2600 February, 1984

Published monthly by 2600 ENTERPRISES, an eleemosynary organization. Subscription rates are $10 annually. Write to 2600, Box 752, Middle Island, NY 11953.

*0#D

VOLUME ONE, NUMBER TWO

HACKING ON TELENET
It's as easy as 123456!

Telenet. Or, to be more specific, GTE Telenet. A massive network formed by the people and technology that were used to develop packet switching for the Department of Defense. Telenet was purchased by GTE in 1979 and has been growing in size and revenue ever since.

There are quite a few data networks in existence today. Datapac, Autonet, Tymnet, Arpanet, to name some of the better known. A data network is basically a collection of mainframes, specialized minis, and high-speed lines. Through Telenet, you can connect to literally thousands of computers, all over the country, even the world if you know the proper procedures. All this is possible by making a local phone call, in most parts of the country. [Telenet access numbers are made readily available to the public by Telenet and systems on the network, such as the Source, Compuserve, etc.]

Once your modem is connected to Telenet, you have to hit two carriage returns. You'll see:

TELENET
XXX XXX

where the first 3 X's are the area code you're connected to and the rest comprise the Telenet node identifier. You'll then be asked for your terminal identifier. Usually "D1" works for most terminals, but a simple carriage return is also accepted.

At this point you first receive the @ prompt. It is from here that you get places. And that's what's so unique about Telenet—the *way* in which you get places. You simply type a "C", a space, and the Telenet address. Then you enter the *area code* of the computer you want to connect to, followed by a two or three digit code. That's all there is to it. Telenet tells you whether or not you've found a working computer. If you want to exit from one computer and connect to another, just type an "@". You'll then get the Telenet @ prompt. Before you type the next address, type "D" to disconnect from the computer you're still connected to.

Hackers across the country have for years programmed their computers to scan the system for interesting things. All that has to be done is this: Pick the city you want to scan—let's say Boston. The area code is 617. Have your computer start its search at address 617001. If you get connected to a computer, Telenet will skip a line and print 617 001 CONNECTED. If you don't get connected, there are a variety of messages you could get. 617 001 REJECTING, 617 001 NOT RESPONDING, 617 001 NOT REACHABLE, 617 001 REFUSED COLLECT CONNECTION are a few of them. They all mean basically the same thing—there is no way to hook up to this address.

At this point, several things can be done. Naturally, you'll want to increment the address by one and search for a computer at address 617002. But how do you have your computer recognize when a connection has been made? This is necessary because you can't just keep entering C XXXXXX over and over—once you get connected, you have to enter the "@" to get back to the Telenet prompt, followed by a "D". Of course, you could type C XXXXXX, followed by "@", followed by "D" for *every* attempt, but that can get rather time consuming. It's better simply to be able to save to disk or output to a printer the addresses of connections. And, fortunately for hackers, Telenet makes that very easy.

You can either search for a string that has the word "CONNECT" in it somewhere—the only time you'd find one would be when you got the CONNECTED message. But, as we mentioned earlier, an extra line is skipped right before the CONNECTED message, for some reason. Why not simply look for that extra line? If you get it, record the address, send the "@" and "D" and increment by 1. If you don't get the extra line, simply increment by 1.

Naturally, you will be collecting Telenet addresses for informational purposes only, to find out which computers are located where, in case you ever have to get onto one in an emergency of some sort. Keep in mind that you are not *entering* any of these computers; you're merely connecting for a brief second or two. And there is no login procedure or identity check for Telenet, so you're not fraudulently using their system either.

Also, the area code system is not the only system that works on Telenet. These are simply set up to be convenient, but an address can actually have any kind of a number in it. For example, addresses beginning with 311 or 909 (the latter being Telenet's own private "area code") also abound, and there are certain to be many more.

Without a doubt, though, it's the existence of the area code system that has helped Telenet become one of the easiest data networks to hack. And until they install some sort of a user identification program, or at least have the system disconnect after it becomes obvious that there's a strange person online, hackers will continue to be one of Telenet's biggest problems.

If you have information to share with us about this or any other data network, please send it in. Requests for anonymity will be respected.

ESS: ORWELL'S PROPHECY

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

From *Nineteen Eighty-Four*

ESS is the big brother of the Bell family. Its very name strikes fear and apprehension into the hearts of most phreakers, and for a very good reason. ESS (Electronic Switching System) knows the full story on every telephone hooked into it. While it may be paranoid to say that *all* phreaking will come to a screeching halt under ESS, it's certainly realistic to admit that any phreak whose central office turns to ESS will have to be a lot more careful. Here's why.

With electronic switching, *every single digit* dialed is recorded. This is useful not only for nailing phreaks but for settling billing disputes. In the past, there has been no easy way for the phone company to show you what numbers you dialed locally. If you protested long enough and loud enough, they might have put a pen register on your line to record everything and prove it to you. Under ESS, the actual printout (which will be dug out of a vault somewhere if needed) shows *every last digit* dialed. Every 800 call, every call to directory assistance, repair service, the operator, every rendition of the 1812 Overture, everything! Here is an example of a typical printout, which shows time of connect, length of connect, and number called.

DATE	TIME	LENGTH	UNITS	NUMBER
0603	1518	3	1	456-7890
0603	1525	5	3	345-6789
0603	1602	1	0	0000-411
0603	1603	1	0	800-555-1212
0603	1603	10	2.35*	212-345-6789
0603	1624	1	0	0000-000 (TSPS)

A thousand calls to "800" will show up as just that—a thousand calls to "800"! *Every* touch tone or pulse is kept track of and for most phreaks, this in itself won't be very pretty.

Somewhere in the hallowed halls of 195 Broadway, a Traffic Engineer did an exhaustive study of all 800 calls over the past few years, and reached the following conclusions: (1) Legitimate calls to 800 numbers last an average of 3 minutes or less. Of the illegal (i.e. phreakers) calls made via 800 lines, more than 80 percent lasted 5 minutes or longer; (2) The average residential telephone subscriber makes five such calls to an 800 number per month. Whenever phreakers were being watched, that number was significantly higher. As a result of this study, one feature of ESS is a daily log called the "800 Exceptional Calling Report."

Under ESS, one simply does not place a 2600 hertz tone on the line, unless of course, they want a telco security representative *and* a policeman at their door within an hour! The new generics of ESS (the #5) now in production, with an operating prototype in Geneva, Illinois, allow the system to silently detect all "foreign" tones not available on the customer's phone. You have exactly twelve buttons on your touch-tone® phone. ESS knows what they are, and you had best not sound any other tones on the line, since the new #5 is programmed to silently notify a human being in the central office, while continuing with your call as though nothing were wrong! Someone will just punch a few keys on their terminal, and the whole sordid story will be right in front of them, and printed out for action by the security representatives as needed.

Tracing of calls for whatever reason (abusive calls, fraud calls, etc.) is done by merely asking the computer right from a terminal in the security department. With ESS, everything is right up front, nothing hidden or concealed in electromechanical frames, etc. It's merely a software program! And a program designed for ease in operation by the phone company. Call tracing has become very sophisticated and *immediate*. There's no more running in the frames and looking for long periods of time. ROM chips in computers work fast, and that is what ESS is all about.

Phone phreaks are not the only reason for ESS, but it was one very important one. The first and foremost reason for ESS is to provide the phone company with better control on billing and equipment records, faster handling of calls (i.e. less equipment tied up in the office at any one time), and to help agencies such as the FBI keep better account of who was calling who from where, etc. When the FBI finds out that someone whose calls they want to trace is on an ESS exchange, they are thrilled because it's so much easier for them then.

The United States won't be 100 percent ESS until sometime in the mid 1990's. But in real practice, all phone offices in almost every city are getting some of the most basic modifications brought about by ESS. "911" service is an ESS function. So is ANI (Automatic Number Identification) on long distance calls. "Dial tone first" pay phones are also an ESS function. None of these things were available prior to ESS. The amount of pure fraud calling via bogus credit card, third number billing, etc. on Bell's lines led to the decision to rapidly install the ANI, for example, even if the rest of the ESS was several years away in some cases.

Depending on how you choose to look at the whole concept of ESS, it can be either one of the most advantageous innovations of all time or one of the scariest. The system is good for consumers in that it can take a lot of activity and do lots of things that older systems could never do. Features such as direct dialing overseas, call forwarding (both of which open up new worlds of phreaking which we'll explore in later issues), and call holding are steps forward, without question. But at the same time, what do all of the nasty implications mentioned further back mean to the average person on the sidewalk? The system is perfectly capable of monitoring *anyone*, not just phone phreaks! What would happen if the nice friendly government we have now somehow got overthrown and a mean nasty one took its place? With ESS, they wouldn't have to do too much work, just come up with some new software. Imagine a phone system that could tell the authorities how many calls you placed to certain *types* of people, i.e. blacks, communists, laundromat service employees... ESS could do it, if so programmed.

This was the first in an occasional series on the fun and dangers of ESS.

Times Changing For Directory Assistance

Combined News Sources

Directory Assistance promises to have a very different future, both in the U.S. and in France. Here in the States, customers are being threatened with a 75¢ charge for long distance information requests. In a few parts of the country, Indiana (812) for instance, a request for a phone number produces startling results: a human will answer and ask for the city and name, and after finding it will hit a button, whereupon a machine takes over and spits out the number with a digitized voice. You are then given the option to hold on to be reconnected to another D.A. operator.

This kind of system makes multiple requests quite inconvenient—forcing one to either wait to be reconnected to a human, or dial over and over again. This latest step towards *total* mechanization also strikes fear into the hearts of the D.A. operators, many of whom do not wish to lose their fun jobs.

France, meanwhile, has a nationalized phone system run by the Ministry of Posts and Telecommunications, an agency which has been experimentally offering computerized telephone information (Teletel) to 70,000 users. The Ministry provides, for free, a small terminal called a Minitel which has a keyboard that folds up over the screen.

To find a number, a user enters the name, address, region of France, and profession of the person they're looking for. If just the name and city are entered, all of the people with that name in that city will be displayed. The system does not yet list all of France, but should by June. The Ministry expects to have 3 million terminals in use within two years. In addition to Teletel, 15 other services will be provided, including news, stock quotations, shopping catalogs, banking systems, as well as railroad, airline, and movie schedules.

Perhaps this will give AT&T some ideas. Imagine being able to call a distance city and get phone numbers for everybody named Smith! Electronic phone book hacking could be a considerable amount of fun.

No Hacking While Flying, Please

Combined News Sources

Eastern Airlines now specifically prohibits the use of portable computers on all flights, because of adverse effects the airline claims may occur. The new baggage policy excludes calculators from this ban.

The feeling at Eastern is that portable computers can interfere with radar and "distort equipment," causing all kinds of strange things to happen. When a company spokesperson for the Miami based carrier was asked if any specific incident triggered the new policy, she responded that an incident "probably happened" but that nothing more could be said.

A possible boycott of the airline has been proposed by Wayne Green, publisher of the magazine *Microcomputers*.

Trick of the Month

2600 News Service

Many supermarkets in states having passed a "bottle bill" of sorts are installing can-return machines. You put an empty aluminum soda can in the machine, UPC code up, and the machine crunches it and gives you money. Well, some hackers have discovered that these machines work for *all* beverage cans, deposit or not. In some states, for example, non-carbonated beverages (iced tea) don't carry a deposit even though the cans are exactly the same as the ones containing carbonated drinks. A human will not take those cans back, but the machines will, gladly.

By the way, we haven't heard from anyone who's tried putting a *full* soda can in one of these machines. It would be interesting to find out if the machine tries to crush it. More interesting to see if it succeeds.

Death Star Cards Spell Woe

2600 News Service

Many of the long-awaited AT&T credit cards are now being distributed. You will be impressed when you get yours—complete with a picture of the AT&T death star floating over planet Earth, while the new AT&T red, blue, and black stripe looks on.

But with these cards come a few problems. For one thing, many customers of New York Telephone received their PIN cards only days before they got their AT&T cards. What is a PIN card? Well, PIN stands for Personal Identification Number, but other than that, it's really the exact same thing as an AT&T card, except that it doesn't have a magnetic stripe. It also only has four numbers on it—the last part of your 14-digit code (your phone number comprises the first part). New York Telephone proudly claims that this secures your code, since if you lose your card, whoever finds it won't know your phone number nor be able to find out because your name isn't even on it. So along comes AT&T sending out *their* cards to everyone who got a PIN card. AT&T cards have your name *and* your 14-digit code prominently displayed (yes, the last four digits are the same as New York Telephone's). Result: the PIN cards are completely useless, both because they're redundant and because their purpose has been defeated.

AT&T has made a serious mistake with these cards. First of all, since so many of them are in the mail at the same time, many will be stolen, perhaps within the post office itself. Second, there are *no* security precautions whatsoever at those new credit card phones. You simply plug in the card and dial away. No identity codes to enter, like the bank cards require. With 5,000 of these phones (which also accept American Express cards) scheduled to be installed this year, credit card fraud for AT&T will almost certainly rise, not so much due to phone phreaks, but rather, simple common thieves.

An official at AT&T said that they were not overly concerned. "We're counting on people's honesty," they said. We'll see what they say next year.

ADS Investigation Moved?

Word of Mouth

It's been rumoured that the FBI investigation of IBM Audio Distribution System hackers has now been headquartered in another city (i.e. *not* Detroit). Last month, *2600* published a rather extensive report on the investigation, including the name of the city and the informant who started this whole mess, John Maxfield of JFM Industries in Detroit.

Several threats have allegedly been made by Maxfield to a group of hackers who helped expose him. This is reportedly being done against the wishes of the FBI. *2600* is currently investigating the authenticity of these threats and, if they check out, you can count on seeing a transcript next month.

SOME THOUGHTS ON "GARBAGE PICKING"

Garbage picking is the art of finding things that someone else has thrown away. Hackers on time-sharing systems are long familiar with the technique of asking the operating system for some memory or mass storage space that has not yet been zeroed out, and then dumping out whatever was in there to the screen or printer. Things like password files and system programs are always updated or backed up from time to time, and that's when a "garbage copy" will be created. The alert hacker will find this if he or she looks hard enough.

You can even do some garbage picking with your own microcomputer! Occasionally, when a software house creates a disk, it copies over an entire disk, not just the programs that they happen to be selling on that disk. You might find old copies of the vendor's programs sitting in there, or all kinds of other stuff.

For those of you without computers, there are other ways you can join in on the fun. Many a tale has been told on the local bulletin boards about the enterprising phone phreaks who snuck around to their local phone company's central office early one morning and snooped through the dumpsters. In the old mechanical switching areas, you might find wires, relays, and other bits and pieces that an electronics hobbyist would enjoy. In areas served by electronic switching, computer printouts are more likely, and you might even find the garbage hoppers locked to prevent pholks like you from snooping around. Remember, other people's garbage is sometimes considered their private property. **Be sure to check with your local authorities on the legalities of digging into large corporations' back yards before you find out what the rules are the hard way.** One person who almost got into trouble over this was a New York City sculptor who was poking through the trash cans around Richard Nixon's townhouse and got picked up by the SS (Secret Service). He told the judge that he was planning to make a sculpture of the former president out of garbage, and he wanted to use the real stuff. The judge, obviously, a man of refined artistical tastes, allowed the sculptor to poke through the garbage without molestation.

Other kinds of garbage picking require some more technical knowledge and a bit of construction ability. One possibility that could keep you project builders busy is a cross-talk amplifier. For those of you who aren't familiar with the term, cross-talk (on your telephone) is when you hear another conversation (usually very faintly) underneath a phone conversation that you're having. If you build an amplifier that can filter out the background noise and amplify only the narrow bandwidth where the voice is transmitted through the phone lines, you might be able to make out what the folks are saying, for all the good it will do you. But there are other things you can hear in this electronic garbage heap. Suppose one day you hear cross-talk of a modem conversation? If you could amplify it and feed it into your computer, you would be able to monitor someone else's entire computer session. Suppose you hear someone entering in touch-tone® codes to some local call extender? All you have to do is build yourself a tone decoder (you can find schematics for these things in any Radio Shack) and figure out what the person entered. Obviously, once you are able to amplify the cross-talk to a reasonable level, your best bet is to tape-record the material so that you can experiment with the best way to feed it into the computer or tone decoder that will be further deciphering it.

There have been tales told of one enterprising phreak who built a tone decoder and then called up his favorite call extender. He then called some "dead" line (such as the silent half of a loop line somewhere; other possibilities could be a disconnected number [you hear silence after the recording finishes] or even your own phone, if you have a second line you can use) and turned on his tape recorder. It wasn't too long before he heard the cross-talk of someone else using the extender, and he picked up ten new codes inside of a week! Of course, he needed a working code to sign onto the thing in the first place, but there are some extenders where you can "hold the line open" by hitting some key every now and then. The nice thing about this kind of hacking is that you only need to make one phone call to find things out, while standard hacking requires a separate phone call for each attempt at a new code. No system in existence could detect a fellow with a tape recorder and a tone decoder listening in, although it's certainly possible that someday, someone could design their phone circuits to be 100% free of cross-talk.

That's all we have for now on the subject of garbage picking. If you come up with any more places where an inquisitive person might find some interesting information lying around, be sure to write in and let us know. Please include your method of "digging up" the garbage, and suggestions to all those other people out there who will try to duplicate your results.

Q&A

Got a question for us? Write it down and send it to us! We'll do our best to come up with an answer. Send it along to:

2600
Box 752
Middle Island, NY 11953

Q. How does the operator find out if you are calling from a fone booth or a house fone? Is there any way to defeat this?
—California

A. A pay phone is wired up directly to the TSPS (Traffic Service Position System, basically the operator at a switchboard) circuit. A light on the console flashes and shows the caller to be at a pay phone. To convince the TSPS that it wasn't actually a pay phone, you would have to go into the switch room and rewire it. The distinction is not made within the phone itself, but in the central office. You receive a dial tone through the TSPS circuit before it goes to the central office—it's connected in series with it. Everything you do goes through the TSPS circuit, whether it's local or not. In short, there's no way around it.

2600 needs writers! This could be your big chance!! If you come up with something to contribute, send it in to the address at the end of Q & A. Please send us your comments and criticisms as well. And spread the word! 2600 *is bringing the good word of hackers and phreakers throughout the land of disks and relays!*

AFGHANISTAN - 93
ALBANIA - 355
ALGERIA - 21 - 3, 4, OR 5 *
ANDORRA - 33 - AP 078
ANGOLA - 244
ARGENTINA - 54 - 1, 21, 41, OR 51
AUSTRALIA - 61 - D1-3
AUSTRIA - 43 - D4
BAHRAIN - 973
BANGLADESH - 880
BELGIUM - 32 - D1-2
BELIZE - 501
BENIN - 229
BHUTAN - * - 1400 PHONES
BOLIVIA - 591
BOTSWANA - 267
BRAZIL - 55 - D2 (X1)
BRUNEI - 673
BULGARIA - 359
BURMA - 95
BURUNDI - 257
CAMEROON - 237
CAPE VERDE - 238
CENT. AFRICAN REPUBLIC - 236
CHAD - 235
CHILE - 56 - D1-2
CHINA (MAINLAND) - *
COLOMBIA - 57 - D3 OR D5
COMORO IS. - 269
CONGO - 242
COSTA RICA - 506
CUBA - *
CYPRUS - 357 - D2 (X1)
CZECHOSLOVAKIA - 42
DENMARK - 45 - CODES 1-9, FAROES IS 42
DJIBOUTI - 253
DOMINICA - *
ECUADOR - 593 - D2 OR D4
EGYPT - 20
EL SALVADOR - 503 - D2 OR D4
EQU. GUINEA - 240
ETHIOPIA - 251
FALKLAND IS. - *
FIJI - 679
FINLAND - 358 - CODE 0 OR D2
FRANCE - 33 - CODE 1 OR D2
FRENCH GUIANA - 594
FR. POLYNESIA - 689
GABON - 241
GAMBIA - 220
GERMAN DEM. REPUBLIC - 37 - D1-5
FEDERAL REP. OF GERMANY - 49 - D2-4
GHANA - 233
GIBRALTAR - 350
GILBERT IS. - 686
GREECE - 30 - CODE 1 OR D2-3
GRENADA - *
MACAO - 853
MADAGASCAR - 261
MALAWI - 265
MALAYSIA - 60 - CODES 3 OR 5
MALDIVES - *
MALI - 223
MALTA - 356
MARIANA IS. - *
MARTINIQUE - 596
MAURITANIA - 222
MAURITIUS - 230
MEXICO - 52
MONACO - 33
MONGOLIA - 976
MOROCCO - 21 - CODES 0, 1, OR 2 *
MOZAMBIQUE - 258
NAURU - 674
NEPAL - 977
NETHERLANDS - 31 - D2 OR D4
NETH. ANTILLES - 599 - D1
NEW CALEDONIA - 687
NEW HEBRIDES - 678
NEW ZEALAND - 64 - D2-5
NICARAGUA - 505 - D1-2
NIGER - 227
NIGERIA - 234 - D2-3 (0XX)
NORWAY - 47 - D1-2
OMAN - 968
PAKISTAN - 92
PANAMA - 507
PAPUA NEW GUINEA - 675
PARAGUAY - 595
PERU - 51 - D2-4
PHILIPPINES - 63 - D1-4
POLAND - 48
PORTUGAL - 351 - D2
QATAR - 974
REUNION - 262
ROMANIA - 40
RWANDA - 250
ST. HELENA - *
AMER. SAMOA - 684
SAN MARINO - 39 - AP 541
SAO TOME (PRINCIPE) - 239
SAUDI ARABIA - 966 - D1-2
SENEGAL - 221
SEYCHELLES - 248
SIERRA LEONE -232
SINGAPORE - 65
SOLOMON IS. - 677
SOMALIA - 252
SOUTH AFRICA - 27 - D2 (X1)
S. W. AFRICA - 264
SPAIN - 34 - D1-2
SRI LANKA - 94
SUDAN - 249
SURINAME - 597

GUADELOUPE - 590
GUAM - 671
GUATEMALA - 502 - CODES 2 OR 61
GUINEA - 224
GUINEA-BISSAU - 245
GUYANA - 592
HAITI - 509
HONDURAS - 504
HONG KONG - 852 - CODES 3, 5, OR 12
HUNGARY - 36 - D1-2
ICELAND - 354
INDIA - 91 - CODES 11 OR 22
INDONESIA - 62
IRAN - 98 - D2-4 (XXX1)
IRAQ - 964 - D1-2
IRELAND - 353 - D1-2
ISRAEL - 972 - D1-2
ITALY - 39 - D2-3
IVORY COAST - 225

JAPAN - 81 - D1-2
JORDAN - 962

KAMPUCHEA - 855
KENYA - 254 - AP 2
N. KOREA - *
S. KOREA -82 - D2
KUWAIT - 965

LAOS - 856
LEBANON - 961
LESOTHO - 266
LIBERIA - 231
LIBYA - 21 - CODES 8 OR 9 *
LIECHTENSTEIN - 41 - AP 75
LUXEMBOURG - 352

SWAZILAND - 268
SWEDEN - 46 - D1-3
SWITZERLAND - 41 - CODE 1 OR D2
SYRIA - 963

TAIWAN - 86 - D1-2
TANZANIA - 255
THAILAND - 66 - AP 2
TIMOR - 672
TOGO - 228
TONGA - *
TRINIDAD - *
TUNIS - 21 - CODE 2 OR 6 *
TURKEY - 90 - D2 (X1)
TURKS & CAICOS - *
TUVALU - *

UGANDA - 256
UAE - 971/978/979
UK - 44 - D1-3 - 25 MILLION PHONES
USA/CANADA/CARIBBEAN - 1 - D3 (XOX OR X1X)
- 190 MILLION PHONES
UPPER VOLTA - 226
URUGUAY - 598
USSR - 7 - 20 MILLION PHONES

VATICAN CITY - 39 - AP 6
VENEZUELA - 58 - D1-2
VIETNAM - 84

WEST. SOMOA - *

YEMEN - 967
YEMEN PDR - 969
YUGOSLAVIA - 38 - D2 (X1)

ZAIRE - 243
ZAMBIA - 260
ZIMBABWE - 263

DEFINITIONS:

DX - X REPRESENTS THE NUMBER OF DIGITS IN A COUNTRY'S CITY CODES. CAN BE OF A RANGE 'DX-Y' BETWEEN X AND Y DIGITS.

(X1) TYPICAL ROUTING CODE. X CAN BE ANY DIGIT. 1 IS ARBITRARY.

AP - ALL POINTS. USE THIS IN FRONT OF ANY LOCAL NUMBER.

CODE REPRESENTS AN INDIVIDUAL CITY CODE. USE ANY OF THE CODES LISTED, OR IF ANOTHER RANGE IS SPECIFIED, ALSO FOLLOW THAT FORMAT.

* USE INTERNATIONAL OPERATOR EITHER FOR ALL CALLS TO THAT COUNTRY IF NO CODE IS LISTED, OR FOR CALLS TO PARTICULAR AREAS DENOTED BY THE '*'.

NOTE: USA COUNTRY CODE '1' COVERS ALL OF THE CONTINENTAL USA, ALL OF CANADA, ALASKA AND HAWAII, AND PORTIONS OF NORTHERN MEXICO. IN ADDITION, THE USA AREA CODE 809 COVERS PUERTO RICO, THE US AND BRITISH VIRGIN ISLANDS, AND VARIOUS OTHER CARIBBEAN ISLANDS. THE 709 AREA CODE IS ROUTED THRU CANADA TO COVER FRENCH POSSESSIONS IN THE HEMISPHERE, NOTABLY THE ISLANDS OF ST PIERRE AND MIQUELON.