DIALTONE Newsletter

January-October 2025

50,000 Phones for AT&T's New Neighbor

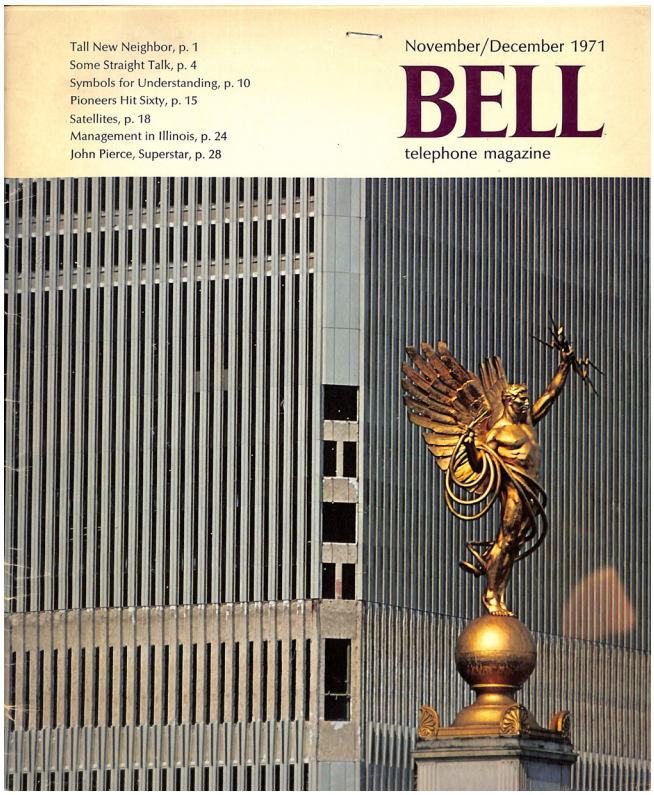
Yes, 50,000 phones for the One World Trade Center, and it's 1971!

Out of our many Telephone Company newsletters and magazines, we chose the November/December 1971 issue of Bell Telephone Magazine to feature, because of the iconic One World Trade Center, and it's construction during that year. This was one mammoth complex, and it was build next door to the former American Telephone & Telegraph Co. (AT&T) headquarters, which itself was constructed in 1912, and opened in 1916.

The interesting details probably most hav never heard about, unless you were in the Bell System, or were part of the construction project at One World Trade Center, are retold in this issue of DIALTONE, with original images from that 1971 Bell Telephone Magazine issue.

We hope you find this interesting, as it's part of American history, past and present, and something worth preserving to continue to tell the story of this iconic building site.

Also, we included in this issue the 'AT&T Response Terrorist Attack September 11, 2001', which details the devastating effects of the destruction of the World Trade Center complex, exactly 30 years after their construction, and how AT&T and their National Disaster Recovery teams worked around the clock to restore destroyed critical communications infrastructure that Western Electric had installed in these buildings. This issue of Dialtone is dedicated, not only to the first responders who risked their lives to do rescue and recovery, but also those who constructed these mammoth buildings, and the Bell System engineers and technicians that installed all that communications infrastructure that handled long distance, local and regional telecommunications.



November/December 1971 Bell Telephone Magazine

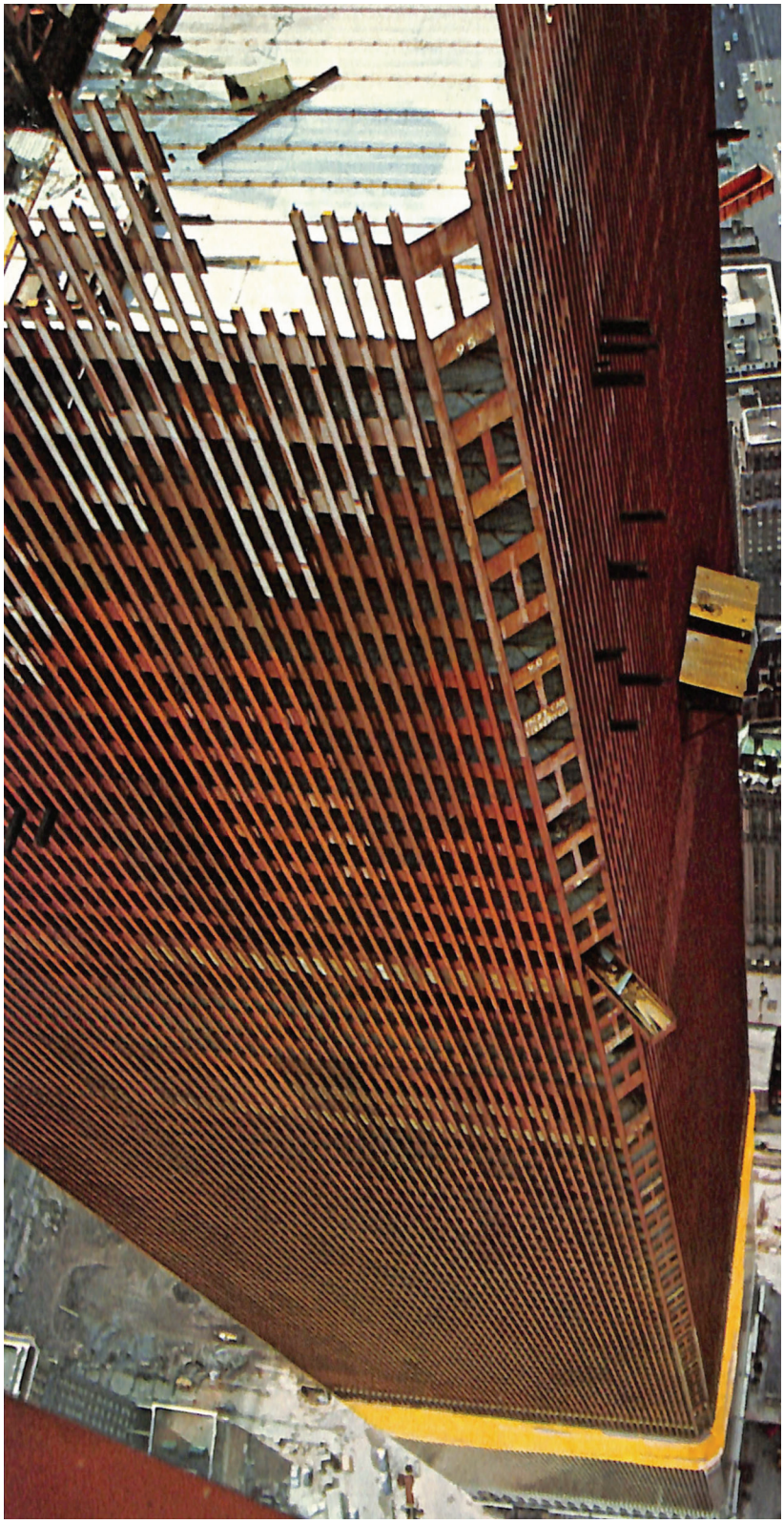
(continued on page 2)

50,000 Phones for AT&T's New Neighbor (Continued from page 1)

World Trade Center Tops Out

A "city" with the phone capacity of Galveston, Tex., or Poughkeepsie, N.Y., is opening for business on a16-acre site in lower Manhattan. Assign designating the address of the North Tower in the building complex reads:
"This Is One World Trade Center. And that it is, whether one considers the address or the magnitude of the project. The South Tower, Two World Trade Center, like its twin, is 110 stories —1,350 feet tall. The complex also will include a U.S. Customs House, Northeast and Southeast Tower Plaza buildings, each nine stories high,

a 17-story hotel and below-ground parking for 2,000 cars. Fifty thousand people will work at the center, which is expected to attract 80,000 business visitors every weekday. Together, the twin towers will have 204 elevators. Each express elevator will be capable of carrying 55 people at a speed of 1,700 feet per minute.
The $575 million World Trade Center will offer nine million square feet of rentable space. When completed, it will have required 200,000 tons of Japanese steel, 600,000 square feet of tempered, heat-reflective glass and 5,000 construction workers on the site at one time. It will take a 49,000-ton system of air conditioning to cool the place.



(Continued on page 3)

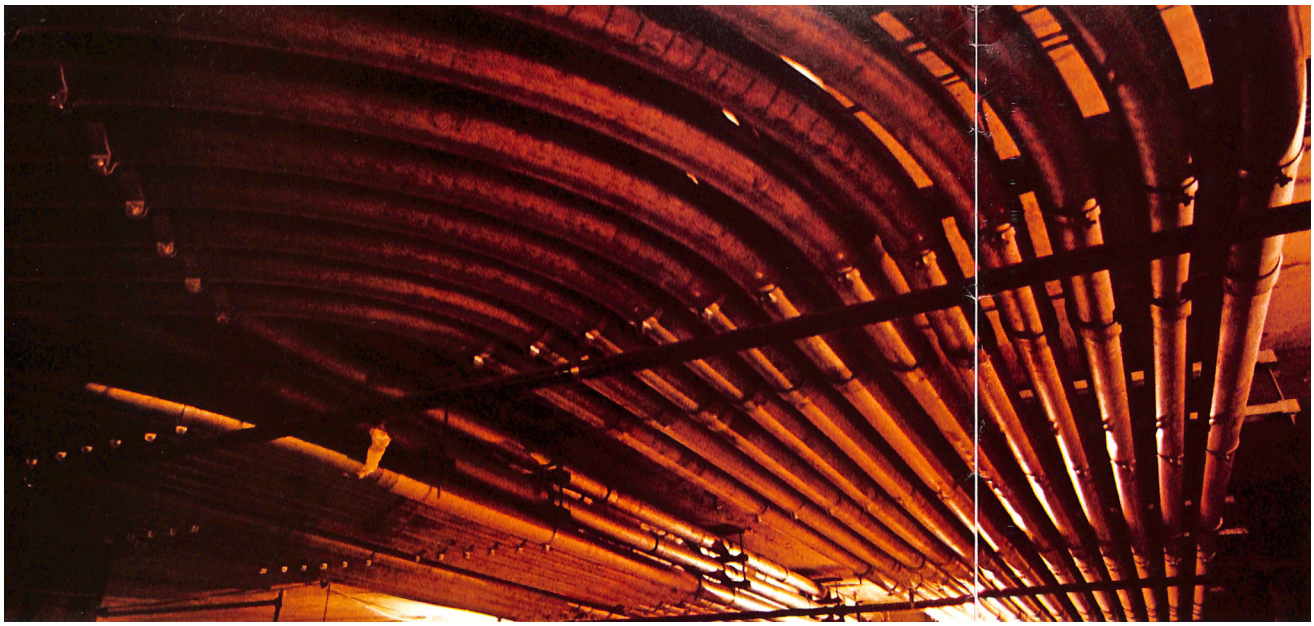
January-October 2025

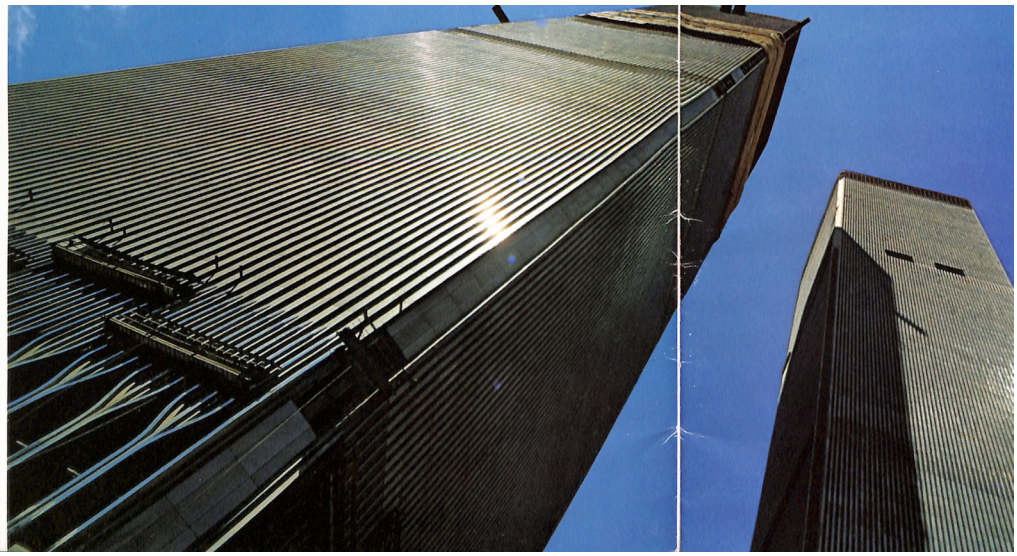
Editor
DW Hoopes

DIALTONE Newsletter

DIALTONE the magazine issued periodically by Bell System Archives, PO Box 1770, Surprise, AZ 85378-1780, (212) 393-8255. Send all editorial contributions to the attention of the editor.

50,000 Phones for AT&T's New Neighbor (Continued from page 2)





Lower left, view of 195 Boradway, AT&T Headqueaters with 'Spirit of Communication' statue

(Continued on page 4)

50,000 Phones for AT&T's New Neighbor (Continued from page 3)

The center will have 50,000 telephones and will consume 600 megawatt hours of electrical power daily. New York Telephone and Western Electric, among 167 sub-contractors working on the project, have a total of more than 100 people installing telecommunications equipment and coordinating plans with the general contractor, Tishman Realty and Construction Corp., and the center's owner, the Port of New York Authority. When completed, the complex will require more than 200 full-time New York Telephone employees to serve it. Six Electronic Switching System (ESS) offices will be installed in the South Tower. They will serve the complex as well as future downtown growth. New York Telephone will occupy five floors in the South Tower — more than 150,000 square feet —for central office and administrative space. The company will invest more than $65 million in telecommunications equipment to provide service at the center. Some 200,000 miles of telephone conductors are piped into the complex —enough to reach eight times around the world.

The center is scheduled for completion in late 1973. More than 100 customers now occupy lower floors of the North Tower, which was topped out las t December. Tenants and visitors alike will be afforded views of New York City's harbor, Staten Island and the Verrazano-Narrows Bridge to the South; the Hudson River immediately below; New Jersey to the West; Brooklyn and Queens across the East River on Long Island, and all of Manhattan Island, including that renowned second tallest building in the world — the Empire State.

Some time in the future the Empire State Building will drop to third in height and the World Trade Center to second with completion of Chicago's Sears-Roebuck Building.

Areal view of One World Trade Center under construction - 1971

Installing the Phone System of the World Trade Center - AT&T Archives

https://www.youtube.com/watch?v=_iXW_j1KD2k

A short film about the building of the World Trade Center AND the telephony challenges the construction posed. The Bell System had installed a #1ESS Western Electric central office switching system within the towers. There are plenty of shots of the Towers being built, and then filled by companies, back in the 1970s.

After 9/11, it was reported that one of the few things to survive the WTC attacks was AT&T's switching system, which was good because many people relied on the mainframe for their telephone connectivity. AT&T's local network switching equipment that routes telephone calls was located in a deep sub-basement of the Towers and somehow survived the collapse of the buildings. None of AT&T's employees were hurt in the attacks.

Footage courtesy of AT&T Archives and History Center, Warren, NJ

AT&T Response Terrorist Attack September 11, 2001

Summary of Key AT&T Responses

- Pro-active management of the network to handle increased call volumes, prevent network equipment from going into overload, and manage around congestion situations.
- Placement of the on site work force on the highest alert status in the affected areas to expedite restoration activities
- Placement of all AT&T network locations on heightened security status.
- Activated Telecommunications System Priority (TSP) process to assure critical government services are restored with the highest priority.
- Cooperation with and support of FEMA and local authorities to establish emergency communications in the affected areas, and with financial institutions to facilitate resumption of stock exchange operations in NYC.
- Support of communications for police and other emergency personnel.

AT&T Network Disaster Recovery WTC NYPD Headquarters Support

NDR deployed an Emergency Communications Vehicle (ECV) to provide emergency phone service for the New York City Police Department's command center near the World Trade Center disaster site. The ECV provided 44 voice lines for NYPD's use and dedicated four lines for use by the families of missing members of the NYPD and FDNY.

(Continued on page 6)

AT&T Response Terrorist Attack September 11, 2001

(Continued from page 5)

Summary of Key AT&T Responses

- Global Network Operations Center and Emergency Operations Center coordination of recovery activities for all network functionality

- Constant interaction with Verizon and other carriers at all levels to provide assistance and assure coordinated recovery –from executive to working level

- Deployment of the network disaster recovery team

Disaster Recovery Site World Trade Center Disaster

(Continued on page 7)

AT&T Response Terrorist Attack September 11, 2001

(Continued from page 6)

Disaster Recovery Site World Trade Center Disaster

TARGET: Accept traffic in 72 hours

"RESULT"
Traffic-ready capabilities in 48 hours

(Continued on page 8)

AT&T Response Terrorist Attack September 11, 2001

(Continued from page 7)

Disaster Recovery Site World Trade Center Disaster

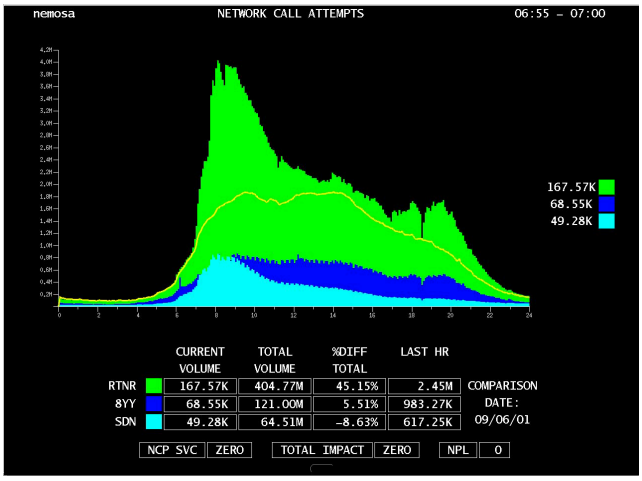
AT&T Network Disaster Recovery WTC "Ground Zero" Relief Support

On Friday, September 21, the Manhattan ECV was moved to a location within the WTC disaster zone to provide emergency communications for New York City emergency response agencies and for humanitarian relief purposes. The phone bank was set up in the Spirit of New York, a dinner cruise ship, that is being used as a rehabilitation center for the crews working on the WTC disaster site.

(Continued on page 9)

AT&T Response Terrorist Attack September 11, 2001

Impact - September 11th Terrorist Attack



AT&T Network
- AT&T average nationwide call volume is 300M calls per day
- Previous daily record call volume was 330M calls
- 9/11/01 nationwide voice call volume reached 431M calls

United States Pentagon
- No Service was lost
- The situation was monitored continuously
- Simulations were conducted to develop an effective recovery plan for immediate implementation should the need arise

New York City/ World Trade Center
- Unprecedented
- Local Network Services' (LNS) two largest Transport Nodes in WTC were destroyed … Six others in Manhattan were OK
- Lost use of two switches due to building damage and two others due to loss of power … Seven others in Manhattan were OK
- Major issue is connectivity to AT&T Core and LNS nodes, Verizon network nodes, and Customers

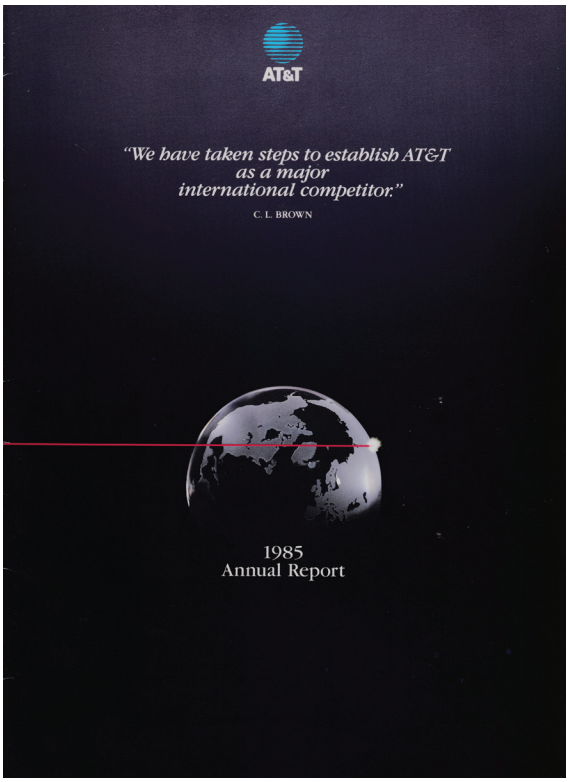
Recovery - September 11th Terrorist Attack

Switching Recovery
- Recovered two local switches on Day 4 Upgraded one ORM to full switch on Day 6
- Recovered third local switch on Day 18
- Re-homing affected customers to other switches

Transport Recovery
- Built new Transport Node, including new Digital Cross Connect Systems by Day 18
- Using Broadband Wireless wherever possible … 24 installations thru Day 24
- Rebuilding entire Lower Manhattan fiber and transport ring network

Presentation to NRIC V – PJ Aduskevicz; October 30, 2001

After nearly 20 Years, Our AT&T Investor Annual Reports is Almost Complete!



1985, The Elusive Annual Report

After hunting and searching all over the Internet, and collectors forums, Bell System Archives finally has that one annual report that was virtually impossible to locate. It was far easier to locate early 1900's or 1920's annual reports than it was the post divestiture AT&T 1985 Annual Report, be we now have it, and is now uploaded to our website.

The 1985 AT&T Corp. Annual Report sheds more on the inner workings of the once dominant AT&T, which is a shadow of its former Bell System parts prior to January 1, 1984. This report is replete with details of the technological advancements, and foray into computers.

The irony of actually finding this 1985 annual report on eBay, exactly 40 years since the financial information was compiled which made this report even more interesting

Go to **Historical Phone Company Financials** https://memorial.bellsystem.com/att/historical_financial.htm to view this report under 1985

Lexmark Cartridge Collection Program (LCCP)

LCCP
Lexmark Cartridge Collection Program
xerox™
Lexmark™

As a reseller for Lexmark printers, Network Services offers our customers the free service of helping collect their Lexmark, and now Xerox toner cartridges, and waste toner cartridges for shipment back to the manufacturer for recycling.

The free and easy way to return your Lexmark toner cartridges for reuse and recycling.

When you return your empty supplies through LCCP, you are helping to reduce impact on the environment and promote sustainability. Each year, millions of pounds of materials are responsibly reused and recycled, and it starts with you. You can do your part by following the steps below to recycle toner cartridges.

From Wikipedia:

Lexmark was formed on March 27, 1991, when investment firm Clayton & Dubilier completed a leveraged buyout of IBM Information Products Corporation, the printer, typewriter, and keyboard operations of IBM. Lexmark became a publicly traded company on the New York Stock Exchange on November 15, 1995 (under NYSE:LXK).

On December 23, 2024, Lexmark announced that Xerox would be buying the company from Ninestar and PAG Asia, with the deal expected to close in the second half of 2025. The acquisition was completed on July 2, 2025. Xerox's COO, John Bruno, stated that Xerox would continue using the Lexmark name for an "undetermined amount of time" but ultimately plans to discontinue it, merging Lexmark product lines with Xerox's own

Contact Network Services to setup collection schedule.

Advanced Information Systems

Tech Tips

HERE WeGo

Most of us use a GPS navigation app on our smartphones, and it's usually Apple Maps or Google Maps, but have you ever tried the, 'Here WeGo' web mapping and satellite navigation software that is available on your computer, or app store?

Nokia originally released this as 'Nokia Maps' in 2007, and is currently owned by Audi, BMW and Mercedes-Benz.

This mapping system is far more accurate than any of the other platforms, and our labs have tested this for it's efficacy. We even found that, one of our medical office clients had Google Maps take their patients, and first responders to an apartment complex to the rear of the building, which has no access to the medical facility. Apple Maps did the same thing! Now, when we tested Here WeGo, it was flawless, and took people exactly where to go. The interface is clean, and is available globally, including North America.

You can download this on the Google Play (Android), and Apple Store (iOS).

Web: https://wego.here.com

iOS: https://apps.apple.com/us/app/here-we-go-maps-navigation/id955837609

Android: https://play.google.com/store/apps/details?id=com.here.app.maps&hl=en-US&pli=1

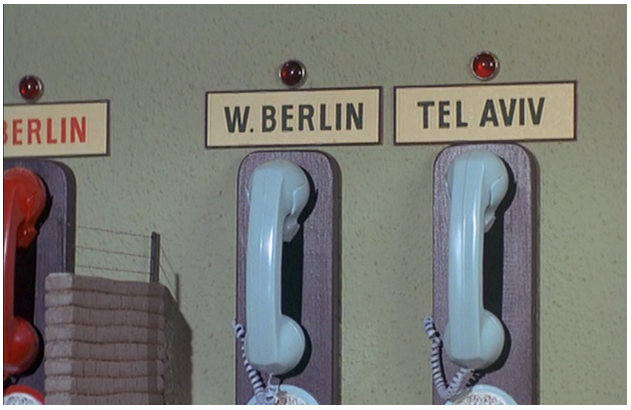
Oops!

At Dialtone, we will feature some odd incidents that we find on TV shows relating to phones.

Chief of Control (Edward Platt) answering one of the "secret" phones in his office. Notice all friendly nations are -65 AQUA BLUE; -114 BRIGHT RED for Communist nations, and -59 ROSE PINK for Paris! Peking is somehow slanted, though this could be anyones guess. Wall phones are possibly Automatic Electric (AE).

Oops! (Continued)

Get Smart (TV Series); The Man from YENTA (1967)
Time Index: 08:44



Notice to left, the miniture Berlin Wall that separates the W. Berlin and E. Berlin phones.

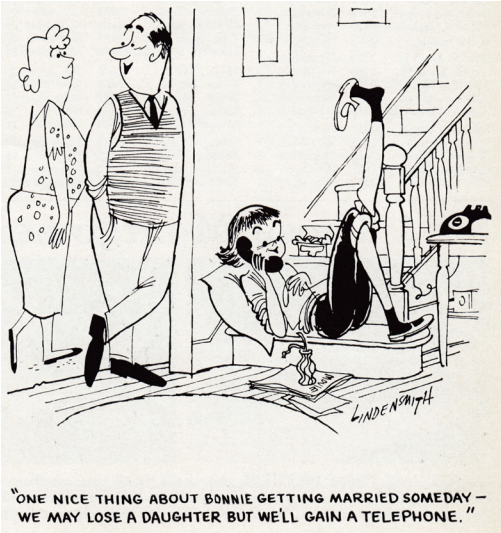
Images courtesy of CBS Productions, CBS Media Ventures and HBO Home Video

Unbelievable

At Dialtone, this section we will feature communication inside and outside plant that has clearly either been neglected, destroyed purposely by vagrants, or sloppy technicians who clearly could care less about quality installations.

CenturyLink Cabinet in Sun City West, AZ; Camino Del Sol & R.H. Johnson Rd. This cabinet, for many years had an issue, where the doors would not close properly, and was a result of the dirt and gravel builup that prevented closure. This was on the side of the Chase Bank, and no one from CenturyLink bothered to correct this issue, so our company took the inititive to clear the gravel and dirt that built up over 40 years, and now the doors close properly, and the outside elements no longer affect the internal wiring

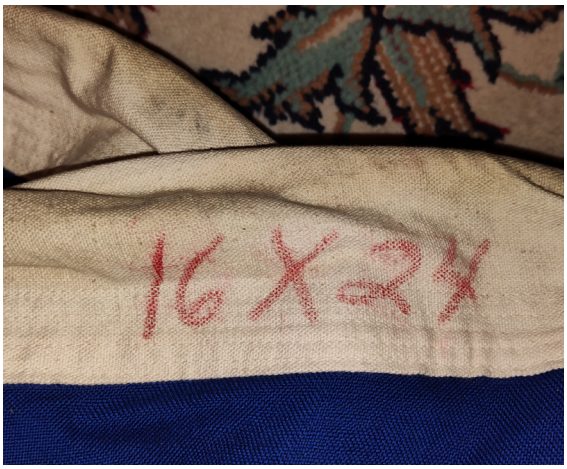
Cartoon



(Reprint from Western Electric The Montgomery Monitor Magazine - 1958)

New to Archives

The massive 16 x 24 ft (4.9 x 7.3 m) 1948 Bell System flag was donated to our Bell Archives, and is in beautiful condion, and resides in our temperature controlled archive facility.



Bell System logo used between 1939-1964, as seen on this flag, minus the lettering in outer rim

(Continued on page 14)

New to Archives **(Continued from page 13)**

This 1969-1983 Bell System flag is 12 x 18 ft (3.7 x 5.5 m), and replaced the previous version throughout the Bell System.

All flags are well taken care of, and we carefully displayed these as best we could just to take archival images, and then stored them back in boxes. Folding these are a multiple person job!

Bell System logo used between 1969-1983

(Continued on page 15)

New to Archives (Continued from page 14)

A thank you to Edward B. (Ted) Kaye, Vexillum Editor, The North American Vexillological Association (NAVA) for the donation of the two flags, which are important pieces of telephone history. As with all donations, we greatly appreciate them. Ted had worked with the Phone Company, and had been given these flags when he worked at 140 New Montgomery, and they were no longer needed. Below are post Bell System business cards that Ted shared with us, and we wanted to share who Ted was when he worked for the Phone Company.

Ted is currently Secretary of the North American Vexillological Association (NAVA) https://nava.org/

PACIFIC TEL
Services

Edward B. Kaye
Staff Manager

Diversified Businesses Group Staff
140 New Montgomery St., Room 703
San Francisco, California 94105
415-542-1417

PACIFIC BELL
A Pacific Telesis Company

Edward B. Kaye
Director - Financial Management
Operations - North

2600 Camino Ramon, Room 2N301
San Ramon, California 94583
415-867-6480

PACIFIC TELESIS
Group

Edward B. Kaye
Staff Director
Executive Services

Pacific Telesis Center
130 Kearny Street, Suite 2800
San Francisco, California 94108
415-394-3772
Fax: 415-391-8065

The two respective flags in our Bell Archives had flown atop this iconic building. This was the headquarters of The Pacific Telephone & Telegraph Company, the part of the Bell System that served customers in California and Nevada.

Pacific Telephone

Logo used between 1970-1983

PACIFIC TELESIS PACIFIC BELL

Logo used between 1983-1997

The holding company for Pacific Bell, Nevada Bell, Pacific Telesis International, PacTel Mobile Services and PacTel InfoSystems was Pacific Telesis. Pacific Telesis was created in 1983 for the impending breakup of AT&T Corporation on 1 January, 1984, and Pacific Telesis was one of a total of seven Regional Bell Operating Companies, "RBOCs" or "Baby Bells" that divested from AT&T Corp.

- **Ameritech (30 S. Wacker Dr., Chicago, IL)**
- **Bell Atlantic (1600 Market St, Philadelphia, PA)**
- **BellSouth (1155 Peachtree Street, NE, Atlanta, GA)**
- **NYNEX (335 Madison Ave, New York, NY)**
- **Pacific Telesis (140 New Montgomery St, San Francisco, CA)**
- **Southwestern Bell [SBC] (909 Chestnut St., St Louis, MO)**
- **US West, Inc. (1801 California St., Denver, CO)**

140 New Montgomery Street, San Francisco, California, The Pacific Telephone & Telegraph Company Building, known as the "Telephone Building", and also The Pacific Bell Building (Pacific Telesis Group (PacTel) The PacBell Building after 1984. When 140 New Montgomery opened in 1925, at 435 feet high, it was the tallest skyscraper in San Francisco. see https://140nm.com/

(Continued on page 16)

1963 postcard showing flagpole atop Pacific Telephone HQ

Circa 1920-1929 postcard showing Bell System flag atop Pacific Telephone HQ

Circa 1925-1935 Pacific Telephone HQ

Future issues of Dialtone, 'New to Archives' will retroactively go back in our collections and pay respect to those that have donated items, and also those items we have acquired over the years. We have, on occasion mentioned items we have acquired, or were donated, on our 'What's New' section on the Bell System Memorial website, but feel that having this special section on this publication affords a more special feature that is retro.

So, those of you that have donated items to us, stay tuned, because we will showcase these, and add any special notations of where such items originated from to chronicle history

Security Tips

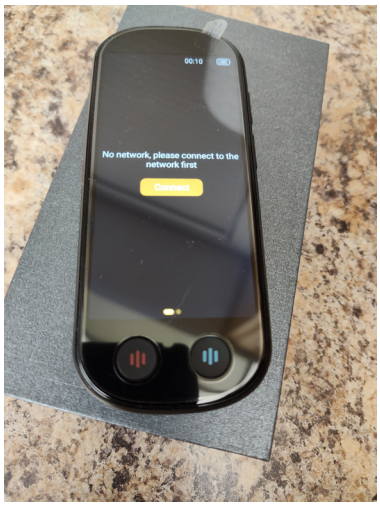
The art of Artificial Intelligence has broadly expanded to include handy little devices that will translate just about any language on the planet. However, this comes at a price...privacy and data security! The old school adage you have nothing to hide should really no longer be used as a saying, especially when it comes to security of your conversations.

The selection of AI Language Translators are specific ones that we tested at our labs. Though this is not an exhaustive review, and there are many other professional ones to read up on, we were able to gain some rather unusual security insights into two totally independent, and yes, unbranded AI Language Translator devices. These all seem to come unbranded, and 100% of these are made in Peoples Republic of (Communist) China (PRC).

Both of these devices claim you need no WiFi at all, and that they just magically translate once you charge up. The earbud version, which will translate 164 languages requires you install an app on your phone, and then will sync in real time. This may not require WiFi, but will require some sort of Internet, which is your phone. The handheld device has all this built in, and though it also claims no WiFi needed, you still need to connect to something. The screen says; "No network, please connect to the network first". We did just that, but on a segregated WiFi network. On our secure, and purposely region specific IP blocking we have, noticed that Baidu 百度, which is a massive PRC technology company, was gaining access to this device, as it is the core of the system. At first Baidu tried to sneak past our security, but thankfully it was blocked, with Access Denied.

The AI Translation Earbuds fared even worse, as the security we have through our cell phones would not even allow the app to function, as this device was also connection to PRC data servers.

Language Translator device, claimed no WiFi needed (notice loswer left image clearly shows network connection needed. 150+ languages instant two way Translator Device: $84.98



AI Translation Earbuds Real Time, 164 Languages & Accents Device: $34.99

The bottom line, after our testing, and the higher security in our network, we found issues most normally would not even be aware of, and this should be very worrying. Better off using Google Translate, and be very cautious about any mobile app, or device that is associated with Communist China, especially Baidu, which is secretly embedded in many mobile apps that many are not even aware of.

(Continued on page 18)

FBI Denver Warns of Online File Converter Scam

Released
March 7, 2025

The FBI Denver Field Office is warning that agents are increasingly seeing a scam involving free online document converter tools, and we want to encourage victims to report instances of this scam.

In this scenario, criminals use free online document converter tools to load malware onto victims' computers, leading to incidents such as ransomware.

"The best way to thwart these fraudsters is to educate people so they don't fall victim to these fraudsters in the first place," said FBI Denver Special Agent in Charge Mark Michalek. "If you or someone you know has been affected by this scheme, we encourage you to make a report and take actions to protect your assets. Every day, we are working to hold these scammers accountable and provide victims with the resources they need."

To conduct this scheme, cyber criminals across the globe are using any type of free document converter or downloader tool. This might be a website claiming to convert one type of file to another, such as a .doc file to a .pdf file. It might also claim to combine files, such as joining multiple .jpg files into one .pdf file. The suspect program might claim to be an MP3 or MP4 downloading tool.

These converters and downloading tools will do the task advertised, but the resulting file can contain hidden malware giving criminals access to the victim's computer. The tools can also scrape the submitted files for:

Personal identifying information, such as social security numbers, dates of birth, phone numbers, etc.)
Banking information
Cryptocurrency information (seed phrases, wallet addresses, etc.)
Email addresses
Passwords
Unfortunately, many victims don't realize they have been infected by malware until it's too late, and their computer is infected with ransomware or their identity has been stolen.

The FBI Denver Field Office encourages victims or attempted victims of this type of scheme to report it to the FBI Internet Crime Complaint Center at www.ic3.gov.

In addition, the FBI Denver Field Office recommends taking the following actions to protect yourself from this scam:

Take a breath, slow down and think. Be aware of your actions online and what risks you could be exposed to.
Keep your virus scan software up to date and scan any file you receive before opening it to help eliminate malicious software from being installed on your computer.
If you are a victim of this scam, here are some steps to take:

Contact your financial institutions immediately. Take steps to protect your identity and your accounts.
Change all your passwords using a clean, trusted device.
Make a report at IC3.gov
Run up-to-date virus scan software to check for potentially malicious software installed by the scammers. Consider taking your computer to a professional company specializing in virus and malware removal services.

Source: https://www.fbi.gov/contact-us/field-offices/denver/news/fbi-denver-warns-of-online-file-converter-scam

(Continued on page 19)

Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

Last Revised: September 03, 2025 Alert Code: AA25-239A

Executive summary

People's Republic of China (PRC) state-sponsored cyber threat actors are targeting networks globally, including, but not limited to, telecommunications, government, transportation, lodging, and military infrastructure networks. While these actors focus on large backbone routers of major telecommunications providers, as well as provider edge (PE) and customer edge (CE) routers, they also leverage compromised devices and trusted connections to pivot into other networks. These actors often modify routers to maintain persistent, long-term access to networks.

This activity partially overlaps with cyber threat actor reporting by the cybersecurity industry—commonly referred to as Salt Typhoon, OPERATOR PANDA, RedMike, UNC5807, and GhostEmperor, among others. The authoring agencies are not adopting a particular commercial naming convention and hereafter refer to those responsible for the cyber threat activity more generically as "Advanced Persistent Threat (APT) actors" throughout this advisory. This cluster of cyber threat activity has been observed in the United States, Australia, Canada, New Zealand, the United Kingdom, and other areas globally.

This Cybersecurity Advisory (CSA) includes observations from various government and industry investigations where the APT actors targeted internal enterprise environments, as well as systems and networks that deliver services directly to customers. This CSA details the tactics, techniques, and procedures (TTPs) leveraged by these APT actors to facilitate detection and threat hunting, and provides mitigation guidance to reduce the risk from these APT actors and their TTPs.

This CSA is being released by the following authoring and co-sealing agencies:

- United States National Security Agency (NSA)
- United States Cybersecurity and Infrastructure Security Agency (CISA)
- United States Federal Bureau of Investigation (FBI)
- United States Department of Defense Cyber Crime Center (DC3)
- Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
- Canadian Centre for Cyber Security (Cyber Centre)
- Canadian Security Intelligence Service (CSIS)
- New Zealand National Cyber Security Centre (NCSC-NZ)
- United Kingdom National Cyber Security Centre (NCSC-UK)
- Czech Republic National Cyber and Information Security Agency (NÚKIB) - Národní úřad pro kybernetickou a informační bezpečnost
- Finnish Security and Intelligence Service (SUPO) - Suojelupoliisi
- Germany Federal Intelligence Service (BND) - Bundesnachrichtendienst
- Germany Federal Office for the Protection of the Constitution (BfV) - Bundesamt für Verfassungsschutz
- Germany Federal Office for Information Security (BSI) - Bundesamt für Sicherheit in der Informationstechnik
- Italian External Intelligence and Security Agency (AISE) - Agenzia Informazioni e Sicurezza Esterna
- Italian Internal Intelligence and Security Agency (AISI) - Agenzia Informazioni e Sicurezza Interna
- Japan National Cybersecurity Office (NCO) - 国家サイバー統括室
- Japan National Police Agency (NPA) - 警察庁

(Continued on page 20)

Security Tips **(Continued from page 19)**

- •Netherlands Defence Intelligence and Security Service (MIVD) - Militaire Inlichtingen- en Veiligheidsdienst
- •Netherlands General Intelligence and Security Service (AIVD) - Algemene Inlichtingen- en Veiligheidsdienst
- •Polish Military Counterintelligence Service (SKW) - Służba Kontrwywiadu Wojskowego
- •Polish Foreign Intelligence Agency (AW) - Agencja Wywiadu
- •Spain National Intelligence Centre (CNI) - Centro Nacional de Inteligencia

The authoring agencies strongly urge network defenders to hunt for malicious activity and to apply the mitigations in this CSA to reduce the threat of Chinese state-sponsored and other malicious cyber activity.

Any mitigation or eviction measures listed within are subject to change as new information becomes available and ongoing coordinated operations dictate. Network defenders should ensure any actions taken in response to the CSA are compliant with local laws and regulations within the jurisdictions within which they operate.

Background

The APT actors have been performing malicious operations globally since at least 2021. These operations have been linked to multiple China-based entities, including at least Sichuan Juxinhe Network Technology Co. Ltd. (四川聚信和网络科技有限公司) Beijing Huanyu Tianqiong Information Technology Co., Ltd. (北京寰宇天穹信息技术有限公司) and Sichuan Zhixin Ruijie Network Technology Co., Ltd. (四川智信锐捷网络科技有限公司). These companies provide cyber-related products and services to China's intelligence services, including multiple units in the People's Liberation Army and Ministry of State Security. The data stolen through this activity against foreign telecommunications and Internet service providers (ISPs), as well as intrusions in the lodging and transportation sectors, ultimately can provide Chinese intelligence services with the capability to identify and track their targets' communications and movements around the world.

For more information on PRC state-sponsored malicious cyber activity, see CISA's People's Republic of China Cyber Threat Overview and Advisories webpage. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239

Baidu apps found to be 'leaking' personal data
https://www.bbc.com/news/technology-35669817

Baidu Maps could have leaked details of millions of users
https://www.techradar.com/news/baidu-maps-could-have-leaked-details-of-millions-of-users

Google Delists Chinese Baidu Apps for Stealing Users' Data
https://cisomag.com/chinese-baidu-apps/

Backdoor in Baidu Android SDK Puts 100 Million Devices at Risk
https://thehackernews.com/2015/11/android-malware-backdoor.html?m=1m=1

How your solar rooftop became a national security issue
https://techcrunch.com/2025/08/15/how-your-solar-rooftop-became-a-national-security-issue/

There are still some things Americans know how to do best.

1. One of them is building our phone system. The calls Americans make will double by 1985. So the people at Western Electric and Bell Labs have developed a new switching system to handle more than 350,000 long-distance calls an hour.

2. The first of these electronic systems will go into service in early 1976. Western Electric installer Bob Doss and phone company technician Kathy Czap help put it through the equivalent of 20 years testing in months.

3. The "brain" of this switching system connects 100 calls a second, while it tests itself and reports on its own performance.

4. Tiny electronic memories control the correct path for every call out of billions of possible connections.

Making a phone call may be a small thing to you.

But to us it's a big job.

It takes a delicately balanced network of more than a trillion parts for you to reach the one phone you want out of 140 million.

Working with Bell Labs and your phone company, we at Western Electric help make sure that all the parts work together with just one goal in mind:

Making your phone system the best system in the world.

Western Electric

We're part of the Bell System.
We make things that bring people closer.

Western Electric Magazine ad on ingenuity and craftsmanship of Bell System Technology - 1976)

RBOC Services & Pension Benefits Contacts

AT&T

- Business Services (Internet, Phone): 800-222-0400
- Consumer Services (Internet, Phone): 800-222-0300
- Mobility Services: 800-331-0500
- Enterprise Infrastructure Solutions: 844-EIS-ATT1
- Public Sector Solutions: 888-740-4158
- Benefits Center: 877-722-0020
- Fidelity Pension & 401 (k) Service Center: 800-416-2363
- Service outage info: https://www.att.com/outages/

Bell

- Small Business (Internet, Phone): 800-668-6878
- Residential Services (Bell TV, Internet, Phone): 866 394-6331
- Mobility Services 866 709-6079
- Medium/Large Business: 855-312-5329
- Bell Pensioners' Group (BPG): P.O. Box 41132 Elmvale P.O. Ottawa, ON K1G 5K9
- Service outage info: https://support.bell.ca/Outage-Check

LUMEN / CenturyLink

- Business Services (Internet, Phone): 800-526-3178
- Consumer Services (Internet, Phone): 800-837-4966
- Mobility Services: 800-922-0204
- Enterprise Center: 800-569-8799
- Federal Solutions: 844-825-8389
- Retiree Benefits Connection: 855-489-2367
- Service outage info: https://www.verizon.com/support/check-network-status/

verizon

- Business Services (Internet, Phone): 800-603-6000
- Consumer Services (Internet, Phone): 800-244-1111
- Enterprise Infrastructure Solutions: 800-871-9244
- Public Sector: 888-597-2455
- Pension Center: 888-324-0689
- Service outage info: https://www.centurylink.com/home/help/internet/internet-or-phone-not-working.html

Western Electric / AT&T Network Systems / Lucent Technologies / AVAYA / agere systems

- AVAYA Pension Benefits: benefits@avaya.com

- AT&T Network Systems/Lucent Technologies/Agere Systems Benefits (NOKIA): 888-232-4111

Here's one way to reach more personnel, faster, with more effective military training programs.

Tele-Lecture.

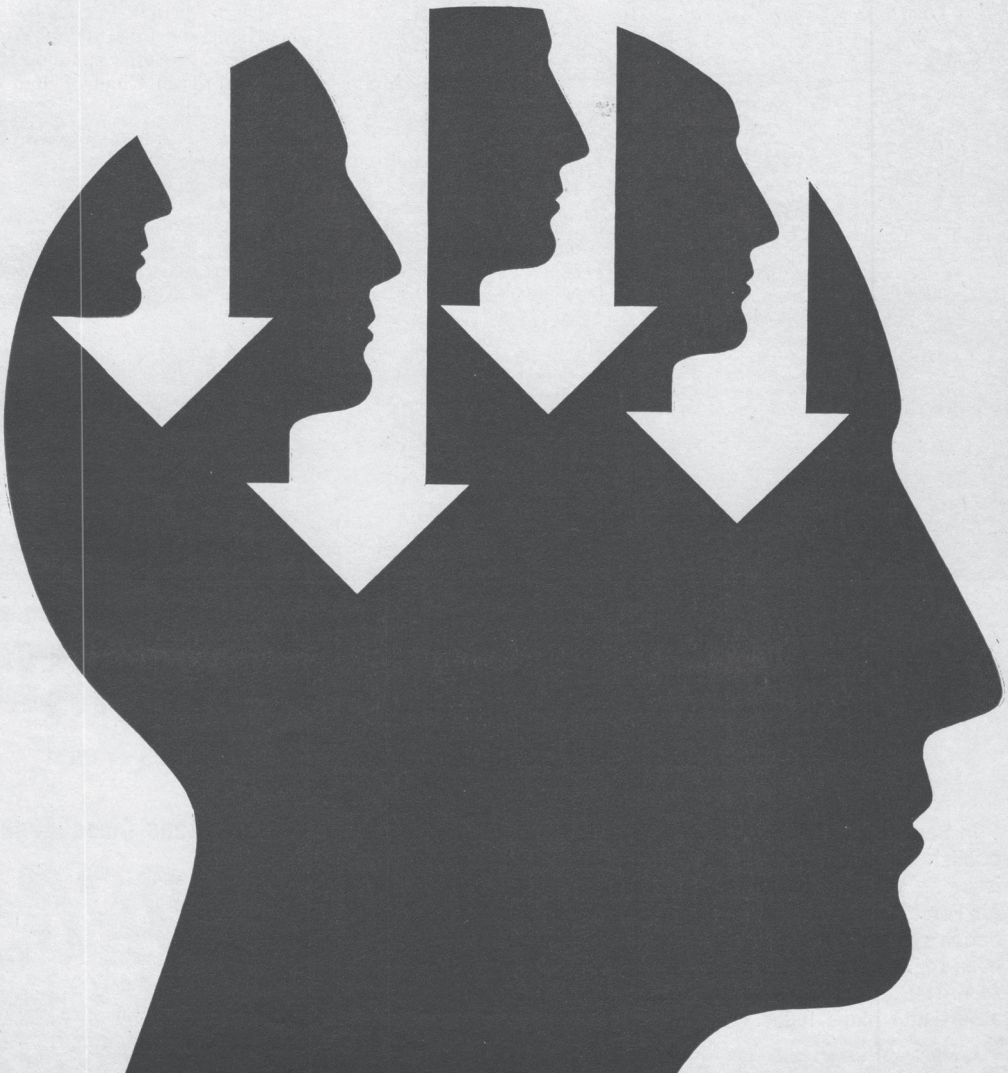
Using Tele-Lecture the presentations of your best instructors penetrate instantly into any number of scattered classrooms. Lectures and discussions are delivered by phone...and received over amplified speakers. Because it's two-way, students ask questions and get answers on the spot.

If lectures need illustration, add a visual dimension using Telewriting service to supplement Tele-Lecture presentations. With Telewriting, handwritten notes, charts and maps travel by phone and are projected on a large screen for easy group reading.

Use the network that's already there to add flexibility and long-range control to your training programs. For more information about these and other educational services, call your local Bell System Communications Consultant.

BELL SYSTEM AT&T and Associated Companies

Penetrate



Bell System Magazine Ad on Tele-Lecture, precursor to modern teleconferencing - 1968)

NETWORK SERVICES

Who We Are

Principal Products & Services

Advanced Information Systems

- UNIX® (TrueNAS and Apple OSX, Apple iOS)
- Linux (Ubuntu, Debian) Programming
- ThinkCentre, ThinkStation®, ThinkPad®, and ThinkVision®
- Lexmark printers (high yield laser printers)
- Comsphere PBX VoIP service
- Business cybersecurity implementation
- Webhosting services

Premises Distribution Systems (PDS)

- SYSTIMAX® SCS network cabling (copper and fiber wiring and accessories)
- CommScope® coax and security cabling
- Enhanced broadband support with Local Exchange Carrier (LEC) or known as the "Phone Company" *

Advanced Mobile Phone Service

- Motorola® ThinkPhone® with enhanced proprietary DNS and mobile app protection to mitigate intrusion and eavesdropping
- Proprietary Bellboy secure internal messaging application, dedicated to your business

Bell System Directory Services

- Search Directory Optimization (SDO), consolidates and enforces a unified online directory presence for the multitude of digital directory systems, and aggregators