS) to comply with assistance capability requirements prescribed by the Communications Act for Law Enforcement Act of 1994 (CALEA). It required that the capabilities requested by the Department of Justice (DoJ) and the Federal Bureau of Investigation (FBI) be implemented by wireline, cellular, and broadband PCS carriers. In other words, communications service providers would now be required to implement the Telecommunications Industry Association (TIA) interim standard (J-STD-025) and several "punch list" capabilities as well. The compliance deadline was set as 30 June 2000, with packet-mode communications capabilities to be in place by 30 September 2001.

At the time this was being written, many of these issues are not yet resolved and the body of court cases is not sufficient to provide guidelines in all instances. For further information, consult current Web sites that provide news on these matters and cross-reference the Radio Surveillance chapter for additional information on wireless technologies.

5. Descriptions and Functions

5.a. Listening Devices

Devices that direct or enhance sound vibrations are the most common kinds of listening devices. They provide a more effective path for vibrations to travel from the sound source (or near the source) to the ear or recording microphone or they channel or focus the sound in order to provide acoustic amplification. Some also provide electronic amplification, and the most sophisticated utilize computer processors to selectively choose or improve a sound. Some sound devices are designed to detect specific types of situations and to automatically trigger an alarm or sequence of events. There are five general categories of listening devices:

Sound-detecting devices are those that responds to sound (usually loud sounds). They can be designed to selectively detect the cry of a baby, the sound of an explosion or a bursting pipe, or a car accident at a freeway interchange or traffic intersection. The simplest devices respond to loud sounds or those of a particular frequency. The more sophisticated devices respond to specific types of sound (e.g., screeching brakes followed by a bang). Sound-detecting devices are often hooked up to alarms or other emergency indicators or may be programmed to shut down machinery, heating systems, to freeze traffic lights, or to turn on a camera.

Sound-channeling devices are those that direct sound. They range from water glasses costing a few cents to stethoscopes costing a couple of hundred dollars. They are frequently used to eavesdrop. Sound-channeling devices are also used to help diagnose or monitor traffic flow in digital networks or mechanical linkages in production lines. The flow of data in a digital circuit can sometimes be heard through a device attached to network cables or terminal points. Some technicians are so adept at monitoring the sounds in electrical equipment, that they can aurally detect switching points and traffic flow in banks of telecommunications devices.

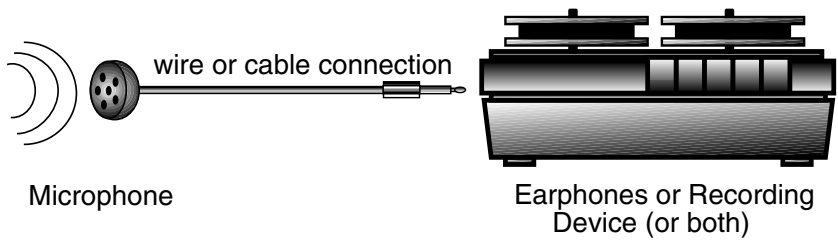
Sound-focusing or acoustical-amplifying devices generally use cone shapes (like megaphones) or parabolic shapes to focus and enhance a sound. They are sometimes used in combination with electronic amplifiers. These range in price from $20 for a simple megaphone-style amplifier to about $500 for hand-held parabolic listening devices. The most sophisticated 'lapel-style' parabolic amplifiers use both acoustics to capture the sound and electronics to amplify the sound, which are more expensive. One common listening device that is often overlooked is a basic hearing aid. With electronic miniaturization, these are now so small, they can be hidden in the ear canal and are almost undetectable if the hair is worn over the ears. They can boost sounds or can be designed to selectively enhance sounds in particular frequency ranges (e.g., to listen to animal sounds).

Electronic sound-focusing and/or amplifiers are devices which capture sounds and transmit them to another location or a recording device and may also increase gain and enhance the volume; some will also improve the quality of the sound through computer processing. Computer-based amplification systems are capable of detecting a specific voice or set of keywords, of analyzing the sound, and of carrying out some complex processing. Electronic and computerized amplifiers/processors can range in price from $100 to thousands of dollars, depending on their features. The more sophisticated systems are usually desktop-based, rather than portable, and are usually used to process recordings made at another location, although van-based listening labs could be employed to process sounds in realtime at a cost of several tens of thousands of dollars. Most electronic 'bugs' are in this electronic category.

Sound converters are devices that respond to a sound and convert the stimulus into another form such as lights, motion, or text. Sound converters are useful in situations where sounds are being monitored by someone who is hearing impaired or who doesn't wish to have sounds in the area where the surveilled signals are being monitored, as in covert surveillance or the monitoring of wildlife that's easily spooked. The sounds of a dog barking, a car honking, an alarm, or a telephone ringing can be converted to a vibration or an illumination. Vibrating devices will sometimes be placed against the spine or the skull to increase bone-conduction and may have connections to earphones. More sophisticated devices can be designed to respond to specific sounds or to screen out ambient sounds (to reduce the chance of false alarms). The more recent programmable devices can be configured to learn to recognize a particular sound (since phones, for example, ring at different frequencies from phone to phone). It is probably only a matter of time before someone programs a listening device that can radio a pager and print a short text message such as "The smoke-alarm is ringing." or "A child is crying."

Microphones

Small microphones can be used to listen to conversations and other sounds and can often be interfaced with public address systems and recording devices. They are usually powered by lithium, AAA, or AA batteries.



Wired microphones. Left: This tiny microphone can be clipped to a lapel or pocket and attached to an amplifier or recording device, from Jing Deng Industrial Co. Ltd. Plug adaptors are available. Middle and Right: These electret condenser microphones are compact, high-sensitivity, omnidirectional, wide frequency-range 1.35-volt units that can be connected with public address systems or recording devices (e.g., for recording a conference), available from Yoga Electronics Co. Ltd. [Classic Concepts diagrams ©2000, used with permission. Supplier information courtesy of http://www.asia.globalsources.com/.]

There are also extra-sensitive piezoelectric subminiature microphones which can pick up sounds to about 20 or 30 feet. Some of these tiny microphones use the same technologies that are used in doctors' stethoscopes. Piezoelectric mics can be used as 'bugs' in walls or decorative furnishings and may be wired or wireless. A stethoscope itself is sometimes used to listen to sounds emanating from the next room by placing it against an adjacent wall. Small

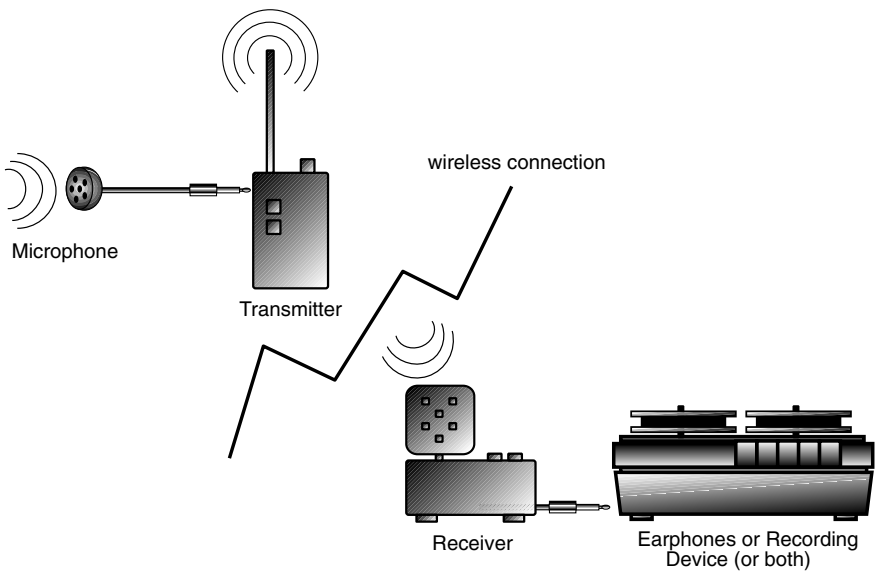
microphones range from $30 to $250.

Audio plug connections come in a variety of sizes and it's important to get one that fits correctly. Adaptors are readily available in electronics stores. Some plugs are monaural and others are stereo (stereo is now more common).

Olympus makes a small telephone recording microphone that can record both voices of a telephone conversation, whether it's a wired phone or a cellular phone. The small device doubles as an earphone for listening to a radio or tape player. Jack sizes (with adaptor) are 2.5 mm and 3.5 mm. The microphone can be used to record to a microcassette recorder. Street price is about $30.

Suction-cup telephone pickups are designed to allow quick-and-dirty recording of a conversation in a location where a direct connection to the line isn't feasible (as on an airport payphone). The suction-base sound pickup is attached to the telephone mouth- or earpiece and connects with a wire that ends in a microphone jack. The jack can be plugged into a recording device or transmitter. The sound clarity isn't especially good, but if it's an important business transaction, a rough recording is probably better than nothing. Kits are about $15, assembled about $30.

BASIC COMPONENTS OF A WIRELESS SYSTEM



Wireless microphones usually transmit on FM, UHF, or VHF frequencies. Frequencies of 900 MHz and 2.4 GHz, which are widely used for short-range video and telephone transmissions, are also becoming more common for small wireless audio transmitters. Wireless microphones come in two basic models, a microphone with a separate transmitter connected by a cable or a microphone and transmitter built into the same housing. Wireless audio devices are often used for body-worn systems, e.g., 'wearing a wire.' [Classic Concepts diagrams ©2000, used with permission.]

Small, unobtrusive, wireless microphones come in a variety of shapes and sizes. Top Left: A tiny microphone which links to an FM transmitter and sends to a receiver up to 100 meters away, from Guangdon Takstar Electronic Co. Ltd. Top Middle: A tiny collar or lapel microphone sold together with a transmitter that can be placed in a pocket or on a belt to send audio to the receiver about 15 to 30 meters away from SCE Company Limited. Top Right: A condenser tie-clip or lapel-clip microphone which is sold separately from the VXM-168LTS wireless transmitter/receiver. Bottom Left: A wireless microphone that runs on AA batteries with 80-12000 Hz frequency response from Hisonic Audios Mfg. Group. Bottom Middle: This compact handheld microphone/transmitter works on a AA battery and weighs 210 grams, from Sekaku Electron Industry Co. Ltd. Bottom Right: This is an omni-directional electret condenser microphone with an FM transmitter/receiver that works in the 110-120 MHz frequency range, from Yoga Electronics Co. Ltd. [Classic Concepts diagrams ©2000, used with permission. Supplier information courtesy of http://www.asia.globalsources.com/.]

Parabolic Microphone

Security, border patrol, military patrolling, wildlife biology, sportscasting, investigative reporting, and private detection are all professions in which parabolic listening devices to amplify sounds within a couple of hundred feet of the listener are used.

Parabolic microphones are sometimes also called 'umbrella' microphones due to their dish-like umbrella shape. They have highly reflective surfaces that use physics to 'capture' the sound and acoustics and electronics to equalize the sound and to actively filter it to produce the effect of amplification. If they are aimed carefully, they can be quite effective at bring the sound 'nearer' to the listener. The sound tends to amplify more at the higher frequencies.

Parabolic microphones are used by the news media to capture sports events, by field biologists and filmmakers to record animal sounds, and by law enforcement agents and private detectives to capture sounds from a distance. Most are portable and run on batteries, though some may have AC adaptors for stationary use. Prices vary from about $200 to $2,000+ depending on the size, model, and sound quality. Miniature versions are now available, but the majority are a foot or two in diameter. The range for common consumer models is about 100 to 250 feet.

Note, when using earphones with sound-amplifying equipment like parabolic microphones, it is important to use earphones or a microphone with a high-decibel shutoff system. This is a system which detects sudden loud noises and screens them out. Otherwise, if you try to use

a normal headphone or earphone, you might either 'blow' the electronics by overloading them or, worse, damage your hearing with a sudden blast of amplified sound.

Left: A parabolic microphone uses a dish shape to collect and direct sound to the electronic components that process the sound and send it to the earphones. Right: A shotgun microphone is designed to pick up distant sounds directly in front of the microphone while minimizing surrounding noises. Both types are usually equipped with 'shutoff' circuits to prevent loud blasts of sound from damaging the hearing of the listener. [Classic Concepts drawings and photo ©1999, used with permission.]

Shotgun Microphone

A shotgun microphone resembles a long wand. It is designed to directionally pick up sound from a distance by attenuating the 'side' sounds. These microphones are used in conjunction with earphones, recorders, and video cameras and are especially popular for newscasting and detective work. They are a little less obvious than the umbrella-shaped parabolic microphones but need a bit of equalization (which also emphasizes unwanted noise) to the sound to get the same 'naturalness' as a parabolic microphone. Good quality shotgun microphones range from about $300 to $500. Small, handheld shotgun mics can be found for under $100.

Laser Listening Devices

A laser listening device is a piece of optical equipment intended to be aimed at a physical structure which is vibrating as a result of sounds near the structure (e.g., people talking inside or outside, near a window). The laser beam hits the structure and the sounds are then reflected back by influencing a change in the character of the beam. *This is a high-precision instrument and is only effective in ideal conditions.* In fact, in testing, the instrument is found to work better if it is focused on the debris and dust clinging to the surface of a window rather than the glass itself. Incidental vibrations from other sources, poor focusing, an incorrect angle, or vibration of the transmitter will all significantly degrade the returning signal.

For example, assume a conversation inside a distant building is being carried out over the noise of a television or radio broadcast, the complex vibrations hitting the window from both the conversation and the broadcast don't produce a 'clean' signal. Another limitation is that the window may be influenced by other vibrations, most often wind or traffic noise, which will confound the speech vibrations. Noise and interference are also likely to occur from poor weather with rain or hail. This is particularly severe if the precipitation is pelting the window. Finally, the conversants need to be near the window and speaking loudly enough to cause the surface to vibrate. If they are standing at the far end of the room and speaking in whispers, it's not likely that anything useful will be picked up by the system.

Laser listening devices come in two basic types:

reflecting laser The laser is aimed at a vibrating object, such as a window, which presumably is vibrating in response to the sounds nearby, such as a conversation. The laser beam hits the window, where it is influenced by the vibrations on the window from the inside, and acts as a 'carrier wave' to transmit the window vibrations back to the receiver.

interferometric laser Many of the limitations and characteristics of a reflecting laser also apply to the more sophisticated interferometric laser. A stable base and a good vibrating surface from which to surveil the sound are essential to its effective use. The precise angle of targeting is also essential as the beam needs to travel back to the exact receiving point in order to 'interfere' with the outgoing beam.

Since sound vibrations travel outward from the source in waves, the communication on one part of the window will be vibrating at a different part in the conversation than another part. As fast as sound travels, it's not instantaneous. Thus, the laser device must be firmly mounted on a very solid, unmoving base in order to precisely pinpoint one area of the window. One other limitation of laser devices is that they only work when aimed at surfaces that are firmly mounted and vibrate readily. Thick walls or moving objects do not make good laser targets. Laser listening devices are sometimes used in conjunction with other types of listening devices.

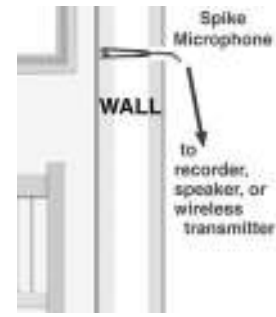
Laser listening devices are precision instruments requiring a tripod or other stable mounting base and are only effective under nearly ideal circumstances with clear line-of-sight, no precipitation, a precise focus and angle, and no interfering sounds. Commercial laser listening devices typically include a transmitter, a receiver, and an amplifier. Because they need to be solidly mounted and focused, they may be hidden inside camera or telescope housings to make them less obvious as listening devices, though there is still a likelihood that a camera aimed at suspect conversants may rouse suspicion. The mounting will usually have headphone/recorder connections and may also have a small speaker or a speaker connection. They are usually battery-powered, weighing about 15 pounds. The laser is usually tuned to the infrared spectrum (approx. 800 mm) in order to be invisible to unaided human eyes.

Sound Conduit Bugs

Sometimes bugs are cleverly installed against 'sound conduits.' In other words, the bug may not be in the room, but may be monitoring the sounds in the room through a heating duct or ventilation shaft some distance away. A metal vent can 'channel' the sound from a room quite well to a location several rooms away. Try talking through a long giftwrap tube to see how well sound will emanate from the far end of a tube or put a metal ruler against your ear and have someone whisper to the other end with his or her mouth close to the ruler. With some experimentation, you can get an understanding of how sound travels through ducts and materials. This, in turn, can aid in determining where someone might try to hide a bug.

Amplifying Microphones

Amplifying microphones are designed to pick up soft noises, whispers, animal sounds, machinery sounds, ticking, etc., in order to make them louder. These can be used to locate stowaways, burrowing animals, fugitives, leaking pipes, tunnels, bombs, and counterfeiting presses. Some amplifying microphones have special automatic 'gain' properties that allow them to boost the sound of a whisper without amplifying the other undesirable noises and loud sounds.



An acoustic listening device can be a simple glass that directs the sound to the ear or a more sophisticated device such as a stethoscope (middle) or contact/spike microphone (right). The Omnibus Crime Control and Safe Streets Act of 1968 has strict restrictions and penalties on listening devices used for unauthorized interception or disclosure. There are some exceptions for consenting parties and administrative or authorized law enforcement interceptions. [Classic Concepts photos ©2000, used with permission.]

5.b. Recording Devices

A recorder is any technology which provides a means to symbolize and imprint physical stimuli or events, so they can be reread or replayed. The more faithful the playback to the original event, the 'better' the recording. A recorder provides a way to document activities and store them for delayed or remote playback. Some recordings are transient or fragile, of only limited use, but most commercial recording devices are reasonably robust. Tapes are somewhat fragile, since the data can be damaged by magnetic interference; the data on newer 'hard' storage media such as CDs or DVDs are less likely to degrade over time.

Recorders are widely used to monitor activities, to provide a record of those activities, or to later analyze or evaluate the activities.

Audio recording is not synonymous with voice recording. Audio recording may include environmental sounds, footsteps, doors opening and closing, switches being thrown, or vehicles coming and going. While this information may not seem significant in itself, in the context of grounds security or an investigation, general activity levels, the timing of activities, or their presence or absence, may be important clues.

The most common recorders are audio and video recorders, though scent, tactile, and motion recorders have many applications, especially in scientific research. A seismograph is an instrument for recording earthquake characteristics and magnitude, but the same technology could be adapted to detect, track, and analyze movements within a building, within a vehicle, or along the ground.

Audio Recording Products

Commercial recording products come in many designs and price ranges, depending on their characteristics and features. As a general rule of thumb, the smaller the unit and the longer the recording times, generally the higher the price (except for professional desktop multitrack recorders). Typically, also, the greater the degree of automation, the higher the price, as they vary from manual to fully automatic. These are the basic types of recorders:

manual The recording occurs only when activated, usually by a human or a tripping mechanism.

manually activated, delayed The recording is manually activated, but delayed (as in setting a timer on a camera that causes the picture to be taken a few moments later).

This allows the person to exit the scene without wasting recording time.

automatic timed The recording unit records on a timed basis, which may be scheduled, delayed, or random. Scheduled recorders may also be set to turn off at a certain time or after a certain interval.

automatic triggered The recording unit records in response to a signal or trigger, such as voice, speech (a particular spoken command), touch, motion, light, or a particular tone. In order to prevent constant on/off recording in a case of a conversation, there is often a built-in delay that the system will continue recording for a few seconds after the sound stops (since it may begin again after a pause).

Analog versus Digital Recorders

Digital recorders are becoming more popular, but are still limited by recording times, unless they are larger units equipped with hard drive storage. Removable PC Cards, similar to those used in digital cameras, can be used to increase recording times on smaller units, but have the same disadvantage as tape–the cards have to be exchanged. At the present time, handheld tape recorders usually record up to about 120 minutes, whereas digital recorders usually record up to about 20 or 60 minutes. With improvements in memory capacity, digital recorders will probably eventually supersede tape-based recorders and provide longer recording times.

Analog recording has the advantages of availability and low cost. Digital recording has the advantages of compression, quick upload to a computer system for storage, and opportunities for immediate or remote analysis of the data. Digital recording also creates an opportunity to edit the data. In the simplest case, unnecessary noise or information may be filtered out. *However, in terms of the integrity and admissibility of the information in court, it is very difficult, and sometimes impossible, to determine if digital data have been 'doctored,' that is, altered to serve the interests of the party doing the recording.*

Now that digital recording devices are becoming less expensive and more sophisticated, there is the probability that programmers will design 'smartcorders' that can selectively play back recordings according to a list of 'rules' based on priorities. Since humans are obsessively concerned with recording everything and since it's impossible to predict what might happen at any given moment in time, we store the recordings because a sound that's insignificant today might be highly significant tomorrow. However, there isn't necessarily a net gain. We may be creating a storage and playback nightmare in which we end up spending more time listening to tapes, managing archives, and searching for information, than being productive and encouraging people to take responsibility for their actions.

How can we alleviate these storage and retrieval problems? One way is to not to make the recordings in the first place. The gain in information (and prosecutions) in some cases may not gain enough to offset the expense, time, storage, and operations costs that are associated with constant monitoring. It's sometimes cheaper to hire a security guard to patrol the premises than to hire a technician to keep the system running and an archivist to swap tapes, put on labels, and manage a library full of recordings. The second way is to create smart recording devices that can prioritize and play back the portions that are more likely to be significant (unusual patterns, schedules, sounds, or sound levels). This may not work in all circumstances, but if it worked in 80% of cases, it could save an enormous amount of clerical work and expense. With digital technologies, the idea is particularly feasible, since a digital recording device can selectively play back specific parts of a recording without winding through a long tape to find it.

Commercial Recorders

Cassette tape recorders are one of the oldest recording technologies, and still one of the most common in covert activities. A high proportion of gathered intelligence arises from verbal communications between individuals recorded on tape.

Portable recorders are usually $25 to $60. Miniature recorders range from about $30 to $400, depending on features. High quality desktop recorders can range from $350 to $5,000, with high-fidelity, multiple-track recorders at the high end.

Many miniature audio recorders are voice-activated, or activated by removing a pen, or other common implement, in order to hide the fact that the recorder has been activated.

Units that record on tape usually advertise the *total recording time*. Keep in mind that the *unattended* recording time is usually half of that claim. That is, if the manufacturer claims six hours of recording, it usually means turning over the tape after three hours. Some units are equipped to record on both sides without handling the tape, but these are in the minority and are usually a little bigger to accommodate the extra mechanisms. They also tend to be more expensive.

Left: This portable desk recorder begins to record automatically when the call is initiated. It has two speeds to provide longer recording times and works on AC or DC power. It decodes a number that has been dialed and records the information on the tape. Lelux Electronics Ltd. Middle: A palm-sized message recorder with LCD status display and timer alarm can randomly search and delete recorded messages. Headphones, external microphone, and IC memory cards are options. CASIL Research & Devel. Co. Ltd. Right: This tiny keychain digital recorder uses 4 button-cell batteries and records up to eight seconds for quick messages or important reminders. CASIL Research & Devel. Co. Ltd. [Classic Concepts ©2000, used with permission. Supplier information courtesy http://www.globalsources.com/.]

Telephone-answering machines are one of the most common devices used to record phone calls. They are equipped with a variety of features, including the ability to decode outgoing phone numbers and store them on the tape along with the recording or, if the Caller ID service is available, to store incoming numbers in association with the message. Time and date functions are usually supported. These features make it possible to create a record of business transactions, without having to type or handwrite notes about the time or party called.

Digital tape recorders are becoming more popular, but are still limited by recording times, unless they are larger units equipped with hard drive storage. Removable PC Cards, similar to those used in digital cameras, could be used to increase recording times on smaller units, the disadvantage being that they have to be manually exchanged.

Analog recording has the advantages of low cost and wide distribution. Digital recording has the advantages of compression, quick upload to a computer system for storage, and opportunities for analysis of the data. Digital recording also creates an opportunity to edit the

data. In the simplest sense, unnecessary noise or information may be filtered out. In fact, many of the new tiny recorders have computer interfaces. You could theoretically upload the data, shuffle it around, delete, insert, and reload it to the recorder.

Many miniature audio recorders are voice-activated, or activated by removing a pen, or other common implement, in order to not call attention to the fact that the recorder has been activated. Others are hidden inside calculators, cell phones, pencil sharpeners, smoke detectors, clocks, and pagers.

Left: The Samsung SVR-P700 digital pen recorder weighs 41 grams and uses a AAA battery which lasts about 4 hours. It will record up to 70 minutes on flash memory and interfaces with other electronic devices. It can be reviewed with an earphone. The street price is around $200. Middle: This digital pen recorder looks like a gunmetal business pen and comes in models to record 40 or 20 seconds in two channels or 10 seconds of audio. Union Electric Corp. Right: The Samsung Voice Stick digital recorder records up to about 4 hours on 8 MB flash memory cards and is PC-compatible with a high-res LCD display for about $200. The voice-activated Micro-bar digital audio/phone/cell phone recorder with up to 8 hours recording is around $600. [Classic Concepts diagrams ©2000, used with permission. Supplier information courtesy http://www.globalsources.com/.]

Remote Monitoring through a Phone Line

There are also systems that use the remote telephone itself as the listening device. In other words, you can attach a device to the phone line, call the number and listen to a conversation going on in the vicinity of the phone that was called or the device itself, if it is self-contained. Some of these systems will even defeat the ringer so that people at the remote location don't know that a phone call has come through and are not aware that the sounds in the room are being monitored. They can further be used to monitor the conversations of someone who has just hung up the phone. The listening range is usually up to about 20 to 30 feet from the phone depending on the design of the room and other ambient noises. These systems generally require that a device be attached to the remote phone line, necessitating access to the premises. There are legitimate and illegitimate uses of this technology. Some people use them to monitor a business after hours or to check on the activities of teenagers who have been left at home for a short while.

A similar device is a phone-hold monitor. This device monitors a remote phone conversation, but only when the hold button has been pressed at the other end. Since people often comment on the conversation at hand while on hold, the phone-hold tap can be revealing.

Most recorders work off the telephone power source, making them detectable by normal bug-sweeping procedures. They retail for about $200 to $500 with the more expensive units capable of monitoring more than one line. Many are self-contained, resembling a telephone junction box, and do not require a telephone (just a live telephone line) for operation.

When an audio or video recorder is placed covertly on a human, it is called 'wearing a wire' or 'being wired.'

Recorder Accessories

Switches that allow a regular tape recorder to be sound-activated can be purchased in kit form for about $10. They usually interface through the remote plug on the recorder.

5.c. Monitoring Phone Communications

Wiretapping involves the use of a device to access a conversation at some point in the physical connection related to the call, traditionally through a phone wire or cable. In recent years, the term is used more generically to include eavesdropping on both wired and wireless communications. The tools to tap a conversation have become more varied and sophisticated as electronic technologies provide ever-increasing ways to communicate using wires or radio waves in various forms.

Personal and business recording of phone conversations typically occurs at or near the phone being monitored, since the activity is usually consensual or illegal. Law enforcement tapping typically occurs adjacent the premises (in order to avoid issues of illegal trespass, search, or seizure) or at the local phone switching station (with the cooperation of the communications carrier).

The telephone in its most basic sense consists of two speaking/listening devices connected to each other by a string or wire, or other filament capable of conducting sound. For many years telephones were not much more than a power-amplified enhancement of this basic scheme. Thus, it doesn't take much effort or sophistication to attach a third listening device somewhere along the length of the conducting wire, to listen to the conversation at hand or to use a tape recorder to record it. This is the essence of phone tapping.

Pen Registers

The evolution of electronics has opened the door to other types of 'taps.' Sometimes the eavesdropper isn't listening to the content of the conversation, but rather is interested in who is being called or where or when. Since the advent of touchtone phones, this information is easy to determine, and there are handheld acoustical phone decoders (pen registers) that will log and display the numbers that are being called from a selected phone. Pen registers are used in business and law enforcement activities.

Communications Logging Devices

A logging device is one that keeps statistics on various aspects of calls, including the time, date, and duration of the calls. High-end pen registers, called pen register/loggers, sometimes have this information in addition to the numbers dialed. Some of these units can be combined with CallerID services to provide additional information.

Basic Telephone Listening and Recording Devices

Analog phone technology, at its heart, is not complex, so listening to or *tapping* a phone conversation often doesn't involve high cost or complicated equipment. The conversations that occur on most systems consist of 'raw data,' words that are not scrambled or coded or spread over several frequencies. However, as phone technologies become increasingly digital (and increasingly wireless), tapping becomes more difficult. Digital technologies allow more opportunities for encryption and transmissions that can hide, obscure, or scramble the conversations.

The most common form of phone voice recorder is the pervasive telephone answering machine. Most answering machines will record two sides of an ongoing conversation simply by activating the record mode or memo mode with the touch of a button. There are laws protecting conversants from covert recording, so many answering machines are equipped with

beeping tones to inform the person on the other line that the call is being recorded. In some regions one party must consent to the recording; in other regions, both parties must consent.

Some units have an option to disable the beep, as the beep is annoying if it is a legitimate call and both parties have agreed to the recording (e.g., a long-distance business transaction).

Wiretapping Devices

Some wiretaps are set up at the local switching office with the assistance of the service provider, but other (usually illegal) taps occur in the vicinity of the phone being tapped. Taps also occur legally in work environments at the discretion of a business owner.

Most nonanswering-machine sound recorders consist of a control circuit, which is either integrated into the recording device or housed in a separate box, and a transmitting or recording mechanism. These are essentially wiretapping devices. Most of the lower-priced consumer units are configured for single-line phones. Sometimes the control circuit and recording unit are integrated into the phone itself. Most voice recording units are advertised for their 'silent operation,' that is, no beeping tones are emitted while the call is taking place. Prices range from $25 to $300+. Units with good sound quality, dual-speed, long-play, and voice-activation features are in the $150 to $250 range. Those with extra features, such as call logging and enhanced CallerID displays are in the $300+ range.

Most wiretapping devices connect in series with the phone line, but there are some activating mechanisms that are connected in parallel. Some taps are not physically connected to the line. They are connected just adjacent to the line (or surrounding the line without touching it) and pick up electrical emanations from the line. This requires sophisticated equipment with noise filtering and gain to clean up and amplify the signal. The quality of the sound may not be as good as regular wiretapping devices, but the chance of detection is much lower and less expensive tap-defeating systems do not affect them.

Premium units that only record when actual conversation takes place, rather than during the entire duration of the call, provide longer recording times. Longer recording times can also be accomplished with combination digital/analog systems, where there is a digital buffer for the conversation which is then stored to analog tape without the long gaps or pauses that are common to conversations. Hybrid digital/analog systems can also interpret the touch tones to intercept and record the number dialed, and display them to a visual display incorporated into the unit, similar to a CallerID display. When hooked into a computer system, a high-end voice recording system can include databasing of the conversations, voice stress analysis, and other evaluations of the data. With banks of high-capacity storage devices, virtually unlimited recording is feasible.

A basic voice-recording model comprises a cigarette-package-sized box with a power switch, RCA audio jacks to hook to a recording device, and an RJ-11 phone jack to connect to the phone line. Longer recording times are possible with some simple modifications to the drive mechanisms of many recorders. Some systems are configured with two or three recording speeds. Slower speeds usually result in lower quality audio. Most tape-based surveillance units will record from one to twelve hours. Digital microcassette units usually record from 10 minutes to about an hour. Computer peripheral units usually connect through RS-serial or USB interfaces.

Most phone voice recorders are designed for analog systems, and are generally only able to detect a single line. Depending on the location of the unit they may or may not record calls taken on extension phones to that line. Thus, many of them don't operate on private branch exchange (PBX) lines in offices and institutions. To overcome this limitation, there are inex-

pensive units that connect between the phone and the handset to monitor the specific call taking place. Since these units can be seen by passersby, they are not suitable for covert recording.

Another device for digital PBX and other multiline systems is an adaptor that converts the signal from digital to analog, thus allowing recording devices, modems, and other analog equipment to be used. Adaptors are small enough to fit in carry-on luggage or in a laptop carrying case pocket, and sell in the $140 range.

The simplest phone taps include two leads that are hooked directly to the phone line on the one end, and attached to a listening device on the other end (like an earpiece or headset). A telephone lineworker's test set, which looks like a telephone handset with a dial and two wires hanging out, is a common piece of equipment that can be purchased almost anywhere. The test set can be connected to a phone box to monitor an ongoing conversation. Phone taps can be designed to record the conversation to an attached recorder, usually a simple cassette recorder, or can transmit the conversation without wires to a listener nearby, such as a receiver in a van half a block away, not unlike the 'spy vans' commonly seen on television shows. A surveillance van is usually equipped with a high quality antenna (sometimes several antennas) to intercept the signal.

As with all listening devices, there are ways of detecting that the phone is being tapped, and there is always the possibility, if the conversation is transmitted elsewhere, that some ham radio buff in his attic or basement may pick up the signal and blow the whistle on the eavesdropper.

Wiretap Accessories

It is possible to build components which attach to the remote and microphone jacks of standard or miniature tape recorders to cause the tape recorders to automatically start recording when the phone is picked up. Kit price is about $22.

Audio Transmitters

Wireless transmitters are those which convert the audio into radio signals and back to audio again at the receiving end. FM transmitters are attached to the phone line or hidden inside the phone. Most of the line transmitters are connected in series to one of the two copper wires that typically attach to a phone. The phone line is both the aerial and the power source (which makes it vulnerable to detection). These usually transmit from about 100 to 300 feet. An FM receiver tuned to the same frequency is needed to receive the signal. Kits sell for about $20 for both the transmitter and receiver. Longer range transmitter kits with tunable frequencies are about $30.

Sound transmitters are microphone/transmitting units that are essentially the same as intercom systems. They can be one-way or two-way, wired, wireless, or fiber optic. Wireless systems sometimes use the building wiring as an aerial. Intercoms are usually about $30 and kits, which may be smaller and less visible, about $20.

Basic fiber optic audio links consist of a microphone, a length of fiber-optic cable, and a speaker or connection to a recording device. While the microphone will still generate electrical disturbances, the cable itself does not and thus is less vulnerable to detection than electrical cable systems. Distance depends on the construction/style of the cable. Kits are about $35. Two-way fiber-optic system kits are about $62.

Stethoscope-style transmitters are based on the idea of using the listening portion of a stethoscope (the sensitive endpiece) in a suction-cup shape so it can be fastened on outer surfaces without entering a premises. It includes a transmitter (usually FM) to transmit up to about 500 feet.

Watch phones like those depicted in spy comics in the 1960s are now a reality. Tiny programmable phones that are worn on the wrist with digital displays that provide about 90 minutes of conversation and about 60 hours of standby are being distributed by Samsung featuring speech-recognition technology by Conversa, a Redmond-based company. [Conversa news photo 2000, released.]

Video and Digital Recorders

Video camcorders can be used as audio surveillance devices when other more specialized audio devices aren't available. The lens cap can be left on if video is not desired. Recordings on video tape have good quality sound and can be further enhanced by attaching a quality condenser microphone, parabolic antenna, or wireless audio receiver to the camcorder through a connecting cable.

5.d. Audio Changing or Jamming Devices

Sometimes confusing a bug is easier than finding and disabling it. Devices that protect against audio eavesdropping in this way usually consist of devices that generate a range of frequencies that run through the human audio spectrum to 'muddle' the vibrations and disturb any audio receivers that may be monitoring the location. The lower frequency usually starts around 5 to 20 kHz and the upper frequency is usually around 1,300 to 20,000 KHz (human hearing is about 20 to 18,000 KHz, depending on the age of the subject).

5.e. Institutional Phone Tapping

In movies and television shows, detectives and government agents are commonly shown tapping into personal and criminal conversations from receiving units in vans and stakeouts in abandoned buildings. In actual fact, there is a lot of paperwork involved in getting permission to tap. Timing is also of considerable importance in wiretapping for law enforcement purposes as permission to tap is specifically restricted to certain types of alleged crimes, usually violet crimes and drug-trafficking-related crimes. These crimes can often take two to five years to 'crack,' whereas permission to tap may last about 30 days. (See the history section in this chapter for the regulations and debates about the legality of wiretapping.)

In order to tap, law enforcement agents must go through a process more complicated than obtaining a general search warrant. In general, they must:

- obtain approval by the Attorney General, or his or her current acting agent,
- apply to a local U.S. Attorney to apply to the appropriate court,
- provide very specific information in the wiretap request. It must not only show probable cause for the tapping operation, but also must list some specific terms such as the identity of the person or persons being tapped, the location of the tap (with exceptions for roaming conversations), and even the types of conversations that might be expected to be accessed, and
- turn off monitoring if there are lengthy conversations on topics unrelated to the investigation.

All these precautions are in place because the tapping of a phone intrudes not just on the privacy of the suspect, who may be discussing issues unrelated to the suspected crime (and who is innocent until proven guilty), but also invades the privacy of the other people with whom the suspect is conversing, who may be innocent of any wrongdoing.

Once a law enforcement agency has permission to tap, the process is not over. It is usually necessary for the law enforcement agency and the phone service personnel to cooperate in establishing a tap, especially now that electronics have become more varied and complicated. With dozens of new ways to place calls on cell phones, Internet phones, and radio-based personal relay technologies, the technical challenges of tapping a call have greatly increased. Spread-spectrum phones also make it more difficult to access a conversation in progress, because the frequencies are changed and may further be encrypted. These systems are less vulnerable to both jamming and eavesdropping and they are now available to consumers for under $150.

Phone Conversations - Tracing a Call

Sometimes the source of a message is as important as, or more important than, the content of a message. 'Tracing' a line is another aspect of telephone surveillance which is commonly depicted in films and TV. Tracing involves identifying the source of the call. The methods for tracing wired communications are somewhat different from tracing wireless communications.

Prevalence of Law Enforcement Taps

The U.S. Department of Justice Criminal Division reviews a little over 1,000 wiretaps per year and provides assistance to federal enforcement agencies on the use of emerging technologies. The number of taps per year has increased very gradually over the last decade or so, but the increase is not statistically significant in relation to the increase in population in the U.S. The number of calls monitored with each tapping authorization varies greatly but may reach as high as 2,000. Historically, law enforcement has also contracted to outside detective agencies for various surveillance services and there are no records of how much information obtained from private detectives may be from tapping or bugging activities, if any.

There are two exceptions to the typical wiretap authorization requirements. The President can, following a declaration of war, authorize a wiretap for foreign intelligence for up to fifteen days without a court order through the Attorney General. Also, if the communications are exclusively between foreign powers or involve intelligence other than spoken communications from a location under the exclusive control of a foreign power there may be some leeway in tapping. (As the economy and politics of the world become more global, it is almost certain that U.S.-initiated foreign taps will be scrutinized and criticized by allies and other nations.)

At the present time, the Attorney General must inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence of all wiretap activity. The information is classified, but the Attorney General must provide the Administrative Office of the United States Courts with an annual report.

Who Gets Tapped?

Two-thirds of court-authorized law enforcement taps are related to drug-trafficking operations. The other third is mostly related to investigations of wide-scale fraud, such as Medicare/Medicaid scams, military-contractor fraud, and situations in which law enforcement officers or politicians are found to be involved in illegal schemes. Wiretaps lead to just over 1,000 convictions per year, an average of about one conviction per non-FISA tap.

In the mid-1990s, the average cost of installation and monitoring of an institutional wiretap was almost $70,000.

An individual or corporate spy can probably find out what she or he wants to know through just listening in to phone conversations, but law enforcement agents need concrete evidence. They have to record the calls for the wiretap information to be useful in court. The calls must be recorded so there is no doubt as to its source or authenticity and no indication that the information has been altered in any way.

Given all this bureaucratic procedure, it is far more likely that you are being tapped by your Little Brothers: friends, neighbors, or business competitors, than by law enforcement agents. It is pretty easy for a neighbor to listen in to conversations on a party line or through a radio phone tuned to the same frequency as your cordless phone, or for a kid down the street to hook into your external line with parts from a new electronics kit he got for his birthday, or for an ex-spouse to attach an illegal tap to your line that was purchased for a few dollars on the Internet. In fact, in many cases, employers can legally tap into your calls at work with nothing more than a brief memo or mention that she or he might be 'monitoring' employee calls.

5.f. Covert Listening Device Countermeasures

People involved in high stakes activities, e.g., business deals, often suspect that they are being bugged, even when they aren't. People having relationship problems sometimes bug one another. Criminals seeking to avoid law enforcement agents sometimes use bugs, taps, and radio scans to monitor their movements to avoid capture. Criminals sometimes also bug a location in order to 'case the joint,' that is, to gather information, to determine when to enter the building without being detected or when security personnel are absent.

If there is reason to believe there are covert listening devices installed in a building or vehicle, there are a number of steps that can be taken to try to locate the bugs. Some people choose to hire a professional technical surveillance consultant who usually has the equipment to search for a variety of types of bugs; others try to do it themselves.

Success in detecting listening devices depends in part on making some good guesses on the type of device that is being used. Since most covert devices are electronic 'bugs' or wiretaps, most of the detection devices that are available are designed to locate changes in the electrical properties of a wireline, transmissions through the air, or electrical anomalies in the vicinity of an eavesdropping device. The process of locating bugs is called *bug sweeping* since many devices are swept through the air in much the same way that a metal detector is often swept back and forth along the ground.

Bug sweepers vary in type and sophistication. Some can only detect a bug when it is transmitting and are essentially scanners that seek a stronger signal within a range of frequencies, a pretty limited type of device, but since many bugs are purchased as hobby kits or through Internet dealers, they share common design features. These consumer bugs tend to send out signals that are in the standard FM broadcast bands or just below the frequencies of the standard FM broadcast bands. Knowing this makes it easier to detect this common type of bug. (There is more information about wireless transmitters/receivers and common broadcast frequencies in the Radio Surveillance chapter.)

Detecting Bugs

Because of legal restrictions and FCC requirements, the majority of audio transmitting devices that are used as small 'bugs' transmit in the FM broadcast ranges. Frequencies around 73 MHz are common. The biggest disadvantage of these as covert devices is that the trans-

mission can be picked up by anyone scanning through channels on an FM radio or specialized receiver within the range of the transmitter. Transmitters which are designed for 'educational purposes' as electronics kits or from schematics or which are being used illegally to eavesdrop sometimes include FM transmitters that use frequencies outside the regular broadcast ranges. These require a special scanner or receiver tuned to the corresponding frequency. Nonbroadcast frequencies are less likely to be accessed by someone carrying a 'boom box' nearby, but they can be picked up by a nearby FM scanner. Since FM transmitters send a signal in all directions, they are highly vulnerable to detection.

Other frequencies that are typical include VHF, around 180 MHz (±50), and UHF, around 650 MHz (±300) with FM modulation.

There is a 'metalevel' of thinking that a lot of people overlook in surveillance and countersurveillance activities. Never forget that solving an eavesdropping puzzle is solving a logic puzzle and a psychology puzzle. Physically hunting for the bug isn't necessarily the best way to find it. Getting the person in the room responsible for planting a bug and watching their eye movements, or where they ask you to sit can be clues. Checking credit card statements for recent purchases from electronics retailers can be another. If you find out what type of devices the vendor sells, it's easier to choose the right type of bug-sweeping device (note, the legality of these actions varies with the circumstances). Many people shout 'hallelujah' with relief on finding a bug and overlook that fact that there may be others (or that they can be reinstalled). Never assume there is only one bug and never assume that multiple bugs are of the same type. Be suspicious of renovations, empty rooms next to a room that is suspected of being bugged, or furniture that has been shifted.

Because bugs may be difficult to find, some people choose to counter a bug, not by removing it, but by defeating its acoustical properties. Voice changers, voice scramblers, and noise generators are devices that alter or confuse the local sounds to make it difficult for them to be recorded or interpreted. High frequency radio waves can be used to temporarily or permanently disrupt nearby electronic devices (not feasible if sensitive components are nearby). Other people simply look for wide open spaces in which to carry out confidential conversations, like golf courses (and then make the mistake of hiring a questionable caddy or renting a bugged golf cart).

Sometimes metal-detecting wands and physical 'pat-down' searches are used to see if someone is 'wearing a wire' when entering a premises or the area where a transaction is about to take place. Public transportation systems (e.g., airlines) now routinely use walk-through access devices and wands to detect bombs and other weapons, but these devices can sometimes also be used to detect body-worn bugs and recording devices.

Detecting a bug that is hidden in a building or vehicle is generally a four-step process consisting of:

- making some common-sense preliminary guesses on where the bugs might be and what type they might be (if you're wrong, you back up and try other strategies)
- doing a preliminary visual search for changes or unusual aspects to the premises or vehicle (new paint, a small pile of dust, a crooked picture)
- discerning the frequency on which it is transmitting (wireless bug) or anomalies in the electrical signal strength or characteristics of the transmission (wireline bug), and
- finding the actual location of the bug or wiretap.

One type of bug that is more difficult to detect by these methods is a 'light bug' or fiber optic device. Light doesn't emanate from a cable in the same way that electricity emanates from a cable. The weak point of fiber optic devices is that the cable itself has to be hidden somewhere and simple visual inspection, various ultraviolet lights, penetrating X-rays or other surveillance devices may detect the physical presence of a cable under a carpet, in a wall, or above the ceiling tiles (a very common place to run wires). Another light device is an infrared transmitter/receiver. Infrared transmitters can be designed to convert sound to light and the receiver can turn the signal back into sound again through a device that is worn or held near the head and which may have an earphone for quiet or covert listening. Such devices exist for the hearing-impaired and might also be appropriate for certain covert operations. These devices have three limitations: they are limited in range, they require an unobstructed line of sight, and the beam can be detected with an infrared sensor. They are useful, however, in noncovert surveillance in which radio waves are not an option (perhaps because of interference) and a clear line of sight is available.

A test sound is often generated in an area that is being swept for bugs to stimulate the microphone into electrical activity in order to detect its presence or measure its properties. Handheld computers are sometimes used in conjunction with bug sweepers to display statistics or mathematically analyze phase differences that can aid in finding the actual location of the bug.

Wiretap Countermeasures

There are a large variety of devices designed to detect wiretaps and bugs. In traditional landline phone conversations, the phone is powered by the line itself. Many tapping devices will use power from this line and the slight effect on the power in the line can be detected with the right equipment. Newer or more expensive tap devices are designed to create a minimum disturbance to the line to which they are attached. Bugs are usually powered by batteries.

A general understanding of phone system wiring and accessories is helpful in locating telephone taps. Many taps masquerade as common consumer jacks and accessories or are built into standard store-bought accessories.

Many telephone 'inside-premises' tapping devices are either built to look like normal phone accessories or they are hidden inside standard working phone accessories. These diagrams show some that are particularly vulnerable to tampering. Wall plates can be removed, the wiring altered, and replaced. Phone bugs are now so small, they can be hidden inside standard splitters and adaptors. Junction boxes and bell ringers are easy receptacles for hiding bugs, as they have room to spare and tampering is rarely noticed. [Classic Concepts photos copyright 1999, used with permission.]

Frequency counters, bug-sweeping devices for seeking out wireless transmitters are available as portable *scanners*, capable of scanning through a wide range of frequencies. Some come with LCD indicators, others with status lights. More sophisticated models can also keep a log of time and date and location through GPS and many personal computer interfaces.

More expensive models usually scan over a wider range of frequencies.

Bug detection kits will often come with a variety of swappable sensors, called *sondes* to detect radio waves, infrared radiation, etc. More sophisticated systems with computerized readouts may require technical expertise to interpret the information. Professional systems will sweep through a wider range of frequencies, some as high as 4.5 GHz and can detect scrambled signals or spread-spectrum transmissions. They check for AM/FM radio transmissions, sub-carrier, carrier-only, SBB, and DSBSC signals. Most consumer models sweep up to about 2.4 GHz and may not be able to detect spread-spectrum transmissions.

High-end tap-detecting systems are significantly more powerful and versatile than most of the consumer bug-sweeping devices. Since the majority of taps are unsophisticated, they are not especially difficult to detect with experience and basic equipment. However, there are circumstances where the tap is miles from the premises and designed to be difficult to detect. It is difficult to physically trace the connection to this type of wiretap and it is sometimes necessary to use diagnostic equipment that can trace the phone line status from the premises all the way to the local telephone provider. This type of equipment can also detect anomalies at the junction boxes without physically inspecting them (though an inspection is recommended, whenever possible). But even with these devices, there are limitations in trying to trace a line that is within a private branch exchange (PBX). For these, the status of the lines inside the exchange has to be tested and then the status of the lines leading into the exchange must also be tested. The price range for more sophisticated bug detectors is from $1,000 to $4,000.

Telephone handsets and telephone answering machines can also harbor bugs and taps. The mouth and earpieces of the older rotary phones are easy to unscrew in order to insert bugs. Deskset phones are usually accessible by screws in the bottom. Telephone answering machines can be readily opened and modified or equipped with a bug. [Classic Concepts photos ©1997, used with permission.]

Some cellular phones are now being equipped with detectors for transmitters that will sound a tone or cause the phone to vibrate to indicate there might be a bug nearby.

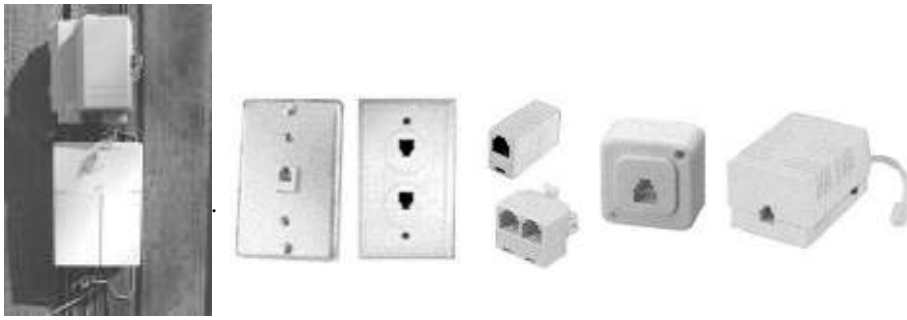
There are telephone 'guard' systems that are designed to detect and react to anomalies on the phone line, deactivating not only a large number of common wiretap devices but also deactivating the automatic recording feature on many phone recorders. Most of these systems are based on an electrical activity 'reference' and thus must be calibrated to a line when installed in order to detect future anomalies.

Warning Signs

How can you find out if your phone is bugged? There are general warning signs and specific measures you can take to prevent bugging.

- The first warning is if people seem to know things they shouldn't. This is not an electronic countermeasure, it's a common-sense countermeasure.

- Are there changes in the phone line while you are engaged in conversation? These can include unusual sounds, volume changes, popping noises, static or sound emanating from the phone when it's not in use.
- Do you get calls where the phone rings, but no one is on the line and you hear unusual sounds?
- If you have a radio near the phone that acts strangely, there may be a bug in the vicinity of the radio (or television).



Things to look for include junction boxes with extra wires, or messy wiring, decoy 'boots' (the dark protective sleeves on wires near telephone poles) that look like real ones but actually hide wiretap components and transmitters, and phone taps hidden inside common commercial phone components. [Classic Concepts photos ©2000, used with permission.]

Some tapping devices are wireless, transmitting the conversation using radio frequency (RF) signals to another location rather than directly recording or amplifying it at the source. These can be detected with 'scanners,' devices designed to scan through a range of radio frequencies to detect an outgoing signal.

Some wiretap detection devices can only detect a tap when it is active. There are also devices designed to detect audio bugs even when they are inactive, in walls or on phone lines. Non-linear junction detectors are one example. Some devices are based on detecting and analyzing harmonic levels to determine whether a signal is originating from an electronic or nonelectronic source.

Some private branch or multiline phone systems are sold with built-in security by including *telephone-line analyzers* as part of the hardware. These systems can scan up to a couple of dozen phones (or more) to check for taps or transmitters associated with the lines. They are not infallible, but they can serve as a deterrent.

Since phone lines are also used for other types of communications, e.g., fax machines, there are also systems for encrypting or otherwise scrambling the signal prior to transmission. Thus, voice scramblers and fax encrypters are available which may be built in or portable/handheld. Voice-changers are also available. They don't encrypt the content of the message, but they change the sound of the voice to make it difficult to identify the person engaged in the call.

To defeat wiretapping equipment, some systems will constantly broadcast noise or nonsensical speech through the line. Thus, if a recording device is attached, the tapes or other memory buffer will fill up with hours and hours of unusable signals.

Sometimes bug-detecting devices are permanently installed on a secure line, with LCD displays describing any unusual occurrences or likely causes of anomalies. Systems that pro-

vide maximum security with line-monitoring, readouts, and noise broadcasting sell in the $600 range.

This book does not provide a detailed description of telephone switching systems or the detailed mechanics of telephone tapping. Its purpose is to provide a broad understanding of the technology and there are many references off and on the Internet that give precise details of the functionings of various telephone systems. A few of the more common concepts and glossary terms are included at the end, to aid in your understanding, but you are urged to consult technical references if you want engineering information on the various technologies mentioned here. See also the Radio Surveillance chapter for more information on wireless technologies.

6. Applications

Listening devices can be used to monitor children, the sick, or the elderly, the sounds of wildlife, or business transactions. They can also be used to detect emergency situations (car accidents, explosions, etc.) and to activate alarms, warning lights, or other emergency responses. In military applications, they can be used to detect the presence of hostile forces, bombs, and hostile troop communications. In law enforcement they are used to monitor illegal gambling, racketeering, drug trafficking, violent crimes, and insider trading activities.

7. Problems and Limitations

Wireless Transmissions

The biggest problem with wireless devices is that most of them transmit radio waves which travel in every direction and can readily be intercepted with scanners or other receivers tuned to the same frequency as the outgoing signal. This makes third-party eavesdropping or detection more likely than with wired transmissions. Encrypted or spread signals make content of the conversation more difficult to detect, but the presence of the communication can still be detected.

Installation

The installation of surveillance devices is becoming easier, as tiny, self-contained consumer models are manufactured and sold to the general public. There are still circumstances, however, where technical expertise is needed to install components (particularly certain types of beacons and wireless systems, as well as laser-based listening systems). Access to the inside or near outside vicinity of the premises is necessary for the majority of listening devices and may be difficult in some circumstances.

Wiretap Detection

Many phone tapping devices can easily be detected and defeated, particularly those which make a physical connection to the phone line and use power from the line. Checking for anomalies in the power usage or differences between pretap characteristics and post-tap characteristics of the line are common ways in which taps are detected.

Recording Times and Vulnerability

The vast majority of recording devices have limited recording times, or significant degradation of the quality of the recording with longer recording times. Most require that a tape be turned over or a flash memory card swapped out. The smaller the devices, usually the shorter the recording time. Larger van-based units, or room-based units can be hooked up to large

recording machines or large computer storage drives to extend recording times.

Because recording units are larger than basic listening units, they are more vulnerable to detection. A body-worn audio wire is very small and easy to hide in clothing, but the transmitter or recorder can often be detected by a visual inspection or pat-down search. Room-based recording units and their tapes or drives are vulnerable if there is access to the room. Thieves have often been known to break into recording rooms to take the tapes or recording devices that have captured a break-in or vandalism.

Emissions

One of the problems with electronic surveillance devices is that they emit radiation that may interfere with other nearby devices or may be compromised by radiation from other sources. Since the history of surveillance technologies is somewhat shrouded in myth and mystery and since many of the devices are illegal, not all of them have been manufactured to FCC standards or have been through FCC testing. This is also true of the kits and components sold for educational purposes which people sometimes try to use in offices or homes. Inadequate shielding or proximity to electronics devices is usually the reason for problems with buzzing, static, or erratic functioning.

Change of Use

One of the biggest problems with audio surveillance is that once the equipment is in place, intentions change, and monitoring occurs for longer than was originally planned or the purpose of the monitoring changes. The planned destruction or distribution of the information may also be changed after the fact. This tendency to change use or overstep the bounds of the original intention to tap is one of the valid reasons why privacy advocates oppose many types of surveillance.

8. Restrictions and Regulations

Because wiretapping and similar activities have been available to society for some time, restrictions to safeguard personal privacy have been put more firmly in place than for some of the newer surveillance technologies. In terms of the recording of personal phone calls in the U.S., in some states, one party must agree to the recording; in others, both parties must agree. Regulations for employee calls are different, with employers having a certain amount of leeway to protect business interests. It is wise, when making a legitimate record of a call, to ask the recipient on tape if she or he agrees to the recording of the call.

Some U.S. restrictions and laws of particular relevance to audio surveillance and privacy include

Communications Act of 1934. Public Law 416. U.S. Federal regulations established to organize and regulate interstate and foreign communications for national defense and to promote competitive communications technologies and services. The Federal Communications Commission (FCC) was established in accordance with the Act. The Act was amended by the Omnibus Budget Reconciliation Act (OBRA) to preempt state jurisdiction. It organized wireless communications into two categories: commercial mobile radio services (CMRS); and private mobile radio services (PMRS), including public safety and government services. (Note: 1992 Public Law 102-385 amends this Act to increase consumer protection and increase competition in cable television markets.)

Above 890 Decision. A 1959 Federal Communications Commission (FCC) decision which permitted private construction and use of point-to-point microwave links. Private companies could now utilize frequencies above 890 MHz for communications which might be useful on oil rigs, remote power plants, research stations, etc. As microwave communications technologies improved, the FCC was increasingly pressured for access to microwave broadcast frequencies. MCI was the first private commercial carrier service to take advantage of this Decision.

Omnibus Crime Control and Safe Streets Act of 1968. Public Law 90-351. This established procedure by which law enforcement agencies could obtain authorization to conduct electronic surveillance. It required telecommunications carriers to provide the "technical assistance necessary to accomplish the interception." It further created the National Institute of Justice (NIJ), the research and technological development agency of the Department of Justice (DoJ). Section 1212 of Public Law 91-452 repealed section 804 of this Act and was subsequently again repealed and amended.

Consumer Communications Reform Act of 1976. Also known as the "Bell Bill" because AT&T had lobbied for restoration of its monopolistic domination of the market and tried to reduce FCC regulatory authority over long-distance communications competitors. This provoked hearings into the Act and competition in the communications market. The result was the *Execunet Decision* in 1977, opening the long-distance market to competing companies.

Foreign Intelligence Surveillance Act of 1978 (FISA). This Act established legal standards for the use of electronic surveillance for counterintelligence and the collection of intelligence related to foreign activities within the U.S. It provided legislative authority for wiretapping and other electronic surveillance of foreign powers within and without the country. It further established the Foreign Intelligence Surveillance Court (FISC) to review and approve surveillance which could be used to monitor U.S. Persons. Amended in 1994 to provide limited authority for physical searches. Review of cases was conducted by a Committee beginning in the 104th Congress.

Electronic Communications Privacy Act of 1986. (ECPA). This amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968. In essence, ECPA extends existing restrictions on unauthorized interception of communications over traditional media to cover electronic communications. It does not extend prohibitions in cases where one of the parties consents to the interception and does not extend the right into some work-related communications (there are employer exceptions that permit monitoring). There are also some exemptions for communications providers to permit system administrators to manage and troubleshoot the system. A number of state laws are patterned after the ECPA.

Communications Assistance for Law Enforcement Act of 1994 (CALEA). Public Law 103-414. This is sometimes referred to as the 'Digital Telephony' law. It requires that telecommunications providers ensure that law enforcement agents can execute court-authorized wiretaps. In many cases, this requires physical changes or upgrades to the providers' equipment.

Digital Communications and Privacy Improvement Act of 1994. 25 October 1994, signed into law by President Clinton. This was to ensure continued ability of law enforcement officials to conduct court-authorized electronic surveillance.

Comprehensive Counterterrorism Prevention Act of 1996. Signed into law by President Clinton on 9 Oct. 1996. This is a strategy to improve security in federal buildings and aircraft cargo holds. It also authorizes relocation of U.S. forces in foreign stations at high risk for terrorist attacks.

Communications Decency Act of 1996. A provision of the Telecommunications Reform Act that erupted in controversy as to definitions of 'lewd' or other materials that were being promoted as criminal because they might be objectionable to the general public, yet were considered acceptable within the more open climate of Internet communications. The Act was contested and, in June 1997, declared unconstitutional and in violation of individual rights of freedom of speech.

Telecommunications Act of 1996. The first substantive overhaul of the Communications Act of 1934. The intent of this Act is to enable open access to the telecommunications business and to permit any business to compete with any other telecommunications business. The primary impact was on phone and broadcast services with responsibility shifted away from state courts to the Federal Communications Commission (FCC), while much of the administrative workload remained with state authorities. It made it possible for Regional Bell Operating Companies to provide interstate long-distance services and for telephone companies to provide cable television services. Cable companies could now also provide local telephone services.

United States Title 18 - Crimes and Criminal Procedure, Part 1 (Crimes), Chapter 119 - *Wire and Electronic Communications Interception and Interception of Oral Communications*. This chapter covers the interception and disclosure of wire, oral, or electronic communications; manufacture, distribution, possession, and advertising of wire, oral, or electronic communications intercepting devices; confiscation; use-as-evidence prohibitions; authorizations; procedures; reports; recovery of civil damages; and injunction against illegal interception.

Unites States Title 18 - Crimes and Criminal Procedure, Part 1 (Crimes), Chapter 121 - *Stored Wire and Electronic Communications and Transactional Records Access.* This chapter covers unlawful access; disclosure of contents; requirements for government access; backups; delayed notice; reimbursement; civil action; exclusivity of remedies; counterintelligence access to records; and wrongful disclosure.

Communications Assistance for Law Enforcement Act. Public Law 103-414, enacted by the 103d U.S. Congress. Invokes assistance from the telecommunications industry to provide technological solutions for accessing call information and call content for law enforcement agencies legally authorized to do so.

There are many state laws of interest, so these are just examples:

- New Jersey Wiretapping and Electronic Surveillance Control Act
- Pennsylvania Wiretapping and Electronic Surveillance Act

See the Radio Surveillance chapter for information pertinent to wireless communications.

9. Implications of Use

There appears to be an enormous market for bugs, recorders, bug-sweeping devices, amplifiers, and surveillance consultants judging by the number of vendors and products. The sheer sales volume of taping devices alone suggests that phone tapping is a widespread activity, despite abundant restrictions and regulations. This conclusion is further reinforced by the fact that vendors emphasize the 'quiet operation' of recording and listening units, such as the absence of warning beeps to notify a conversant that she or he is being recorded. The steadily decreasing cost of these devices makes it easy for people to consider their purchase.

The Dangers of Call Monitoring

The incidence of recorded calls, both covert and otherwise, is increasing. Many high-tech firms are now recording or listening in on customer product inquiry and technical support calls. Since the caller must be informed that the call may be recorded (in some areas, the caller must be explicitly asked if recording is OK), there is usually a message like, "This call may be monitored for quality control." Since this seemingly innocuous message is commonplace, many people no longer consciously realize that it means the call is being recorded, or may forget during the progress of the call, especially if they are made to wait for a long time while on hold.

This trend may lead to much broader use and acceptance of live monitoring or recording of calls with consequences that might not be in the best interests of the caller. Say, for example, that the call resulted in legal proceedings. Since the caller has tacitly agreed to the recording, but may not have been fully aware of the ramifications or consequences, the information could conceivably be used against him or her. The caller is almost never told what is going to be done with the monitored information, who will listen to it, or how long it will be kept on file. The caller also doesn't know if the call is being processed for voice stress or other psychological factors that might be used to manipulate a sales or business call. A copy of the call is in the hands of the callees, to use as they see fit, but not in the hands of the caller, who must try to remember the nature and contents of the call, which is difficult, especially if the matter comes up months or years later. Clearly, with new technologies that make it easy to integrate Call Monitoring into the phone system itself, the consumer's rights are not being protected in part because of the naive trust of consumers. If they don't understand the technology, they don't understand the ways it can be used to manipulate or compromise their security or safety.

Law Enforcement Monitoring of Calls

Privacy advocates have strongly objected to the monitoring of electronic communications by law enforcement agents. Law enforcement agents, on the other hand, are concerned about falling behind the technology curve and being unable to apprehend criminals who might use technologies in new ways to communicate with one another or might seek to commit new types of crimes made possible by the emerging technologies. It is difficult for law enforcement agencies to implement new policies or to use new technologies in crime prevention and detection without public support. This support will not be forthcoming unless these agencies stress accountability within the system and address the concerns of privacy and civil rights advocates which include

past abuses In the past, wiretapping abuses by law enforcement have been documented by Congress itself, causing the public to be 'gun-shy' of allowing the agencies any wider jurisdiction.

invisible access The adoption of newer remote network technologies can potentially allow law enforcement agents to tap without the same checks and balances that were in place when they had to physically enter a communications carrier's premises to cooperate in setting up a tap. If the equipment is in place and can be accessed remotely, and is decrypted after capture, then law enforcement activities essentially become 'invisible' and less subject to a public or corporate approval process and other traditional safeguards to prevent misuses or corruption.

repurposing There have been many examples of agencies taking information that was approved and gathered for one purpose and later using it for another, particularly when political administrations change. Thus, people are concerned that politically volatile or out-of-context information gathered on prominent public persons could be 'leaked' to the press to discredit someone with a different agenda from the mainstream or that sensitive economic information could clandestinely be used for business-related financial gain by friends or relatives of people within agencies that have access to the information.

discrimination There are concerns that surveillance targets and database lookup systems might be structured in a way that would unfairly target or marginalize minority groups.

Communications carriers and developers have also expressed concerns about law enforcement tapping capabilities being built into digital communications systems because it may build obsolescence into the systems, or may even be outlawed (and unable to be sold) if wiretapping legislation changes in the near future, thus threatening R&D and production expenditures within the telecommunications business community.

Given these concerns, it is important not just to lobby for use of new technologies and to learn to use and implement them well, but to give equal consideration to how accountability structures that protect the public can be built into the systems.

10. Resources

Inclusion of the following companies does not constitute nor imply an endorsement of their products and services and, conversely, does not imply their endorsement of the contents of this text.

10.a. Organizations

Alliance for Telecommunications Industry Solutions (ATIS) - Provides news and information on conferences, educational programs, software, and other support related to the telecommunications industry. ATIS sponsors the Electronic Communication Service Providers Committee in order to assist with compliance requirements for communications carriers. http://www.atis.org/

Cellular Telecommunications Industry Association (CTIA) - CTIA provides member support and wireless products advocacy. The Web site provides news, commentary, information on law and public policy, statistics, consumer resources, and conference announcements. http://www.wow-com.com/

Center for Democracy and Technology (CDT) - This is an independent, nonprofit, public-interest policy organization which develops and implements public policy regarding liberty and democratic values. CDT is following and recording the debate over wiretapping legislation and privacy and providing research and study into this area of concern. Archives of reports are maintained on their Web site. http://www.cdt.org/

Central Computer and Telecommunications Agency (CCTA) - A United Kingdom government agency located in Norwich, which promotes good practices in information technology and telecommunications in the public sector.

Competitive Telecommunications Association (CompTel) - Provides representation for over 300 members before the FCC and Congress and supports the prosperity of the competitive telecommunications carriers and their suppliers in the U.S. and overseas. In 1999, CompTel joined with America's Carriers Telecommunication Association (ACTA). The group holds three conferences per year. http://www.comptel.org

Electronic Privacy Information Center - A public-interest research center located in Washington, D.C. EPIC was founded in 1994 to focus public attention of civil liberties and privacy issues associated with the electronic age. It works in association with Privacy International (U.K.) and others. http://www.epic.org/

Federal Communications Commission (FCC) - An important U.S. federal regulatory organization established in 1934 to regulate the broadcast industry by granting and administering licenses for radio communications. The FCC's responsibilities have been broadened since that time to include product emissions regulation and fair distribution of telecommunications resources. http://www.fcc.gov/

Fiber Optic Association, Inc. - An international nonprofit professional association representing the fiber-optic industry. It provides information, training, and certification. http://www.fotec.com/

Fibre Channel Association (FCA) - An organization supporting Fibre Channel technology which is capable of providing high-speed intercomputer communications for longer distances than the current popular SCSI standard, for example. http://www.fibrechannel.com/

Fibreoptic Industry Association (FIA) - A U.K.-based professional organization which includes educators, installers, and suppliers or fiber technologies. http://www.fibreoptic.org.uk/

Indiana State Archives - This resources includes seventeen volumes of telegraphic correspondence between Governor Morton and President Lincoln, Generals Sherman, Stanton, Grant, and others. The telegraph books and telegraphs not recorded in the books are stored on microfilm and the database index can be searched online. http://www.ai.org/icpr/webfile/archives/homepage.html

International Telecommunication Union (ITU) - The ITU is an important international organization that is based in Geneva, Switzerland and provides education and standards to the telecommunications industry. The ITU evolved from the Telegraph Union which was formed in 1865 (formerly CCITT). http://www.itu.ch/

Nathanson Centre for the Study of Organized Crime and Corruption - Provides historical and contemporary information on crime and corruption, including analysis and intelligence, alternatives to law enforcement, investigation, surveillance and undercover operations, and law and legislation. The focus is on Canada, but there are many generic references and an excellent annotated bibliography. http://www.yorku.ca/nathanson/

National Institute of Justice (NIJ) - NIJ was created as the research and technological development agency of the U.S. Department of Justice to sponsor special projects, research, and development to improve and strengthen the criminal justice system to reduce or prevent violent crime. http://www.ojp.usdoj.gov/nij/

Telephone Pioneers of America (TPA) - A nonprofit organization established in 1911 by the Bell system pioneers. TPA now includes more than 100,000 members. http://www.telephone-pioneers.org/

U.S. Department of Justice (DoJ) - Under the direction of the Attorney General, the DoJ is charged with attaining and maintaining justice and fair treatment for Americans through the combined services of almost 100,000 attorneys, law enforcement professionals, and employees. Part of the DoJ responsibility involves detecting criminal offenders. It is headquartered in Washington, D.C. with almost 2,000 installations throughout the country. http://www.usdoj.gov/

10.b. Print

Arrington, Winston, "Now Hear This! Electronic Eavesdropping Equipment Design," Sheffield Electronics, 1997.

Berkel, Bob; Rapaport, Lowell, "Covert Audio Interception," CCS Security Publishing, 1994, 720 pages.

Blum, Richard, "Surveillance & Espionage in a Free Society," New York, London: Praeger Publishers, 1972.

Brookes, Paul, "Electronic Surveillance Devices," Butterworth-Heinemann, 1996, 112 pages. General descriptions, types of devices, circuit diagrams, and construction information. Of interest to hobbyists and corporate security technicians.

Brown, Robert M., "The Electronic Invasion," New York: John F. Rider Publisher, Inc., 1967. A historical perspective on electronic bugging up to the time of publication. Discusses the evolution and miniaturization of the technology as well as distribution of tapping devices.

Bugman, Shifty, "The Basement Bugger's Bible: The Professional's Guide to Creating, Building, and Planting Custom Bugs and Wiretaps." Includes schematics, blueprints, photos, diagrams, anecdotes on phone taps, microphones, bugs and related audio surveillance devices. For academic study, 320 pages.

Campbell, Duncan, "Big Brother is Listening: Phonetappers and the Security State," New Statesman, 1981, 70 pages. Campbell is one of the more vocal and credible of the high-profile Web journalists reporting on surveillance activities.

Carr, James G., "The Law of Electronic Surveillance," New York: Clark Boardman Co., Ltd., 1977.

Chambers of Commerce of the State of New York, "Papers and Proceedings of Committee on the Police Problem, City of New York, 1905," New York: Ayer Company Publishers, 1905. This title is still available. It describes investigations of police problems at the turn of the century, including the Lexow and Mazet hearings.

Chin, Gabriel J., "New York City Police Corruption Investigation Commission 1894-1994," six volumes, New York: William S. Hein & Co., Inc., 1997.

Chin, Gabriel J., "Report and Proceedings of the Senate Committee Appointed to Investigate the Police Department of the City of New York ("Lexow Report")," five volumes, New York: William S. Hein & Co., Inc., 1997.

Churchill, Ward; Vander Wall, Jim, "The COINTELPRO Papers: Documents from the FBI's Secret Wars Against Dissent in the United States," South End Press, 1990, 468 pages. Includes statistics, information, and speculation on the documented and undocumented aspects of FBI wiretapping and mail openings during Hoover's administration.

Cook, Earleen H., "Electronic Eavesdropping," 1983. Out of print.

Daley, Robert, "Prince of the City: The True Story of a Cop Who Knew Too Much," Boston: Houghton Mifflin Co., 1978. A former New York Deputy Police Commissioner describes witnessing alleged corruption, theft, and perjury within the police department.

Dannett, Sylvia G. L., "She Rode with Generals: The True and Incredible Story of Sarah Emma Seelye, Alias Franklin Thompson," New York: Thomas Nelson, 1960.

Dash, Samuel; Schwartz, Richard F.; Knowlton, Robert E., "The Eavesdroppers," New Brunswick, N.J.: Rutgers University Press, 1959. Even though this is an older text, it is frequently cited by both writers and speakers. It was reprinted by Da Capo Press in 1971, 484 pages.

Diffie, Whitfield; Landau, Susan, "Privacy on the Line: The Politics of Wiretapping and Encryption," Boston: MIT Press, 1998, 342 pages. Recipient of IEEE and other book awards, this takes the reader point-by-point through the history and politics of wiretapping, revealing the opposing opinions and complex issues involved.

Donner, Frank, "The Age of Surveillance: The Aims and Methods of America's Intelligence System," New York: Vintage-Random House, 1981.

Doyle, Sir Arthur Conan, "The Man with the Watches," a story in which Conan Doyle makes reference to the Lexow commission (which investigated the New York police in 1894). The story can be found in various compilations of Sherlock Holmes stories, e.g., Doyle, Arthur C., "Complete Sherlock Holmes," New York: Doubleday Books, 1960.

Edmonds, S. Emma E., "Memoirs of a Soldier, Nurse, and Spy: A Woman's Adventures in the Union Army," Northern Illinois University Press, 1999. Previously published as "Nurse and Spy in the Union Army: The Adventures and Experiences of a Woman in Hospitals, Camps, and Battle-fields," 1865 (384 pages) and originally published as "The Female Spy of the Union Army," Boston: DeWolfe, Fiske & Co., 1864.

Erickson, William H., Chairman, "Electronic Surveillance - Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance," NWC Report, U.S. Government Printing Office, 1976.

Fishel, Edwin C., "The Secret War for the Union. The Untold Story of Military Intelligence in the World War," New York: Houghton Mifflin Co., 1996, 734 pages. Intelligence records usually 'disappear' after a War, but Fishel has uncovered documents that reshape our thinking about military strategists and how they influence the politics of war.

Fitzgerald, Patrick; Leopold, Mark, "Stranger on the Line: The Secret History of Phone Tapping," London: Bodley Head, 1987. U.K. wiretapping history.

Garrow, David J., "The FBI and Martin Luther King, Jr. From "Solo" to Memphis," New York, London: W.W. Norton & Co., 1981.

Goode, James, "Wiretap: Listening in on America's Mafia," New York: Simon & Schuster, 1988.

Greene, Richard M., "Business Intelligence and Espionage," Homewood, Il.: Dow Jones-Irwin, 1966.

Hall, Richard, "Patriots in Disguise," New York: Paragon House, 1993. Women were not welcome in matters of war, but many got involved anyway, in male disguises. Illustrated history of some of the fascinating soldiers and 'male' nurses who eavesdropped during the Civil War.

Hartman, John Dale, "Legal Guidelines for Covert Surveillance," Newton, Ma.: Butterworth-Heinemann, 1993, 235 pages.

Johnson, Pauline Copes, "City of Auburn Souvenir Celebration Booklet Commemorating 20 Years of History 1793-1993," Cayuga County Historian's Office. Includes information on Harriet Tubman, Underground Railroad and Civil War spy.

Jones, R.; Taggart, R.; et al., "Electronic Eavesdropping Techniques and Equipment," Washington, D.C.: National Bureau of Standards, Law Enforcement Standards Laboratory, 1977.

Lapidus, Edith J., "Eavesdropping on Trial," New Jersey: Hayden Book Co., 1973, 287 pages.

Law Enforcement Associates, "The Science of Electronic Surveillance," Raleigh, North Carolina: Search, Inc., 1983.

LeMond, Alan; Fry, Ron, "No Place to Hide: A Guide to Bugs, Wire Taps, Surveillance and Other Privacy Invasions," St. Martin's Press, 1975, 278 pages.

Leonard, Elizabeth, "All the Daring of the Soldier: Women of the Civil War Armies," New York: W. W. Norton, 1999, 320 pages, illustrated. Describes the eavesdropping and spy activities of women in the Revolutionary and Civil Wars in America.

Long, Edward V., "The Intruders, the Invasion of Privacy by Government and Industry," New York: Praeger, 1967, 230 pages. Foreword by Hubert H. Humphrey. Long was unsympathetic to alleged FBI pressure to support their actions while holding a Senate seat, was subsequently defeated, and wrote this account of his experiences.

Marx, G.T., "Undercover: Police Surveillance in America," L.A.: University of California Press, 1988.

Murphy, Walter F., "Wiretapping on Trial," New York: Random House, 1965. Murphy is co-author of "American Democracy," a widely used college text and a former member of the U.S. Marine Corps.

New Haven Board of Police Commissioners, "Report on Wiretapping," 1978.

Office of Technology Assessment, "Electronic Surveillance in a Digital Age," U.S. Government Printing Office, July 1995. Describes progress in electronic communications and surveillance and focuses on the work of law enforcement and telecommunications agencies to implement the Communications Assistance for Law Enforcement Act, Public Law 103-414 and other relevant laws.

Oslin, George P., "The Story of Telecommunications," Macon, Ga.: Mercer University Press, 1992. The author, born in 1899, lived through many of the significant early developments in telecommunications and communicated directly with some of the pioneers in the industry. The book covers the technical and regulatory aspects, as well. He is credited with inventing the 'Singing Telegram.'

Paulsen, Monrad G., "The Problems of Electronic Eavesdropping," American Law Institute American Bar Association Committee on Continuing Professional Education, 1977, 136 pages.

Pollock, David A., "Methods of Electronic Audio Surveillance," Springfield, Il.: Charles C Thomas Publisher, Ltd., 1973.

Records of the Committee on the District of Columbia Subcommittee on the Investigation of Wiretapping. About four linear feet of records from the 81st to 92nd Congresses dating 1950 to 1951 housed as Record Group 46 in the National Archives and Records Administration.

Records of the San Francisco Field Office, 1950 to 1952. This is a series of clippings, affidavits, memorandums, pleadings, and telegrams about controversial program content related to investigations of the radio and television industry and wiretapping. Available through the regional National Archives and Records Administration office in San Bruno, California.

Richburg, Rod; Swift, Theodore N. (illustrator), "Wiretap Detection Techniques," Austin Tx.: Thomas Investigative Publications, 1997.

Ruttledge, Hugh, "Everest 1933," London: Hodder & Stoughton, 1934, 390 pages.

Schartz, Herman, "Taps, Bugs and Fooling the People," The Field Foundation, 1977.

Schneier, Bruce; Banisar, David, "The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance," New York: J. Wiley, 1997, 747 pages.

Shannon, M. L., "The Bug Book: Wireless Microphones & Surveillance Transmitters," with contributions by Kevin D. Murray, Boulder, Co.: Paladin Press, 2000, 168 pages. Awareness, detection, and countermeasures, including anecdotes.

Shannon, M. L., "The Phone Book: The Latest High-Tech Techniques and Equipment for Preventing Electronic Eavesdropping, Recording Phone Calls, Ending Harassing Calls," Boulder, Co.: Paladin Press, 1998, 280 pages.

Swift, Theodore N., "Wiretap Detection Techniques: A Guide to Checking Telephone Lines," Boulder, Co.: Paladin Press, over 100 pages, illustrated. Describes procedures for conducting eavesdropping countermeasures surveys. The author is a former counterintelligence officer who worked for the DEA for 11 years and has developed this book from his experience and his teaching of a law enforcement seminar. Topics include inductive wiretaps, testing for series devices, network schematics, line balance tests, spectrum analyzers, transmitter harmonics, and more.

Thomas, Ralph D., "The TSCM Bible: A Countermeasures Cookbook on Conducting Professional TSCM Services," Austin, Tx.: Thomas Investigative Publications, Inc. Includes almost 300 pages and a computer resource disk. A comprehensive overview on conducting countermeasures sweeps and TSCM services including equipment and testing procedures.

Turner, WIlliam W., "How to Avoid Electronic Eavesdropping and Privacy Invasion," Boulder, Co.: Paladin Press, 1972.

Velazquez, Loreta Janeta, "The Woman in Battle: A Narrative of the Exploits, Adventures and Travels of Madame Loreta Janeta Velazquez, Otherwise Known as Lieutenant Harry T. Buford, Confederate States Army," Richmond, Va.: Dustin, Gilman & Co., 1876. The full text is available online through the University of North Carolina at Chapel Hill Libraries.

Whidden, Glenn H., "The Axnan Attack–A Detailed Composite Case History about How Corporate Electronic Eavesdropping is Accomplished," Technical Services Agency.

Articles

The Center for Constitutional Rights, "If an Agent Knocks: Federal Investigators and Your Rights," New York. Discusses FBI COINTELPRO activities and the rights of individuals who receive visits by FBI agents.

Delaney, Donald P.; Denning, Dorothy E.; et al., "Wiretap Laws and Procedures: What Happens When the Government Taps a Line," Georgetown University, Sept. 1993.

Dempsey, James X.; Weitzner, Daniel J.; et al., "Comments of the Center for Democracy and Technology in the Matter of Communications Assistance for Law Enforcement Act," CC Docket No. 97-213 before the FCC, 20 May 1998. See also Dempsey, James X., "Statements before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the House Committee on Commerce on the Wireless Privacy Enhancement Act of 1999 and the Wireless Communications and Public Safety Enhancement Act of 1999," 3 Feb. 1999 and Dempsey, James X., "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany Law Journal of Science & Technology,"* 1997, V.8(1), available through CDT. http://www.cdt.org/

Denning, Dorothy E., "Encryption and Law Enforcement," Georgetown University, Feb. 1994.

Dichter, Mark S.; Burkhardt, Michael S., "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Communications in the Internet Age," Morgan, Lewis & Bockus, LLP, 2000. Describes trends, laws, and historical precedents regarding employee electronic communications, including some references to corporate wiretapping and how the courts made distinctions between phone tapping and network 'tapping.'

Elder, Willie J., Jr., "Electronic Surveillance: Unlawful Invasion of Privacy or Justifiable Law Enforcement," Yale-New Haven Teachers Institute Curriculum Unit, 1983.

Fillingham, David, "Listening in the Dark - Wiretapping and Privacy in America," MIT paper for Ethics and Law on the Electronic Frontier, 1997. Discusses historical highlights and major legal decisions leading up to present-day encryption debates.

Freeh, Louis, FBI Director, Testimony in the Senate Judiciary Committee, Terrorism, Technology & Government Information Subcommittee, Senator Jon Kyl, Chair, 3 September 1997.

Guinier, Daniel, "From Eavesdropping to Security on the Cellular Telephone System GSM," *ACM SIGSAC Security Audit & Control Review,* 1997, V.15 (2), pp. 13-18.

Internal Revenue Service, "Tax Professional's Corner: Handbook 9.4, Investigative Techniques, Chapter 6, Surveillance and Non-Consensual Monitoring," available online at http://www.irs.gov/bus_info/tax_pro/ in the Part 9, Criminal Investigation section.

Landau, Susan, "Eavesdropping and Encryption: U.S. Policy in an International Perspective," published on the Harvard Information Infrastructure Project site. Discusses the historical role of government in communications policy and cryptographic concerns up to the present day from an international perspective.

Lyon, David, "The New Surveillance: Electronic Technologies and the Maximum Security Society," *Crime, Law and Social Change,* 1992, V.18(1-2).

MacDonald, Fred J., "Don't Touch That Dial: Radio Listening Under the Electronic Communications Privacy Act of 1986," Chicago: Nelson-Hall, 1989.

Matthews, Clark, "Unanymous Nod for Wiretap Bill," *The Spotlight*, Nov., 1994. Discusses the Wiretap Access Bill, passed in Oct. 1994, and FBI lobbying that occurred prior to submission of the bill.

Merhav, N.; Arikan, E., "The Shannon Cipher Systems with a Guessing Wiretapper," *IEEE Transactions on Information Theory*, Sept. 1999, V.45 (6), pp. 1860-1866.

Millman, Gregory, "From Dragnet to Drift Net: Telephone Record Surveillance and the Press," Dudley Clendinen, "Justice Dept. Gets Phone Records of the Time's Bureau in Atlanta," NYT, 6 Sept. 1980.

Miyazawa, Setsuo, "Scandal and Hard Reform: Implications of a Wiretapping Case to the Control of Organization Police Crimes in Japan," *Kobe University Law Review*, V.23, pp. 13-27.

Morse, Wayne, "Wiretapping proposals threaten historic gains," Washington, D.C., U.S. Government Printing Office, 1954.

Ogura, Toshimaru, "Japan's Big Brother, The Wiretapping Bill and the Threat to Privacy," *AMPO, Japan-America Quarterly Review*, 1997, V.28(1). Discusses a controversial move to legalize wiretapping in Japan.

O'Neill III, Thomas F.; Gallagher, Kevin P.; Nevett, Jonathon L., MCI Communications Corporation, "Detours on the Information Superhighway: The Erosion of Evidentiary Privileges in Cyberspace and Beyond," *Stanford Technology Law Review*, 1997, V.3. Provides a historical overview of wired/wireless communications up to the current Internet and legal responses to regulation and changes in the industry.

Saxbe, William B., "Wiretapping and Electronic Surveillance," *Police Chief*, 1975, V.42(2), Feb., pp. 20-22.

Shuy, Roger W., "Tape Recorded Conversations," *Criminal Intelligence Analysis,* Loomis, Ca.: Palmer, 1990.

Skolnick, Jerome H., "Deception by Police," *Criminal Justice Ethics*, 1982, V.1(2). Skolnick is Co-Director of the Center for Research in Crime and Justice. The article discusses ethics, the concepts of legality, and the actions and theorized motives of dishonest individuals in positions of authority. Wiretapping in the Hoover years is discussed.

Steal, Agent, "Tapping Telephone Lines Voice or Data for Phun, Money, and Passwords Or How to Go to Jail for a Long Time," *Phrack magazine Number 16*, Aug. 1987.

Truman Library, "Oral History Interview with Joseph L. Rauh, Jr.," in the National Archives and Records Administration, transcribed by Niel M. Johnson, 21 June 1989. Includes references to Truman, the FBI, and wiretap documents of Tommy Corcoran.

Westin, Alan "Science, Privacy, and Freedom: Issues and Proposals for the 1970s," Columbia Law Review reprint, 1966, 47 pages. This article has been cited in a number of privacy-related legal judgments.

Journals

"Safety and Security," by Carroll Publications, Ohio. Topics include fraud, fire protection, workplace surveillance, public safety, etc.

"Wiretap Report," an annual publication by the Administrative Office of the United States Courts. Provides general and historic information on criminal wiretaps and procedures. There are tables breaking down major offenses by category and state. It can be downloaded in Adobe .pdf format. It does not provide specific information on the actual number of lines covered in each court order and does not specify statistical details for pen register and trap-and-trace activities, which comprise the majority. This type of information was collected by the FBI, however, for a period of two years, in order to estimate law enforcement needs incumbent upon communications carriers through CALEA.

The Department of Justice (DoJ) conducts surveys of Pen Register/Trap and Trace court orders.

See also the general privacy and security journals listed in Chapter 1 - Introduction and the computer communications journals listed in the Computer Surveillance chapter.

Reports and Testimony

Electronic Surveillance Task Force, "Communications Privacy in the Digital Age," *The Digital Pri-*

vacy and Security Working Group papers, Interim Report, June 1997. Discusses electronic surveillance and the evolution of privacy protection and continued law enforcement lobbies for wider discretion in monitoring electronic communications. Lists and discusses key developments and related legislation. Available through the Center for Democracy and Technology. http://www.cdt.org/

Hearings on Wiretapping and other Terrorism Proposals, "Testimony of David B. Kopel, Associate Policy Analyst," Cato Institute, Committee on the Judiciary United States Senate, 24 May 1995. Responds to fears provoked by the Oklahoma City bombing and describes the need for careful consideration of legislation and debates the issues over the expansion of wiretap authority.

Shelby, Richard C. (Chairman) et al., "Special Report of the Select Committee on Intelligence, United States Senate, January 4, 1995 to October 3, 1996," 1997. A report contributing to public accountability that includes information on Committee review of the Foreign Intelligence Surveillance Act (FISA). Topics include reviews of foreign intelligence, legislation, arms control, counterintelligence, counterterrorism, and counter-proliferation.

Subcommittee on Crime Committee on the Judiciary U.S. House of Representatives Oversight Hearing on The Implementation of the Communications Assistance for Law Enforcement Act of 1994, "Dempsey Testimony," Testimony of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology., 23 October 1997. This testimony includes substantial information on CALEA and its proposed implementation and pen register and other surveillance tools used by law enforcement. The reader is also encouraged to read other testimony related to this Oversight Hearing.

U.S. Congress House Committee on Education and Labor. Subcommittee on Labor-Management Relations, "Hearing on House Rule 1900, Privacy for Consumers and Workers Act of 1993," Washington, D.C., U.S. GPO, 1994, 235 pages.

U.S. Congressional Record, Remarks of Senator Jesse Helms, 3 October 1983, V.129(130), pp. S 13452-13461. These remarks refer to surveillance of the activities and associations of Dr. Martin Luther King, Jr. and statements about communists and other 'extremists,' (the speaker included in this category those who were opposed to the Vietnam conflict). Wiretap evidence was ordered to be sealed for a period of several decades.

U.S. Department of Justice, "Electronic Surveillance - Report on the FBI's Publication of the Second Notice of Capacity," January 1997, a report on the telephone system capacity that may be needed by law enforcement to carry out court-approved electronic surveillance with regard to implementation of the CALEA requirements of communications carriers. Later, further details were provided by the FBI on how the wiretap statistics were obtained and the capacity requirements calculated (Congressional Record, 9 February 1996).

U.S. National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, "Electronic Surveillance Report," Washington, D.C., 1976.

10.c. Conferences and Workshops

Many of these conferences are annual events that are held at approximately the same time each year, so even if the conference listings are outdated, they can still help you determine the frequency and sometimes the time of year of upcoming events. It is very common for international conferences to be held in a different city each year, so contact the organizers for current locations.

Many of these organizations describe the upcoming conferences on the Web and may also archive conference proceedings for purchase or free download.

The following conferences are organized according to the calendar month in which they are usually held.

"Computer Telephony Expo," business and developer-oriented conference, Los Angeles, Ca., 7-9 March 2000. The "CT EXPO 2001," is scheduled in L.A. for 6-9 March 2001.

"IP Telephony 2000 - The Emerging Communications Environment," London, U.K., 11-12 April 2000.

"ICASSP 2000 - 2000 IEEE International Conference on Acoustics, Speech, and Signal Processing," Istanbul, Turkey, 4-9 June 2000. IEEE technical conference.

"ICC 2000 - 2000 IEEE International Conference on Communications," New Orleans, Louisiana, 18-22 June 2000. Technical conference.

"Association of Public Safety Communications Officials (APCO) 2000," 66th annual conference, Boston, 12-17 Aug.

"2000 International Conference on Communication Technology - ICCT 2000," Beijing, China, 21-23 August 2000. IEEE technical conference.

"Mobile Battlefield Communications," SMI conferences, London, U.K., 5-6 Sept. 2000.

"DEFCOM - Defence Communications Exhibition," Nexus Media Ltd., London, U.K., 20-21 Sept. 2000.

"PCS '01," wireless PCS telephone communications, Orlando, Florida, 3-5 Oct. 2001.

"Military Satellite Communications," SMi conferences, London, U.K., 9-10 Oct. 2000.

"GLOBECOM 2000 - 2000 IEEE Global Telecommunications Conference," San Francisco, Ca., 27 Nov. - 1 Dec. 2000. IEEE technical conference.

10.d. Online Sites

Adventures in Cybersound. Milestones through 2500 years of communications history. This lists many of the interesting and important discoveries in microphones, sound recording, and wireless broadcasting technologies associated with audio/visual communications. Compiled by Dr. Russell Naughton. http://www.cinemedia.net/SFCV-RMIT-Annex/rnaughton/TV_TL_COMP_2.html

Center for Democracy and Technology. This organization has a specific section on wiretapping (see buttons at bottom of page) which lists developments in wiretapping activities and legislation and provides numerous links to prominent articles and excerpts of testimony related to the subject. There is also an overview of terms and devices. http://www.cdt.org/

DSL Sourcebook. The HTML version of "The DSL Sourcebook: Plain Answers on Digital Subscriber Line Opportunities," by Paradyne Corporation. This includes extensive information on Digital Subscriber Line technologies, including the existing copper-wire infrastructure, DSL concepts, emerging services, network models (including IP/LAN, ATM), and almost three dozen diagrams of performance descriptions, reference models, etc.
http://www.paradyne.com/sourcebook_offer/sb_html.html#ch2

International Privacy and Wiretapping. On the Chicago-Kent Collect of Law Illinois Institute of Technology, there is an online Information Center. One page of particular interest is the U.S. Department of State Annual Human Rights Report (Privacy Report) which has been excerpted by Privacy International to list relevant information that briefly describes wiretapping authority and regulations in the various world nations. http://www.kentlaw.edu/ic3/islat/prvcysum.htm

The Sound Recording History Site. This site by David Morton includes a variety of topics relevant to sound recording including a historical chronology, information about recording devices, ideas that didn't work, dead sound-recording media, and thoughts on the surveillance society.
http://www.rci.rutgers.edu/~dmorton/soundrechist.html

10.e. Media Resources

"The Inspectors," a Showtime Network movie about the lives and works of two fictional federal law enforcement agents responsible for solving a mail bomb case. While this isn't directly related to audio surveillance, inspection of mail and eavesdropping on conversations historically have many parallels and this show includes other surveillance techniques of interest, as well.

11. Glossary

Titles, product names, organizations, and specific military designations are capitalized; common generic and colloquial terms and phrases are not.

AIN	Advanced Intelligent Network. A Signaling System No. 7-based telephone switching network which integrates ISDN and cellular services into PCS services. This may eventually be superseded by Information Network Architecture (INA).
AMPS	Advanced Mobile Phone Service. An analog cellular phone system introduced in the early 1980s.
ATM	Asynchronous Transfer Mode. A high-speed, cell-based, connection-oriented, packet tranmissions protocol that can handle data with varying burst and bit rates. ATM evolved in the mid-1980s through standardization efforts by the CCITT (now ITU-T). It is an important digital data and communications format that is widely used in computer networking. Digital voice communications can be carried over ATM systems, with Voice over ATM being one of a number of models in development.
aural transfer	Defined by U.S. Code Title 18, Part I, Chapter 119 as "a transfer containing the human voice at any point between and including the point of origin and the point of reception."
bug	A covert or clandestine listening or viewing device that is noted for its small, inconspicuous (bug-like) size. Bugs used to primarily mean listening devices, small microphones that could be hidden in plants or phone handsets, but the term now is also used to describe tiny pinhole cameras that are as small as audio bugs used to be twenty years ago. A bug may be wired or wireless and may or may not be sending information to a recording device.
CCITT	Comité Consultatif International Télégraphique et Téléphonique. An important international standards body which is now known as the International Telecommunication Union (ITU).
CDMA	Code-Division Multiple-Access. A digital, wireless communications service based on spread-spectrum technology. Security can be provided through spread-spectrum modulation of the signal.
CELP	Code Excited Linear Predictive. This is a means of translating analog voice data to digital format so that conversations can be sent through digital networks like local area networks (LANs) and the Internet. When Internet phone services began to spring up, traditional long-distance carriers were concerned about loss of business due to people switching to less expensive Internet-based phone services. (While not necessarily CELP-based, there are many formats, videoconferencing systems with small video cameras and microphones can also be used with appropriate software to transmit conversation over the Internet, often without charges other than the Internet access itself.)
circuit switching	A type of end-to-end transmission system commonly used for phone connections in which the resources are allocated to a specific call for its duration and are not usually available for other purposes until the call is completed.
CPDP	Cellular Digital Packet Data. A packet-based open standard released in the early 1990s which is suitable for packet data services for mobile communications to extend landline services for mobile users. CDPD works over AMPS analog voice systems with transmission speeds up to 19.2 Kbps. CDPD is primarily an architectural structure and doesn't prescribe the types of service that can be carried over the system.

DECT — Digital Enhanced Cordless Telecommunications. A set of European wireless standards intended to unify digital radio standards for European cordless phones. It requires more cells than cellular, but supports higher densities.

DLC — Digital Loop Carrier. A telecommunications service provider type that emerged in the early 1970s which utilizes switches and multiplexers to concentrate low-speed services prior to distribution through a local central switching office. It is similar to a Local Loop Carrier in that it provides a physical connection between subscribers and a main distribution frame over copper wires, but of a digital nature.

DTMF — Dual-Tone Multifrequency. Sometimes also called TTMF (touch-tone multifrequency). A signaling method using two specific frequencies.

electronic communication

Defined by U.S. Code Title 18, Part I, Chapter 119 as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(B) any wire or oral communication;

(C) any communication made through a tone-only paging device; or

(D) any communication from a tracking device (as defined in section 3117 of this title)."

ESN — Electronic Serial Number. An identifier associated with wireless communications that is used for location and/or identification. In some devices, the ESN cannot be changed and may include information about the manufacturer. The ESN may further by keyed to services provided by the manufacturer, such as tech support or Web site access.

F-ES — Fixed End-System. A stationary data communications system (non-mobile) in which a mobile subscriber access landline telecommunications services. This is commonly used with computer-based modems.

FISA — Foreign Intelligence Surveillance Act

FWA — Fixed Wireless Access. A wireless radio-based telephone service that works in place of a local wireline loop, with common-carrier phone service. It is commonly used in regions where it's difficult to string wire, such as isolated areas, islands, or temporary installations.

HDSL — High Bit-Rate Digital Subscriber Line

HLR — Home Location Register. The basic service area list maintained on mobile communications subscribers.

IAP — Intercept Access Point. A point within the carrier's system where call information or communications of an intercepted call can be accessed.

ISDN — Integrated Services Digital Networks. A set of standards for digital data transmission that can work over existing copper wires and the newer cabling media. Thus, a traditional phone network can be used for high-speed data transmissions. Part of the difficulty of establishing ISDN services has been that the link to subscribers themselves is still mostly analog and appropriate terminal adaptors have to be installed to set up the service. In addition to this, cable modem services over existing TV cables have made data services available to many computer users at a lower cost than ISDN in many areas, thus hampering the implementation of ISDN services. ISDN is a flexible system allowing both voice and data communications over the same 'line.' There are two basic types of ISDN service, Basic Rate Interface (BRI) and Primary Rate Interface (PRI).

ITU	International Telecommunication Union. The ITU is based in Geneva, Switzerland and provides education and standards to the telecommunications industry. The ITU evolved from the Telegraph Union which was formed in 1865 (formerly CCITT).
J-STD-025	A Telecommunications Industry Association interim standard for defining services and features to support lawful, authorized electronic surveillance.
JATE	Japan Approvals (Institute) for Telecommunications Equipment. A Japanese regulatory agency, established in 1984, which is roughly equivalent to the Federal Communications Commission (FCC) in the U.S.
LEA	law enforcement agency
MFJ	Modified Final Judgment. This was a historic seven-year antitrust lawsuit that concluded in the mid-1980s between the U.S. Justice Department and AT&T in which AT&T was eventually divested. AT&T was permitted to retain Bell Laboratories and AT&T Technologies, but the Regional Bell Operating Companies (RBOCs) were banned from manufacturing. Local Access Transport Areas (LATAs) were created rather than retaining the existing local exchange boundaries.
MIN	Mobile Identification Number. An identifier associated with wireless communications.
MMCX	Multimedia Communication Exchange. A commercial phone/data server software developed by AT&T for providing multimedia services for private phone branch exchanges (PBXs).
MSC	Mobile Switching Center
MTSO	Mobile Telephone Switching Office
NGDLC	Next Generation Digital Loop Carrier. Evolved from Digital Loop Carriers in the 1980s, NGDLC provides telecommunications services based on very-large-scale integration technology intended for use over fiber optic or hybrid optic/copper wirelines.
NPRM	Notice of Proposed Rule-Making
oral communication	Defined by U.S. Code Title 18, Part I, Chapter 119 as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication."
PBX	Private Branch Exchange. A local, internal multiple-line phone system that is commonly found in business and educational environments. You can generally tell you are using a PBX system, if you have to dial '9' before placing an outgoing call to a destination not included on the exchange. Exchange 'locals' are numbers within the exchange to designate individual phones.
PCS	Personal Communications Services
POTS	plain old telephone service. The basic analog communications over copper wires that existed for many decades.
roaming	Engaging in a wireless call while traveling outside of a subscriber's 'home area,' the area in which the basic service is established. Roaming charges, like long-distance charges on a wired line, tend to be higher than the basic service charges. By the year 2000, large carriers were starting to announce widespread coverage with reduced roaming restrictions.
SPCS	Stored Program Control Switch. A type of metropolitan communications switch introduced in the 1960s that is gradually being replaced by digital switches.

SXS	step-by-step. Used with regard to the old electromechanical communications switches used at the turn of the century to route traffic. A few rural SXS systems still exist but they are quickly disappearing.
TSCM	Technical Security/Surveillance Countermeasures
wearing a wire	The wearing of a hidden microphone and transmitting or recording device for the purpose of covertly monitoring or saving the information and characteristics of a personal communication.
wire communication	Defined by U.S. Code Title 18, Part I, Chapter 119 as "... any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such terms does [sic] not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit."
wiretap	*n.* Strategies and equipment set up to access or intercept the contents of a communication, usually a voice call over a telecommunications network. Taps are most commonly made over copper wires, but means to tap directly into the phone unit or communications over fiber optic cable also exist. The term is now used in a broader sense to include 'listening in' on and recording wireless communications as well. Given the increasing complexity of communication and growth of wireless transmissions, the most effective taps are now usually at the source or destination or through switching systems enroute.