Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED
JAN 27 1999
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of:	)	CC Docket No. 97-213
Communications Assistance for Law Enforcement Act	)	

DECLARATION OF JOHN W. CUTRIGHT

I, John W. Cutright, an Electronics Engineer, hereby declare as follows:

1. I am a graduate of Devry Institute of Technology, with a Bachelor of Science Degree in Electronics Engineering Technology. I first worked for GTE as a Network Support Technician, and then I worked at LCI International (now Qwest Communications) for five years. At LCI, I held a position in 800-service design as a design technician. I was then promoted to positions as a Network Design Engineer, Supervisor of Network Design and Switch Engineer. In May, 1998, I joined the Federal Bureau Of Investigation as an Electronics Engineer.

In addition, I am a member of the Army Reserve, serving as a Senior Telecommunications Terminal Device Repairman and supervising the Communications and Electronics Section of my unit. I have six years' experience in this field, including six months' participation in Desert Storm.

I am familiar with the surveillance capabilities that the government is seeking in this proceeding. I submit this declaration to provide technical information relating to those capabilities. To begin, I will discuss background information about the Public Switched Telephone Network and

related telephony concepts. I will then turn to the individual items on the government's "punch list" and discuss the technical matters that relate to those items.

A. Elements of the Public Switched Telephone Network.

2. Telecommunications, in its most general description, is the passage or sharing of information through electromagnetic means. The term "electromagnetic means" refers to some form of electrical, optical or other signal. Today's telecommunications network, commonly referred to as the public switched telephone network (PSTN), is the result of years of technological advances and the introduction of new services and features in response to evolving customer needs and demands. But the basic, underlying intent of telecommunications has remained the same since its inception in 1876, when Alexander Graham Bell first used a "telephone" to communicate to his assistant, Thomas Watson. What follows is a basic description of the various elements that comprise the public switched telephone network as it exists today.

Physical Elements.

3. Telephone device. In voice communications, the telephone device, or set, has six primary functions. The telephone set (1) provides a means for a subscriber to alert the telephone company that a call needs to be made (off-hook), or is complete (on-hook); (2) provides a means for the telephone company to indicate to the subscriber that it is ready to accept dialing information (dial tone); (3) provides a means for a subscriber to alert the telephone company of the number the subscriber wants to reach; (4) converts voice sound into electrical signals to be transmitted; (5) provides a means for the telephone company to alert the subscriber of an incoming call (ringing); (6) converts incoming electrical signals into sound to be listened to by a subscriber. With a telephone

set that accomplishes these six functions, a subscriber can call or be called by anyone else connected to the network.[1]

4. Network. In the very early days of telecommunications, there was no way for telephones to communicate other than to be connected *directly* to each other. What this means is that every telephone had to be physically connected to every other telephone. For a very small number of telephones (perhaps three or four) it made sense to connect each telephone to all other telephones. But as the number of telephones grew, it became apparent that a centrally located mechanism to connect calls would better serve subscribers.

Today, all land-based, or wireline, telephones are physically connected to a local *central office* that houses switching equipment. The most common connection consists of a pair of copper wires, known as the *local loop* or line. These copper wires transmit and receive electrical signals sent from and to a telephone set during a telephone call. In a residential neighborhood, the wire coming from a house and running to the pole is referred to as the *drop wire*. The drop wire from each house joins other similar wires (from other homes in the neighborhood) to form a *distribution cable*. Eventually, several distribution cables join together to form a *feeder cable* that terminates at the central office.

Central offices, sometimes called *exchanges*, serve all of the telephone sets in a specific geographic area. The size of these areas, called *exchange areas*, varies according to the density of telephones (e.g., rural areas tend to be much larger than urban areas). The central office acts as a hub for all the cables and wires necessary to connect every subscriber in a given geographic area. These connections make up the *local exchange*, and the telephone company that offers service in this area

[1] In this document, the word "subscriber" is used as the context may require to denote either an individual who is placing or receiving a telephone call, or an individual who contracts with a telecommunications carrier for a range of services.

is called the local exchange carrier (LEC). Therefore, any subscriber who initiates a call to any other subscriber within the same local exchange area is connected, or switched, to that subscriber either through a local exchange switch or through a remote switch serving the exchange area.

Some calls originate in one local exchange area but need to terminate in a different local exchange area. Each central office switch is connected to other central office switches for the purpose of completing such calls. Because the United States covers a large geographic area and includes a very large number of telephone subscribers, it is impossible to connect all of the central office switches directly. For this reason, local exchange switches are connected in a "hub and spoke" relationship -- connections called *trunks* lead from central office switches to switches called *tandem switches*, that are used to connect the trunks. Switches can thus connect not only subscribers (via telephone lines), but also other switches (via trunks).

5. The Switch. The switch makes connections between other network elements, such as the telephone lines of two subscribers. The earliest type of switching was manual. A subscriber who wanted to place a call would turn a crank, generating an electrical signal and lighting a lamp at the central office. The operator in the central office would respond by coming onto the subscriber's line. The subscriber would verbally give the operator the number he or she wanted to call, and the operator would either make a direct connection to another subscriber within the same local exchange area, or contact another operator to reach a subscriber in a different local exchange area. In the case where the subscriber intended to reach someone in another city, a long distance operator would connect two local operators.[2]

---

[2] Today, the distinction between local and long distance calling depends upon whether the call needs to travel outside the Local Access Transport Area (LATA) where it originated. A local exchange carrier provides service between local exchanges within a LATA, and long-distance carriers provide service for calls that originate in one

The next generation of switches consisted of automatic, or mechanical switches. These switches responded to the pulses created by a rotary dial on the subscriber's telephone set. Although these switches are still in use today, they are largely located in rural areas and are being replaced by more modern switches.

Most switches in the network today are electronic switches. Modern central office switches are entirely electronic. Electronic switches can be based on either analog or digital technology. Modern electronic central office switches are able to provide a vast number of switch-based features and services through the use of Analog Stored Program Control Switches (Analog-SPCS) which were introduced in the mid-1960s, and became the primary switching technology for large metropolitan areas in the 1970s and 1980s. A significant number of Analog-SPCSs remain in service, but they are being replaced by digital electronic switches. Digital Stored Program Control Switches were introduced in the early 1980s.

As mentioned briefly in the above discussion concerning central offices, there are two major categories of switches: local and tandem. A local switch can connect a subscriber's line to another subscriber's line, or to a connection (trunk) to another switching system. A tandem switch connects trunks of one switch to trunks of other switches. Remote switches constitute a third, smaller category of switch. These are local switches where a physical portion of the switch and some of the switch software is located away from the main or *host (exchange)* switch. Host switches can serve several remote switches, and are connected to the remote switches with connection links. This type of distributed network is most common in expansive rural areas where the distance between subscribers and host switches is very large.

LATA but terminate in another LATA .There are over 150 LATAs in the United States.

Switches have numerous resources that are shared among the subscribers served by the switch. Because all the subscribers of a given switch will not attempt to use their phones simultaneously, a switch can be "engineered" to meet very specific demands. For example, a switch serving a sales office with a large number of outgoing calls needs to accommodate more simultaneous attempts than a switch serving a residential community. One example of a shared switch resource is access to dial tone generators, the mechanism a switch uses to alert a subscriber to begin dialing a destination number.

Local exchange switches also allow subscribers a choice between long distance carriers, either by pre-subscription, or on a per-call basis. Every subscriber must choose a long distance service. Subscribers may nonetheless change their long distance provider for the duration of a single call by dialing "1010" and a *carrier identification code*, followed by the destination phone number.

Other Telephony Concepts.

6. Signaling. "Signaling" describes the exchange of information between pieces of equipment within the telecommunications network that are used to provide and maintain service. Signaling may occur over two separate *bands*: a voice frequency band (which carries the voice communications and some signaling information), and a *signaling link*, which is a separate digital channel for carrying signaling information. There are two major types of signaling: (1) in-band signaling, (2) out-of-band signaling. *In-band signaling* is signaling that is carried over the voice frequency band; *out-of-band signaling* is signaling that is carried over the signaling link.

In-band signaling is made up of tones that pass within the voice frequency band, and are carried along the *same* circuit as the voice path that is being established by the signals. A significant portion of the signaling that is initiated by callers in the United States today (e.g., request for service,

dialing, disconnecting) is in-band signaling. Most of that signaling is performed through the transmission of tones (*multi-frequency dialing*).

The modern form of inter-switch signaling, however, is out-of-band.[3] Out-of-band signaling does not take place over the same communications path as the conversation. This form of signaling establishes a separate digital channel for the exchange of signaling information (the signaling link). Signaling links are used to carry all the necessary signaling messages between network elements. Thus, when a call is placed, switches use their signaling links to transmit information needed to route the call through the network (for example, the dialed digits and the trunk selected), rather than using the resources that carry the voice conversation.

Signaling System 7 (SS7) is the architecture used for out-of-band signaling to establish calls and to perform the billing, routing, and information-exchange functions of the public switched telephone network. SS7 both identifies functions to be performed by a signaling system network and provides a protocol that allows those tasks to be performed . SS7 is used only for signaling between network elements.

The operation of SS7 is perhaps best understood through a description of how an ordinary call would be set up using SS7. ***A*** (a caller) goes off-hook, either by lifting the handset or by pressing the speaker key, and the switch serving ***A*** senses the change in state and determines whether service should be provided. The switch provides dial tone to ***A***. As ***A*** begins to dial ***B***'s number, the switch begins to interpret the digits dialed to route the call. After the first digit is dialed, dial tone is removed from ***A***. After all the digits for ***B***'s Directory Number have been dialed, the switch

[3] Not all out-of-band signaling occurs between switches. For example, out-of-band signaling may also occur between the handset and the switch in Integrated Services Digital Network (ISDN) and some wireless applications. Display information for wireless handsets is sometimes transmitted as an out-of-band signal.

determines if ***B*** resides within its local network (i.e., whether ***B*** is a customer served by that same switch). After it has determined that ***B*** is not within its network, the switch now signals the appropriate resources in order to reserve a circuit for voice communications.

The originating switch signals the terminating switch via the SS7 network that a call to ***B*** is being requested. The terminating switch determines that ***B***'s line is not busy, reserves a voice communication path, and then signals the originating switch over the SS7 network to continue the call.

The terminating switch signals the appropriate resources within its network to establish a path to ***B***. ***B***'s switch generates ringing for ***B***, while ***A***'s switch provides a ring back signal to ***A***. (The switches provide separate ringing signals for their respective parties.) ***B*** can respond to the ringing telephone by going off hook, either by lifting the handset or by pressing the speaker key. The terminating switch senses the change in ***B***'s state and removes ringing. ***A***'s switch removes the ring back signal from ***A***.

The two switches now signal the voice resources they have reserved to establish a voice path between the two switches. ***A*** and ***B*** can now begin talking. As we know from using our own telephones, all of the foregoing steps are completed very rapidly -- within the time that it takes a caller to dial, and the second party to answer. When both parties hang up, both switches send out the appropriate signals to tear down the call and release the network resources associated with the call.

7. Call Flow. To make a simple telephone call, a subscriber picks up the telephone ("goes off-hook") and waits for a confirmation dial tone. The dial tone tells the subscriber that the connection between the subscriber and switch is functioning and that the switch is ready to receive

instructions in the form of the numbers to be used for routing a call. The subscriber then dials a series of numbers, and the switch responds by completing a series of actions to put the call through.

For more complex calling, however, the subscriber may use the "flash-hook key" to let the switch know that the subscriber requires further action, because the flash-hook key allows callers to invoke certain features and services.[4] Pressing the flash-hook key briefly and releasing it within one half of a second during the course of a call tells the switch that the caller wishes to dial another number or to give the switch a new command. For example, a caller with call waiting uses the flash-hook key to move between calls.

More advanced phones may have a special key to perform the functions ordinarily assigned to the flash-hook key. On cellular or wireless phones, the "send" key also performs the flash-hook function.

8. Features and Functions. When Analog Stored Program Control Switches were introduced into the national telephone network, they brought subscribers a variety of new features and functions. As its name implies, a Stored Program Control Switch allows subscribers to control certain features by directing the switch to activate, change or deactivate those features. Features that can be controlled at the switch in this manner are known as Custom Calling Services. They include such commonly-used utilities as Call Forwarding, Speed Calling, and Call Waiting. Today, we refer to the traditional type of services that did not include these switch-based features as "POTS," or Plain Old

[4] On basic telephones, the flash-hook key is the button that is depressed when the phone is put into a resting position in its cradle. When this key is released (usually by picking up the phone), the switch knows that it must send dial-tone to the handset. Conversely, hanging up the telephone depresses this key and notifies the switch that a call has ended.

Telephone Service. Even today, when a subscriber can use a telephone only to place and receive calls, it is said that the subscriber has "POTS."

Many more sophisticated specialized services have been developed since the switch-based features that allow for custom calling were first introduced, particularly as Digital Stored Program Control Switches came on line, and the features described below represent only a sample of today's vast array of available services. Historically, the customer was required to notify the telephone company in advance to make the service available. Today, many of these features can be used without pre-subscription, on a per-use basis.

Generally, Custom Calling Services use resources that are shared by users of the switch. Business efficiency dictates that access to particular features be limited to a pre-determined number of subscribers on each switch. If only 10 percent of subscribers who use a particular switch subscribe to conference calling, for example, then a carrier will only engineer (i.e., design, purchase, and install) enough conference calling capability to satisfy the predicted needs of that number of subscribers. For example, when a carrier offers conference calling, it needs to engineer a number of "conference bridges," (the actual physical facility that allows one subscriber to connect to more than one other call simultaneously) and it will calculate and provide the smallest number of bridges that will satisfy conference calling needs on the switch. Carriers must also keep track of the pre-subscription features and services associated with each subscriber's account so that they can restrict access to particular facilities to those subscribers who have signed up (and paid) for them.

a. Call Forwarding

Call Forwarding allows a subscriber to redirect incoming calls to another telephone number. A subscriber activates Call Forwarding by dialing a call forward activation code (e.g., *72) followed

by the directory number to which the calls are to be forwarded. Electronic switching systems are capable of redirecting any incoming call either to another directory number within the same local exchange, or to another, exchange over a trunk connection. When the local switch redirects a call, the call is never transmitted over the line connecting the subscriber's telephone set to the network. Instead, the call is rerouted at the switch and transmitted to the telephone set associated with the forwarded-to number.

In its earliest versions, the call forwarding feature could be activated and deactivated only from the subscriber's telephone set. Today, with the introduction of remote activation of call forwarding, the forwarded-to number can be changed from any telephone.

b. Speed Calling

Speed Calling allows any subscriber, on request, to associate a set of abbreviated numbers (i.e., one- or two-digit numbers) with the telephone directory numbers of frequently called parties. Speed Calling is a central office, switch-based feature.[5] Speed Calling codes (e.g., *74, or *75) allow subscribers to alter their lists of frequently-dialed directory numbers. Some versions of Speed Calling permit subscribers to change the assignment of directory numbers in real time (i.e., during the course of a call), or to change the number assignment remotely from a telephone set that is not associated with the subscriber's directory number.

c. Conference Calling

Conference Calling is a feature that allows a subscriber to talk to more than one person simultaneously. Conference Calling allows a subscriber to add additional parties to a call that is in

[5] Some of today's telephone sets allow a subscriber to store frequently-dialed numbers locally on the telephone set, but this handset-based capability is not Speed Calling.

progress. When Conference Calling is invoked, the subscriber temporarily suspends an ongoing conversation, alerts the switch (by depressing the flash-hook) that a second call needs to be made, connects to a third party and then re-connects (again by depressing the flash-hook) to the initial call. At this point, all three parties may participate in the conversation.

In addition to three-way conference calling, some carriers offer a six-way conference calling feature, which supports conversations that include up to six participants.

d. Call Transfer

Call Transfer is a feature that is similar to Conference Calling, but it allows the subscriber of the service to drop off the call while the remaining parties continue the conversation. This feature is primarily offered to business subscribers.

e. Call Waiting

Call Waiting allows a subscriber who is already participating in a telephone call to become aware of a second incoming call when the switch sends either a tone or a light signal to indicate the presence of the second call. The feature allows the subscriber to place the first call on hold to answer the second call. The subscriber can then alternate between the two other parties, if he or she wishes, by pressing the flash-hook key.

f. Custom Local Area Signaling Services (CLASS)

Custom Local Area Signaling Services (CLASS) are call management features that offer subscribers control over calls. CLASS features are available through both Analog and Digital Stored Program Control Switches that are equipped to support the Common Channel Signaling/Signaling System-7 (CCS/SS7) capabilities. CLASS features place control of the call in the hands of the called and calling parties. CLASS features are unique because they allow the subscriber's switch to react

intelligently to the telephone number of an incoming call. CLASS features allow customers to create, modify, activate, and deactivate lists of calls for screening, at the customer's convenience. CLASS features include the following:

Automatic Recall allows a subscriber to activate a feature by dialing a code (e.g., **69)*, that automatically re-dials the number of the last incoming call, regardless of whether the call was answered. The subscriber need not know the caller's number.

Selective Call Forwarding allows a subscriber to activate a feature by dialing a code (e.g., **63)* to define a list of (incoming) telephone numbers and assign to each a *different* forward-to destination number.

Selective Call Rejection allows a subscriber to dial a code (e.g., **60)*, that will allow the subscriber to define a list of (incoming) telephone numbers to which the subscriber's switch will play a recording and terminate the incoming call.

Automatic Callback allows a subscriber to dial a code (e.g., **66)*, that allows a subscriber who makes an outgoing call and gets a busy signal to instruct the switch to retry the number for a short period of time (usually 30 minutes), so that the subscriber does not have to redial.

9. Feature Keys. Older telephones, with rotary dials, used pulse-dialing. Those pulses were sent to the telephone switch so the switch could route the call. Newer telephones have a numbered keypad and use tone-dialing. The tones serve the same purpose as the older pulses. Early feature keys substituted for pressing multiple buttons, but still resulted in sending tones for the substituted keys. The most recent digital telephones send data messages in addition to, or in place of, tones. Some switches serving these advanced digital telephones can accept only such data messages. The switch can then respond to the messages with recorded announcements to confirm or deny the

subscriber's requests. Given the trend toward digital control of communications, feature codes may soon be as rare as rotary dial telephones.

The subscriber may also use feature codes, such as "*69" to return a call or "*70"to turn off call waiting. Although different carriers and manufacturers were initially inconsistent in assigning the specific code numbers to each "feature," such as call waiting or call transfer, the industry has made efforts to try to standardize codes.

Some telephones have extra keys that perform special functions. Examples are keys for Call Hold, Call Transfer, Call Forward, and Conference Calling. These keys help simplify the use of features by replacing the pressing of a series of buttons with the pressing of a single button, so that the user does not have to remember feature codes and sequences. The "smart" phone will translate that action into the proper signal that the switch understands. Early versions of feature keys were hard-wired on the telephone handset, while recent versions have enabled users to program generic keys to assume the role of any specific feature. The program that interprets the meaning of the keys may be located within the telephone itself or may be located on the switch to keep handsets simple and cheap.

Recent developments have led to the use of "soft keys," where keys are more dynamic and context-dependent. That enables handsets, such as those used for cell phones, to have fewer keys and to allow those keys to perform multiple functions. Because the service program is contained within the network, a menu-driven dialog between the handset and the switch determines how calls and features are controlled. The switch may send a text message to the handset for display. Each selection on the menu corresponds to one generic key on the handset. The subscriber presses a key to signal the switch, which may respond with another menu of options. The menu itself provides the

context for determining the meaning of subsequent keystrokes. The advantage to the service provider is that services can be modified or new services introduced without requiring the handset to be modified or upgraded. The advantage to the subscriber is the ability to use features by simply selecting options without having to learn and remember codes.

10. Timing and Synchronization.

Switches cooperate to setup calls by sending data messages to one another. Each switch must respond very quickly to each received message so that the sequence of messages is completed before the subscriber starts thinking that something is wrong, hangs up, and tries to initiate another call, starting the whole sequence over again. As a result, switches are designed to be able to set up about 360,000 calls an hour, or 100 calls a second. That means that a call can be completed (based on receipt of the final message) every 10 milliseconds.

In order to complete a telephone call, as many as 10 messages must be sent back and forth between switches and other network elements. In cases where a telephone call is completed within one second, the time between the receipt of one message and the generation of the next message would be less than 1/10 of a second, or 100 milliseconds. In fact, switches scan thousands of lines within 10 milliseconds and can begin transmitting a message within 10 microseconds (1/10,000 second) of receiving the message to which it must respond. Compared to such response times, the 3 seconds suggested in FBI/DOJ's Petition for delivering call event messages can be considered a snail's pace. Using 10 milliseconds as a guide, a switch could generate 300 messages within a 3 second time frame.

11. Circuit-Switching versus Packet-Switching.

Under some network configurations, the network's communications paths can be used exclusively for the duration of a call by two or more parties and then, when the call is terminated, switched for use by another set of parties. This type of "switching" is known as circuit-switching and it is really a dedicated and continuously connected path for the duration of a given connection. Today, ordinary voice phone calls generally use circuit-switching.

By contrast, most forms of data are sent using digital signals over networks that use *packet-switching*. Through the use of packet-switching, all network users can share the same paths at the same time and the route which a unit of data travels can be varied as network conditions change. This technology uses network resources very efficiently. In packet-switching, a message is divided into *packets*, which are units of a certain size containing data. Network addresses of the sender and of the destination are added to the packet. Each network element looks at the packet to see where to send it next. Packets of the same message may travel by different routes and may not arrive in the order that they were sent. At the destination, the packets of a given message are collected and reassembled into the original message.

12. Wireless. In wireless telecommunications, as the name implies, the subscriber's handset is not physically linked to the switch. Instead, information is transmitted from the handset to the switch using cellular telephone transmitters. A *cell* is the geographical area covered by a cellular telephone transmitter. The transmitter facility itself is known as the *cell site*. Cells can range in size from less than one mile to more than twenty miles in diameter, depending on terrain and the power of the transmitter.

Several coordinated cell sites are called a *cell system*. Cellular telephone subscribers are given access to their cell system, which is essentially local (similar to local exchange areas in wireline). When a subscriber travels out of the range of this cell system, the cell system can transfer the subscriber's service to a neighboring company's cell system without the subscriber's being aware of the change. This process is known as *roaming*.

Cell sites in a wireless system connect to a Mobile Switching Center (MSC), which in turn connects to the wireline telephone system. Once a wireless subscriber's call has reached the wireline network, the call is handled just like wireline calls.

13. Advanced Intelligent Network. The Advanced Intelligent Network (AIN) is a telephone network architecture that separates service and feature related information from switching equipment, and allows new services to be added without requiring switches to be redesigned to support those new services. AIN encourages competition among service providers by making it easier for a provider to add services, and it offers customers more service choices. AIN is recognized as an industry standard in North America. Its initial version, AIN Release 1, is considered a model towards which services will evolve.

B. The Punchlist.

1. Content Of All Parties To A Conference Call.

Conference calling is a set of features that allows a subscriber to talk to more than one person simultaneously (see paragraph A.7.c., supra). A subscriber with the conference calling feature can add parties to a pre-existing, on-going telephone call. The following call flow demonstrates how a conference call is set-up, or, put simply, how a two-party call may become a three-party call:

Party *A* calls *B*, through the normal process of initiating a call. With the call in progress (*A* and *B* connected), *A* presses the flash hook (or the conference key). The equipment serving *A* recognizes the action taken by *A*, and provides *A* with a second instance of dial tone so that *A* may initiate a second outgoing call. During this time, the equipment serving *A* places *B* on hold. *A* has received the second dial tone and *A* calls *C*, through the usual process of initiating a call. With the second call in progress (*A* and *C* connected), *A* presses the flash hook again (or the conference key). As soon as *A* presses the flash hook this second time, a Conference Bridge[6] is seized. All parties are now in a stable talking state.

A may also have a feature (call waiting, for example), that allows *A* to isolate parties *B* and *C* while *A* pursues other calling activity. Thus, if *A*'s call waiting feature alerts *A* to an incoming call and *A* answers that call, *B* and *C* can still be connected to each other through *A*'s conference bridge.

Without the "content of all parties in a conference call" punch list capability, law enforcement will not receive the ongoing communications between *B* and *C* in this scenario, even though the equipment serving *A* makes the communication between *B* and *C* possible. *A* initiated the original call to *B*. *A* initiated the call to *C*. *A* connected *B* and *C* using a conference bridge available only to subscribers of conference calling. The connection between *B* and *C* exists only because the conference bridge serving *A* supports the communication.

---

[6] A single Conference Bridge is one of a pool of resources available to any of the subscribers served by equipment who have subscribed to the resource, and are therefore allowed to access it. Conceptually, this resource is no different from any other shared equipment resource made available to subscribers. For example, dial tone is a resource that is available to every subscriber, but only a portion of those subscribers may receive dial tone at any one time.

Instead of using *A*'s conference calling feature to support their call, ***A, B*** and ***C*** might have chosen instead to arrange a "meet-me" conference. A "meet-me" conference does not use any subscriber's conference calling feature, but is set up by a carrier by pre-arrangement for the sole purpose of providing the capability for the particular conference call. All parties in the conference must call into an attendant (either automated or human), and enter the conference ID and password. The party is then connected to a dedicated conference circuit that is maintained throughout the call until either the last party drops off or the allotted time for the conference circuit has expired.

2. Party Hold, Party Join, Party Drop.

Many features give subscribers direct control over who participates in a particular call. These features include the ability to place someone on hold, to add someone into a pre-existing telephone call (see the description of conference calling, B.1, supra), or to drop someone from a call. In addition, any one of the participants in a multi-party call may drop off the call for a number of reasons (e.g., the participant hangs up).

The equipment that services the subscriber and carries out the subscriber's commands necessarily knows both what features and resources are available to the subscriber and what calling actions the subscriber is taking at any particular time -- without this information, the equipment could not provide service to that subscriber. For example, if a subscriber has conference calling, the equipment is at the ready to respond to the subscriber's instructions to place a pre-existing call on hold and provide the subscriber a second instance of dial tone so that a second call may be initiated. The equipment is designed to join all three parties into a call as soon as the subscriber initiates the necessary action (pressing the flash hook). The equipment servicing a subscriber also need

information about subscribers so that it can monitor the level of resources (e.g., conference bridges, or dial tone generators) available at any given time.

The "party hold, party join, party drop" punch list capability would provide law enforcement with automated, informational messages that identify when a participant has been placed on hold, has been joined into communications, or has dropped from communications. For the reasons set forth above, the network uses all of this information for call processing purposes.

The information that would be provided by the Party Hold, Party Join and Party Drop messages could not be acquired through the Call Identity, Change and Release messages established under the industry interim technical standard J-STD-025 (J-Standard). This is so because the operative concept under the J-Standard (that of call identity) is broader than the information on call composition needed by law enforcement. Change messages are generated only when there is a change in the Call Identity. They do not necessarily report changes in the number or identity of the participants to the call.

The following example illustrates the inadequacy of the messages provided under the J-Standard. Under the protocol provided by the J-Standard, when ***A*** initiates a call to ***B***, an Origination message would be generated and sent to law enforcement. A Call Identity would also be created to identify the call. When ***A*** receives an incoming call from ***C*** and presses the flash hook in response to call waiting, an answer message would be sent to law enforcement (J-Standard does not require that a new Call Identity be created for this new call). Thereafter, ***A*** could use the flash hook freely to converse with ***B*** and ***C*** in turn, changing the composition of the telephone call every time a switch occurred between the parties. The Call Identity status, however, could remain the same and no Change message would be generated.

An example involving conference calling also demonstrates the inadequacy of the messages provided under the J-Standard. Under the protocol provided by the J-Standard, when ***A*** initiates a call to ***B***, an Origination message would be generated and sent to law enforcement. A Call Identity would also be created to identify the call. When ***A*** initiates a second call to ***C*** by pressing the flash hook and dialing ***C***'s directory number, a second Origination message would be sent to law enforcement. The Call Identity status, however, could remain the same and no Change message would be generated. Furthermore, the Call Identity may not change when either ***B*** or ***C*** drops off the call.

This scenario shows the necessity for the party join and drop messages to inform law enforcement that a participant has been added to the call, or has dropped off. Because Change messages are generated only when there is a change in the Call Identity, and not when one party to a multi-party call is added or drops off, the Call Identity message does not provide law enforcement the information it needs to track communications.

3. Subject-Initiated Dialing and Signaling. The composition of a telephone call may change for any number of reasons. In a few, rare instances, the network itself will cause the change (e.g., by inadvertently disconnecting an ongoing call). The vast majority of changes, however, take place because the subscriber interacts with the network. A simple example is call waiting, where a subscriber places an ongoing call on hold so that a separate incoming call can be answered. Other, more advanced, interactions can take place between a subscriber and the network as digital technology becomes more prevalent.

Today's advanced telecommunications technology has introduced "feature keys" and "soft keys," described in Paragraph A.8., above. Briefly, feature keys can be thought of as a fast way of

doing something -- they are analogous to a "macro" in computer terminology. A single use of a feature key may take the place of multiple keystrokes, or it may alert the network to an action that the network must take. "Soft keys" are available on digital handsets (made available primarily by wireless service providers). These keys are more dynamic and context-dependent -- a menu-driven dialog between the handset and the switch determines how calls and features are controlled.

Under these circumstances, where a telecommunications subscriber may use feature keys and "soft" keys to manipulate calls in a flexible and unpredictable manner, law enforcement must have access to subject-initiated dialing and signaling activity if it is to track the destination and composition of calls.

Post-cut-through dialed digits are also an example of subject-initiated dialing and signaling (see also Paragraph B.7, infra, discussing the extraction and delivery of these digits as a separate punchlist item). Long distance calls, credit card calls, and (in some instances) local calls may be set up so that the signaling information necessary to complete the call and reach the intended party occurs after an initial connection, or *cut-through,* has been completed. For example, a subscriber using a credit card to place a call may use his or her local exchange carrier to make a connection to a long distance carrier's 800-number service. Only when the call to the 800-number service is complete (the *cut-through*), will the subscriber be prompted to dial the final destination telephone number of the person the subject intends to reach.

Under the J-standard, only the 800 number to the long distance service provider would be provided to law enforcement -- information that is relatively useless. Law enforcement would be denied access to the telephone number of the party called, because that number was dialed post-cut-through.

4. In-Band and Out-of-Band Network Signaling. Signals sent by the network to the subscriber to inform the subscriber of telecommunications activity, or to solicit action by the subscriber, are equally important in understanding telephone communications. The interaction between the network and subscribers can be expected to increase as telecommunications services and features increase in sophistication.

The network may send signals to a subscriber "in-band" (signals are passed to the subscriber over the same circuit as the voice communications) or "out-of-band" (signals are passed to the subscriber over a separate circuit) (see Paragraph A.9, supra). Some of the signals sent to a subscriber's telephone handset are not intended to be acted upon by the subscriber.[7] Other signals inform the subscriber of events that invite a response, for example, call waiting tone, lights to indicate call waiting, message waiting tone, call forwarding reminder, ringing and busy tone.[8] Equipment that relies on input from a subscriber necessarily knows what information has been sent to a subscriber to which it expects a response.

Advances in digital switching and new technology have given rise to network-generated information that is vital to law enforcement's attempts to conduct effective electronic surveillance. When a subscriber under surveillance attempts to make an outgoing call or receives an incoming call, the network generates signals such as ringing, busy, or call waiting tones. For subject-initiated call attempts, these signals indicate whether the subject ends a call before the network could complete the

---

[7] In wireless communications, a large number of messages are sent to the handset for the purposes of maintaining an ongoing telephone call. The caller is unaware of these messages, which relay administrative or supervisory information such as the technical information necessary to process hand-offs (the transfer of a wireless call from one radio frequency in one cell to another radio frequency in an adjoining cell).

[8] A variety of different features may employ the same in-band or out-of-band signal. Accordingly, the number of signals used is smaller than the number of features that can employ those signals.

call, or when the called-to number is ringing or busy. For incoming calls, these signals indicate whether the subject's telephone was alerted by tones, a visual indicator, or a text message. These signals are important to law enforcement in order to understand how a caller is interacting with the network, and to understand and track the resulting communications.

5. Surveillance Status Message. In the traditional telecommunications environment, law enforcement has physical access to most interception devices and can therefore verify whether a device is accessing the correct equipment, facility or service. Under the more modern switch-based technologies, however, law enforcement will no longer have access to the intercept location and carriers, who do have access to the switch, must perform this vital function. Unlike most traditional electronic surveillance, where law enforcement physically installs equipment to activate the electronic surveillance, the software-based provisioning of a CALEA solution will necessarily be controlled entirely by a carrier.

A Surveillance Status Message will ensure that the *carrier's* equipment (equipment not used in traditional lawfully-authorized electronic surveillance) is ready and it will ensure that the electronic surveillance software has been activated on the correct target of surveillance. In addition, if law enforcement were to receive a Surveillance Status Message, that receipt would confirm that the communications path between law enforcement and the carrier, over which the message was sent, is still operational. If no information is made available to law enforcement regarding the condition of the lawfully-authorized electronic surveillance, law enforcement will simply have no way of knowing the status of that surveillance.

As mentioned previously, law enforcement currently has physical access to most subscriber service lines and interception devices and law enforcement itself activates the electronic surveillance.

This arrangement allows law enforcement to ensure that the surveillance is accurately provisioned in a timely manner. As CALEA solutions are deployed, however, carriers will have to be responsible for ensuring the accuracy and integrity of the electronic surveillance. The surveillance status message to law enforcement is therefore essential.

Other methods of ensuring the status of lawfully-authorized electronic surveillance could be developed for CALEA-compliant electronic surveillance. Nonetheless, automated notification would be efficient and would reduce the risk that electronic surveillance might be activated on the wrong subscriber. Moreover, an automated message would be timely and would enable law enforcement to respond immediately when lawfully-authorized electronic surveillance has either been incorrectly installed or has been mistakenly de-activated by a carrier.

Some wireless networks may not be configured to poll remote switches and ensure that they are operational. Wireless carriers could, however, transmit surveillance status messages directly from the network elements involved in the surveillance. There would therefore be no need for such carriers to institute procedures to achieve centralized polling.

6. Feature Status Message. Carriers that provide telephone service, and particularly those carriers that provide advanced calling features, keep track of subscribers' use of those features. Carriers monitor the features used by an individual subscriber for two distinct purposes. First, a carrier must know the status of a subscriber's features if it is to provide the subscriber with service. For example, if a subscriber with call forwarding alters the number to which an incoming call is to be forwarded, the carrier must be able to fulfil that request on the next subsequent incoming call, even if that incoming call occurs only moments after the change is made. If the carrier failed to keep track of a subscriber's features and activities, it would be unable to provide those features. Second, carriers

bill subscribers for services used. Any feature that is used by a subscriber just once on a per-usage basis (e.g., call ring back) will be noted at the time that the feature is invoked so that the appropriate billing can take place.

Many telecommunications features, such as call forwarding, have an adverse impact on law enforcement's ability to conduct lawfully-authorized electronic surveillance. Some features made available to a subscriber will dictate how law enforcement conducts lawfully-authorized electronic surveillance, so law enforcement must know what features a subscriber has if it is to monitor that subscriber's facilities effectively.

In particular, law enforcement can only obtain communications from facilities under surveillance if it has procured a sufficient number of circuits for the delivery of intercepted information. When a subscriber activates features that permit multi-party calls to be made, for example, law enforcement can collect all of the communications, pursuant to an appropriate court order, only if it provisions multiple circuits (*call content channels*). If calls are to be intercepted from a subscriber's conference bridge, for example, and the subscriber, *A*, is not only participating in the conference but also engaging in additional call activity, law enforcement would need to provision one call content channel to intercept the various communications to which *A* was a party, and another to intercept conversations occurring, without *A*'s participation, over *A*'s conference bridge. If *A* activates the conference calling feature after a lawfully-authorized electronic surveillance has begun, law enforcement will have no way of knowing that the additional circuit is necessary. An automated message from the carrier to law enforcement provides an efficient way for law enforcement to insure that it has provisioned enough call content channels to intercept all of the information that it has legal authority to acquire.

7. Continuity Check Tone. A "continuity check tone" should be considered to be analogous to the provision of dial tone on any subscriber's line. Dial tone is the sound heard by a subscriber when a telephone handset is picked up from its resting place. Carriers provide dial tone on every wireline subscriber's telephone line for two reasons: (1) to tell the subscriber that the switch is ready to accept dialed digits; and (2) to indirectly notify the subscriber that the physical link connecting the subscriber's telephone to the network (the local loop) is in working order. When a subscriber does not hear a dial tone, the subscriber immediately knows of the interruption in service.

A continuity check tone would serve the same purpose for law enforcement. If the physical link connecting law enforcement to the carrier providing the interception falls silent during the course of lawfully-authorized electronic surveillance, what conclusions should law enforcement draw? As a technical matter, the mechanism for providing a continuity check tone should be no different from that already in place to provide every subscriber with dial tone or for maintenance oversight on carriers' trunk lines.

8. Dialed Digit Extraction.

As explained above in Paragraph B.3., digits dialed after an initial connection often represent subject-initiated dialing and signaling information that is necessary to complete a call and reach the intended party. Generally, dialed digits are interpreted by switches with *tone decoders*. Tone decoders are specifically designed to listen for DTMF tones (Dual Tone Multi Frequency tones), the tones that are produced when a caller presses the numeric keys on the handset, or sometimes when special dialing features or keys are invoked.[9] Tone decoders turn these tones into the corresponding number that switching equipment can understand. In other words, when the number 9 is dialed, a

[9] Tone decoders are also known as tone receivers, DTMF receivers or dialed digit receivers.

switch's tone decoder hears the tone (a combination of two tones: 852 Hz and 1477 Hz) and interprets that as a 9. The same goes for all the digits on the key pad. Tone decoders are resources that are typically shared across the entire switch. Tone decoders respond to dialed digits to set up the call, and then are released for use by other subscribers.

One technical solution to dialed digit extraction would be the "loop-around." Instead of extracting digits within the switch, a "loop-around" mechanism would use trunks, and would thus allow carriers to extract post-cut-through dialed digits without redesigning their switches.

Where post-cut-through digits are dialed by an intercept subject to complete a call, the originating carrier only needs to monitor the particular facilities that are under surveillance in order to identify and extract those digits. If an intermediate carrier (e.g., the carrier providing long-distance service), were to be asked to provide the same dialed digits, by contrast, it would have to monitor every call it received to see which calls were placed from facilities subject to surveillance. Similarly, the terminating carrier (the carrier serving the person called) would have to monitor every one of its switches, because a call could be placed from facilities under surveillance to any subscriber whom the carrier served.

The "post-cut-through dialed digits" punch list capability would require the carrier to use a decoder for post-cut-through dialing and to send the interpreted numbers dialed to law enforcement in the form of a data message. The importance of this information to law enforcement cannot be overstated because it identifies the final destination of a telephone call.

9. Timely Delivery Of Call-Identifying Information. Carriers in today's sophisticated telecommunications networks have an overriding need to synchronize events to ensure that connections are made and subscribers are billed for services. The signaling that takes place between network equipment often contains embedded information that allows the equipment to synchronize. Networks use very accurate clocks that generate periodic signals used for synchronization and are used to control the timing of certain network functions.

Switches today operate very fast. See generally Paragraph A.9., supra. They are designed to be able to set up about 360,000 calls an hour, or 100 calls a second. This means that a call can be completed (based on receipt of the final message) every 10 milliseconds.

The J-Standard calls for the content of communications to be delivered to law enforcement over a circuit separate from the circuit that contains the corresponding call-identifying information. Law enforcement therefore needs delivery of the content of communications to be synchronized with the call-identifying information so that it can associate an event in the network (e.g., a party dropped from a conversation on a conference call), with the content of the conversation. One efficient way to provide this capability is to label, or *time stamp*, the information sent to law enforcement over each circuit. The time stamp would allow law enforcement to match information from the call content channel with information from the circuit providing call-identifying information. Moreover, because of the rapidity of network processing, the application of time stamps would not affect switches' ability to perform call setup tasks in a timely manner. Nor would the application of time stamps affect the delivery of call content.

10. Delivery Interface. In order for carriers to deliver call identifying information to law enforcement in a switch-based surveillance environment, the parties must use a common delivery

interface. A delivery interface is a protocol, such as X.25, that prescribes the form in which information will be transmitted and other transmission-related parameters.

The J-Standard does not contain any limitation on the number of delivery interfaces that carriers may use to deliver information to law enforcement. Under the J-Standard, each carrier would be free to employ a different interface. To ensure that it was capable of receiving information from carriers, a law enforcement agency therefore might find itself having to employ a potentially large number of different delivery interfaces. If the carrier used a delivery interface that the law enforcement agency was not equipped to handle, the delivery would fail and law enforcement would lose the information that it was authorized to acquire.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. Executed on January 27, 1999.

John W. Cutright
Electronics Engineer
Federal Bureau of Investigation