

Wireless Options: Freedom vs. Security

September 2005



National Court Reporters Association

8224 Old Courthouse Road • Vienna, VA 22182
703-556-6272 • www.NCRAonline.org

Wireless Options: Freedom vs. Security

By Gary Robson

Wireless communication is not a goal for the court reporting community. Rather, it is the means to a goal. Wireless technology allows court reporters more freedom and flexibility in delivering transcripts — especially the near-instant realtime delivery that has become the hallmark of the court reporting profession in the past two decades.

From the earliest days of computer-integrated courtroom and total access courtroom systems, court reporters have worked to connect their computer systems to the computers used by attorneys and judges. More recently, realtime transcripts have provided people who are deaf and hard-of-hearing full access to our legal system. Before the availability of reliable and affordable wireless communications, providing access involved stringing wires across courtrooms, drilling holes in walls, pulling up carpets, and otherwise marring courtrooms and deposition suites. Universally accepted wireless protocols have obviated this unaesthetic mass of wires.

As the wiring problem fades away, however, a new problem arises: Security. Wireless technology allows a visiting defense attorney to easily tap into the realtime transcript, but it could also allow the unauthorized newspaper reporter in the hallway to intercept the transmission. Worse, an unprotected wireless network could allow jurors to view disallowed testimony, bench conferences, or even connect to the Internet and read press accounts of the trial.

We will examine the technologies behind wireless communication, their applicability to the court reporting profession, and the security risks involved.

Wireless Technology and Terminology

The meaning of the term “wireless” has changed dramatically since Nikola Tesla and Guglielmo Marconi pioneered wireless communications by radio waves just over a century ago. Radio, television, cellular telephones, and satellite communications are all valid examples of wireless technology, but, today, the term generally refers to data transmission without cables — communication between computer equipment — and that is how the term will be used throughout this article.

Today, the majority of wireless communications in the computer field use one of two protocols, known as Bluetooth and Wi-Fi. Both have their place in court reporting technology, as they have decidedly different applications.

Bluetooth

A group of devices grouped around a computer and communicating without wires is called a wireless personal area network, or WPAN. The devices can include key-

boards, mice, personal digital assistants, cell phones, and printers. The Bluetooth protocol allows for one “master” device (typically the computer) to work with up to seven “slaves.” Bluetooth is a short-range protocol, with a specified maximum range of 10 meters for the most commonly used variety. In court reporting, the most obvious application of Bluetooth would be in connecting stenotype keyboards to computers. Manufacturers of stenotype equipment, as well as third-party vendors, are already offering this option.

Bluetooth was designed for battery-powered devices, hence its short range and low power requirements. It operates in a frequency range not licensed by the FCC (2.4 GHz), which makes it subject to interference from other consumer devices. To avoid this interference, the Bluetooth protocol divides the frequency range into channels, and devices change channels up to 1,600 times per second.

Bluetooth can either be integrated into a device or retrofitted using plug-in cards or USB adapters.

Bluetooth is named for King Harold Bluetooth, who unified warring tribes of Denmark, Norway, and Sweden during his rule in the mid-900s. The Bluetooth protocol was intended to bring together diverse electronic equipment in the same way.

Wi-Fi

For longer-range communications with more devices, the Institute of Electrical and Electronics Engineers developed a set of specifications known collectively as IEEE 802.11. The base protocol has been enhanced several times, and there are two varieties of 802.11 currently in widespread use: 802.11b (usually just called 11b) and 802.11g (similarly 11g). The term Wi-Fi is used as a generic reference to any of the 802.11 protocols.

Like Bluetooth, Wi-Fi operates in the unlicensed 2.4 GHz frequency band, which makes it vulnerable to interference from other consumer electronics. This problem is less of a concern in the courtroom than in a private home, where microwave ovens, baby monitors, wireless video game controllers, and some cordless phones can cause trouble with a Wi-Fi connection.

Such interference, however, is not a new problem. According to a report from the Administrative Office of the U.S. Courts,¹ cellular phones in standby mode have already been found to interfere with digital tape recording systems in courtrooms, thus making it even more critical that a human being (such as a court reporter) monitor all forms of transcript production.

Uses For Wireless Technology in Court Reporting

The obvious places to implement wireless communications are where wired communications are already in use. Aside from power cables, the only wires coming out of the typical court reporter's notebook computer are those that connect to the stenotype keyboard and to an attorney's or judge's computer. Eliminating those wires is the obvious first step for wireless technology. It is not, however, the only step.

Stenotype Keyboards

Traditional "QWERTY" keyboards have always been components of larger devices such as typewriters, keypunch machines, dedicated word processors, and computers. The stenotype keyboard, however, began as a stand-alone device. Only as realtime court reporting has become common over the past two decades have stenotype keyboards been widely connected to computer systems.

Although connecting a stenotype keyboard to a computer brings dramatic benefits with realtime technology, it also restricts free movement of the court reporter. At first glance, this concern seems trivial, but this decreased mobility can affect court proceedings. Probably the most obvious example would be a bench conference in court. For the court reporter to move to the bench without stopping the flow of realtime, the stenotype machine must be tethered to the court reporter's computer by a lengthy cable. Hundred-foot wires coiled on the floor are not unusual.

A similar situation arises for the deposition reporter. Will there be a power outlet where the reporter sits, or will the computer have to be halfway across the room? Will arrival of other parties partway through the deposition require seating to be changed at the table? Must the reporter work in an unusually tight space? Not knowing the answers to these questions in advance requires court reporters to carry unnecessarily long cabling on depositions.

The solution is Bluetooth. Stenotype keyboards like the élan Mira G2, Gemini, Stylus, and Passport all have optional Bluetooth available from the manufacturers. Third-party products like the StenoCast X1 allow Bluetooth to be retrofitted into any computer-compatible stenotype machine. After the one-time installation and configuration is complete, no setup is required. With a typical Class 3 Bluetooth connection, the court reporter will then have freedom to move about with the stenotype machine anywhere within a 10-meter (33-foot) radius of the computer.² The relatively short range limits potential interference with devices such as the microwave oven in the break room across the hall.

Because stenotype machines are typically freestanding on a tripod and usually have integral batteries, the court reporter is free to move about the conference room or courtroom without interrupting the flow of realtime text. The Bluetooth device in the stenotype machine does lower the battery life, but the system was designed for this type of application, so the power draw is small. External Bluetooth adapters like the StenoCast X1 have their own batteries and don't draw power from the stenotype machine.

Attorney and Judge Access

Attorneys and judges have grown accustomed to having live access to the transcript through computer-integrated courtroom and total access courtroom technology. Over the years, a variety of communication technologies have been used to connect the court reporter's computer-aided transcription system to attorneys and judges. All of the systems have been based on a dedicated transcript browser program such as CaseView, Bridge, iBinder, LiveNote, and Summation.

The first systems were interconnected using serial communications, often requiring dedicated splitters for connecting multiple computers. Later, systems such as Total Access for Windows operated across local area network (LAN) systems such as Novell and Microsoft's early networks. With the advent of the Internet, communications between the CAT system and the transcript browser could be standardized and can now operate over virtually any type of network wiring - or no wiring at all.

Before the advent of Wi-Fi, court reporters had to carry a collection of wires, switches, and splitters to accommodate attorneys who wished to connect. Today, courtrooms can have a permanently installed Wi-Fi access point, and deposition reporters need only a card in their notebook computer to establish an ad-hoc network in any conference room. Consider, for example, Courtroom Connect, a company that specializes in establishing wireless Internet service throughout the courthouse that court reporters can easily employ.

For reporters who have already invested in realtime systems and transcript browsers that don't support networking, wireless can be retrofitted. Systems like the StenoCast X7 connect to the serial ports on the CAT system and the attorneys' and judge's computers, creating a wireless replacement for a wired system. The StenoCast X7 uses the longest-range Bluetooth configuration, Class 1, with a range of up to 100 meters (328 feet). This approach has its disadvantages. It won't work with existing Wi-Fi equipment, attorney computers must have serial ports or adapters, the court reporter must carry around the equipment, and it's much more expensive than Wi-Fi. But it is simple and quick to install, with no software updates required.³

Wireless technology certainly isn't necessary for realtime systems, but practical considerations have often limited the implementation of realtime in the courts. It does little for the appearance of a stately courtroom to have wires duct-taped to the floor or holes drilled in the walls, and it is difficult to conduct dignified proceedings when a witness trips over a cable and sprawls headlong on the floor.

Courtroom Accessibility

Now that Communication Access Realtime Translation (CART) reporting has become widespread and easily accessible, people who are deaf and hard-of-hearing can participate in all aspects of the legal system. There are deaf and hard-of-hearing attorneys, judges, witnesses, litigants, and jurors.

It is easy to arrange people around a conference table so that CART providers can sit with their clients. It's much

more difficult in a jury box or a crowded defense table. By using wireless technology in a courtroom, CART providers can be positioned farther from their clients-anywhere they can clearly hear what's going on. A "view only" screen on a handheld computer or PDA is all that the person who is deaf or hard-of-hearing needs. Even Web-enabled cell-phones can receive realtime or near-realtime text feeds.

Simultaneous Editing

When edited certified transcripts are required very quickly, court reporters can either work with a scopist, who edits the transcript as it is written, or in pairs, where one reporter writes as the other edits. Even where CAT systems are designed to allow one person to edit as another writes realtime, the presence of another person in court, typing and checking reference documents, could be distracting.

With wireless connectivity, it is easy to either locate the court reporter's primary computer outside the courtroom or conference room, or connect it to a second computer nearby. Some CAT systems from companies like Stenograph and Cheetah allow editing and realtime simultaneously on a single computer. Other companies, such as ProCAT, have designed software specifically to allow a remote connection for editing. For the former, a variety of "remote control" applications are available, including the venerable pcAnywhere software.

Backups and Redundancy

As with any other network connection, a wireless connection can be used to automate backups. If the court reporter's CAT system is connected to the courtroom network, the transcript can be copied periodically to another system with no intervention from the reporter.

Security Concerns

Since mankind first developed possessions worth protecting, guardians and thieves have waged a war of technological escalation. Locks begat lock picks, chains begat bolt cutters, and computers have generated a massive array of "cracking" tools designed to steal data.

In its simplest form, Wi-Fi provides an access point that can be used by anyone within its physical range. Such "open" access points launched the "war driving" craze, which is when people with Wi-Fi cards in their notebook computers cruise around town checking for available connections. Having such people parked in front of a courthouse or law office, reading confidential transcripts, would be a serious problem.

Security is a serious consideration for any wireless installation, and this concern is even more true when dealing with sensitive documents in our legal system. Any deployment plans should be reviewed by a professional and should use equipment that has been checked and verified as secure.

Entire books have been written about the security concerns in wireless networks, and security is on the agenda at virtually every conference about wireless technology. Although designing secure systems is highly complex, the fundamentals behind security are fairly straightforward.

Concealment

The first and simplest step is to not advertise the presence of your wireless network. Access points have an option to broadcast the SSID, or service set identification. If this feature is enabled, anyone operating a computer with a Wi-Fi card will "see" your network. Computers can even be configured to detect such "open" networks and connect to them automatically. Turn off the SSID broadcast for your network, and turn off the access point entirely when it isn't in active use. Strangers can't connect to the network unless they find out the SSID and the network is running.

Password Protection

Even the simplest wireless networks have the option for password control. Passwords should be enabled and changed regularly. In a sensitive environment, changing them daily is appropriate. Authorized parties can get the day's password when they set up in the morning.

Encryption

Although it is impossible to prevent unauthorized personnel from intercepting data when it is broadcast on the public airwaves, it is possible to make the information useless to them. The best way to accomplish this is through encryption. Encryption systems range from the simple ciphers we learn as children (A=1, B=2, C=3, etc.) to highly sophisticated algorithms based on factoring huge prime numbers. The systems used in computing today are called "public key" systems, which is when the person doing the encoding (the court reporter, in this case) creates a "key pair" for the encryption. The encryption can be thought of as a simple pair of passwords. The private key, known only to the court reporter, is used to encode (lock) the data and the public key is given to attorneys and judges to decode (unlock) it.

This same system is used for digital signatures on transcripts. The court reporter is the only one in possession of the private key, so it is easy to verify that a given transcript was, in fact, encoded by that court reporter. Each key pair is unique. If the reporter's public key unlocks the document (or signature block), then the reporter's private key must have been used to encode it.

Because court transcripts are often sensitive documents, federal courts are required to use encryption. These courts must use government-approved encryption standards known as Federal Information Processing Standard (FIPS) standards. There is a changeover in process today, as the FIPS 46-3 Data Encryption Standard was recently withdrawn by the Secretary of Commerce,⁴ and courts are switching to FIPS 197.

Even for local courts and deposition offices that may not be required by law to use encryption, it is strongly recommended by virtually all industry experts. When putting together a new system, look for compliance with FIPS 197, known as the Advanced Encryption Standard (AES), because that will ensure compatibility with federal systems and provide the greatest security.

Firewalls

A firewall is a piece of software or hardware that filters access to a computer by blocking unauthorized intrusions. There are many services offered over a typical network. E-mail, Web services, file transfers (e.g., FTP), streaming audio and video, and many other data types routinely traverse networks. Firewalls should be configured to block all but the required services.

Modern operating systems like Windows XP have built-in firewall software that is relatively easy to configure. Your firewall should be set up to block anything that you don't want to explicitly allow through the wireless connection. As an example, if you have no need to allow e-mail over your wireless network, disable it.

Secure Data

Along the same theme as firewalls, if a Wi-Fi network is being set up to broadcast transcripts, then transcripts should be the only data available on that network. Use password-protected folders for everything else, or place it in "unshared" areas of your hard disk.

CART

CART was discussed earlier in a courtroom setting, but only a small fraction of CART work today takes place in the court system. CART providers act as interpreters for that large majority of people who are deaf and hard-of-hearing who don't know sign language.

Wireless technology is not required for CART work. CART providers have been working for years while tethered to their screens. In many cases, however, the wires have interfered significantly with CART.

One of the most common venues for CART reporting is education. In large classrooms with theater-style seating, there is rarely room for the CART provider to squeeze in next to the student, and it can be difficult for the provider to hear. Using wireless technology, the CART provider can sit in the front of the room, off to one side, able to see and hear everything perfectly. The client — or clients, as this technology could easily accommodate multiple students — sit in their normal seats and use notebook computers, PDAs, or BlackBerry devices to read the CART provider's text.

This same system can be used in tight quarters such as doctor's offices.

Closed Captioning

In a sense, closed captioning was the first wireless application of realtime court reporting, as the realtime text is transmitted in the "on-air" video signal to home television sets. In the sense of this report, however, closed captioning is likely to be the last stenotype application to benefit from wireless communications.

Like an official court reporter, a stenocaptioner works from a fixed location. Whether that location is a broadcast site where the captioner's computer is wired directly to a caption encoder, or a home office where the captioner's computer is connected to the encoder through a modem, there is little need to move about.

Unlike court reporting, where the recipient of the realtime text is usually in the same room, captioners serve a widely diverse audience. The output from a stenocaptioner's realtime system may be viewed simultaneously by millions of people all over the planet, something Wi-Fi simply can't aspire to.

There are some niche applications, such as connecting multiple captioners in a redundant system, but, for the most part, wireless technologies such as Bluetooth and Wi-Fi do not bring much to the table for most stenocaptioners.

Projections

Most of the currently planned advances in wireless technology are evolutionary rather than revolutionary. Although technologies such as WiMAX may increase both the range and the transmission rates of Wi-Fi, they won't introduce any fundamental changes to the use of wireless in court reporting. Reliability and security will most likely increase incrementally over time — not in a single large jump.

Widespread acceptance of Wi-Fi and Bluetooth will likely increase the number of applications, as developers create more programs and devices specifically for wireless environments. Court reporter education will change dramatically when every student in the class is connected to the instructor's computer. Instructors can then also monitor in realtime how the students are doing on drills and speed trials.

One significant change will be in expectation. Attorneys will consider connecting to the court reporter with Wi-Fi just part of their daily routine. Just as the proliferation of cellular telephones has caused pay phones to be removed from many courthouses, Ethernet connections in conference rooms are likely to grow less common in coming years, not more common.

JCR Contributing Editor Gary D. Robson has written 12 books and more than 200 articles, many of them about captioning and reporting. For more information, see his Web site at www.robson.org.

Endnotes

1. *Considerations in Establishing a Court Policy Regarding the Use of Wireless Communication Devices*, available at www.uscourts.gov/newsroom/wireless.pdf.
2. The StenoCast X1 is a Class 2 device, which provides a range of between 20 and 40 meters (66 and 131 feet). It should be noted that the X7, or "send" unit, must be plugged into AC. StenoCast recently announced the release of the X1-Lithium model. It allows most stenographic machines to write wirelessly to the court reporter's computer. StenoCast X1-Lithium was developed specifically to allow reporters to move freely throughout the courtroom without cables.
3. Note that drivers are needed if the computer is running Windows 2000 or XP SP1.
4. *Federal Register*, Vol. 70, no. 96, Thursday, May 19, 2005.