

Exploding The Phone

www.explodingthephone.com Bibliographic Cover Sheet db343

Title Are telephones addictive?

Publication New Scientist magazine

Date 1973-12-13

Author(s) Campbell, Duncan

V/I/P Vol. 60, No. 876, p. 756

Abstract Overview of phone phreaking in both Britain and the U.S.

- Keywords blue box; subscriber toll dialing (STD); British phreaking; Duncan Campbell; fiddles; Harvard Five; British Post Office (BPO)
- Notes Article has 4 pages, our copy also has a copy of the cover page.

Source Alan Rubinstein

The following pages may contain copyrighted material. We believe that our use of this material for non-commercial educational and research purposes constitutes "fair use" under Section 107 of U.S. Copyright Law. If you wish to use this material for purposes that go beyond "fair use," you must obtain permission from the copyright owner, if any. While it will make us slightly sad to do so, we will nonetheless comply with requests from copyright owners who want their material removed from our web site.

Nine "phone phreaks" were acquitted last month after a seven-week trial at the Old Balley. The trial gave considerable publicity to the techniques used by a small and determined group of intellectuals with a compulsive desire to know the telephone system inside out.

Duncan Campbell ' is a recent Oxford physics graduate who was aquitted at the trial

When Post Office investigators raided a Hammersmith, London, flat in October 1972. they found a "phone phreaks" conference in progress with large quantities of telephone equipment, a computer printout listing supposedly secret Post Office codes, and devices for making calls. A Post Office installed monitoring device showed that one man had spent much of the day experimenting with one of London's international exchanges,

Nineteen men went on trial on 3 October at the Old Bailey. With advance promises of nominal fines, 10 pleaded guilty-one to actually making calls, the others to conspiracy, Fines ranged from £25 to £100. The other nine stood trial for conspiracy to defraud the telephone system. On 13 November, all were acquitted, in a trial estimated to cost more than £100 000.

Most were men in their 20s holding university degrees, primarily from Oxford, Cambridge, and London. Their interest had begun in student days, usually from reading standard texts such as Atkinson's Telephony and moving on to the Post Office Electrical Engineers Journal. Experiments by exhaustive dialling on local networks followed, Soon they exhausted the possibilities of dialling and



Typical phone phreaking equipment, Rear right-an older style AC 9 simulator (Bleeper) with a telephone dial. Front-a newer push-button AC 9 simulator, with an acoustic coupler (an ordinary telephone carpiece). Rear left-a multifrequency simulator. A print-out of telephone codes lies under the equipment.

moved on to electronic aids. Their attitude was neatly summarised by the trial judger Neil McKinnon, QC, when he commented "Some take to heroin, some take to teles phones." He, too, entered the spirit of the thing and asked for the codes used in his own local exchange in south London

Like scientists conducting experiments, the phone phreaks report results to one another And they take a perverse delight in writing to the Post Office to explain new and previously undetected ways to beat the telephone system-often the Post Office does not believe these suggestions until much later The penetration of the Post Office's secrets has been massive. The investigation that led to the recent trial was apparently triggered by the discovery that for some years the Cambridge University Titan computer had held complete and laboriously compiled files detailing the entire trunk and local network system,

Imitate control signals

In general, telephone enthusiasts (as the court genteelly put it) work by imitating the control signals that the telephone system must have. The signals tell an exchange, for example, that a call is coming from another exchange, or that a subscriber has hung up. or that a call has been answered and that charging should begin. On long distance trunk circuits the signals are within the normal telephone speech bandwidth (30 Hz-3 kHz), and the UK Post Office uses pulses of a single frequency-2.28 kHz. As the signalling must take place on the line which will be used for an actual call, there is no way that the Post Office can prevent anyone from imitating the codes. Usually they use a "bleeper" which puts the tone onto the line with an acoustic coupler, similar to that used for portable come puter terminals. Details of using a bleeper to make international calls are given in the box

In the last few years, the Post Office has begun the introduction of the Trunk Transit Network to effect speedier transfer of information. Where the normal system uses pulses of 2.28 kHz to represent numbers (1 pulse for 1, 2 for 2, etc, just like a telephone dial). the new Multifrequency System (MF2) has six different tones, and uses two at a time, permitting 15 possible combinations (10 num bers and 5 control signals). Thus, where the 0 required 10 pulses, it now only requires 1 The Post Office hopes to introduce full nation wide STD using this technique by 1980. This goal was achieved in the USA and many European countries some years ago. General ing the six tones required in the UK is more complex than the traditional 2.28 kHz, and involves a sixfrequency generator. Because many countries have their own sets of tones the international phone phreak will need a

set of bleepers. One presented in evidence at the trial was very elaborate, being capable of simulating seven different signalling systems. Nicknamed the Mighty Wurlitzer, it was runnoured to cost £200 to build. The Post Office offered £20 for it

As new MF2 centres are added to the network-Newcastle, Hull, and Bradford last month-the Post Office is reportedly intensely worried about the vulnerability of MF2. It is perhaps typical that the Post Office were initially complacent, and did not believe the Cambridge undergrad who some years ago told them that MF2 could be beaten.

One defendant revealed that he and others had written a set of letters to the Post Office explaining flaws in the system. His most recent conribution-a dialling sequence known as 9-1-11 which would give irregular free STD service from small country exchanges -- was haughtily rejected by a Post Office expert with "it couldn't theoretically work".

Dial direct

There is a second major way for the telephone enthusiasts to get onto the PO trunk network. As described here previously (vol 58, p 23), some engineers had covertly installed their own unauthorised links. As these individuals had ample opportunity to

Bleeping around the world

At the trial, the Post Office gave a demonstration of how international calls might he made, using a bleener. The telephone enthusiast first dials an STD call to a destination which will be charged at local rate-from London to Badger's Mount just north of Sevenoaks will do. This call is routed automatically through the London STD centre and the trunk exchange in Sevenoaks. When the call (which is made to a number known to be spare) has gone through, he sends the "clear forward" signal, which tells Badger's Mount that the call is finished, Because the enthusiast's telephone is still off the hook, the London equipment believes the call to be still in progress. The result is an open line going as far as the Sevenoaks trunk exchange.

He then sends to Sevenoaks a signal known as "seize" which wakes up the Sevenoaks end. He could then send the digit "1" which will put him on the outgoing trunk lines from Sevenoaks. By dialling the secret trunk codes or routings, he can then dial freely about the trunk network. He could dial to Tunbridge Wells (code 15) and through it to Cardiff (65) and London International (112), At this point, by using other tones he could if he wished experiment in any part of the world.

Unlike STD codes, the trunk codes are not the same throughout the country-to get from Reading to Tunbridge the code would be 35 rather than 15. Thus, the enthusiasts have built up massive files of trunk codes. often produced on computer printouts.

Knowing the codes, however, does little good because they cannot simply be dialled-extra equipment is required. The clicks that an ordinary telephone dial sends down the line are really DC pulses, 67 millisec (ms) long, sent at the rate of 10 per second. Long distance trunk circuits cannot bandle DC, so the exchange automatically converts these to equally long pulses of 2 28 kHz. This signalling system is known as AC9. Having already passed the local exchange, the phone phreak must produce his own 2.28 kHz signals. Some people are actually able to whistle the correct tone, but most phone phreaks use some sort of electronic simulator-usually called a bleeper-made up of a tone generator and a telephone dial or a more complex push button system.

The device must also produce at least one other signal-the Clear For-

another signal which starts the equinment in London charging for the call, Thus, the user of a bleeper is then paying for the call whether or not he ever completes it. But the charge is always for a call to the first exchange dialled (London always thinks the call is to Badger's Mount) so the bleeper user always starts with a call to a local exchange to keep the cost down. The legal question enters at this point-the effect of the recent acquital would appear to be that using a bleeper is not illegal unless a call is actually completed, in which case the phone phreak is getting a long distance call at local rates. Simple possession of bleepers them-

selves is apparently not illegal

although the Post Office has the right

to disconnect the phone of anyone

ward which is 700 ms of 2.28 kHz,

One of the effects of the clear for-

ward signal is to accidentally generate

The seize signal is simply a "1".

who uses one, London STD Sevenooks unbrida Cardifi London centre frunk X nink Londor Badger local Mount zoname Trunk line exchange manana Local líne London local rate calling area

discover the secrets of the telephone network.

the only purpose of such circuits could be

fraud, as was shown in the recent prosecution

of a Bristol engineer who operated an Air

Charter Company on the side. Some other

accesses arose accidentally, caused by careless

or sloppy design. Their utility to telephone

enthusiasts had resulted in a large-scale hunt

for them. A list of these trunk accesses was

eventually passed to the Post Office. Neverthe-

less, suggestions of "sabotage from within"

are hotly denied by the Post Office. But a

recent example is an "engineers fiddle" fitted

to the Chiswick exchange. It allowed North

London Post Office staff who knew it to make

free STD calls, quite illegally, from phones

all over London. By dialling 995 for Chiswick.

then 47, then any four digits to "unlock" the

circuit (since someone, perhaps even an

investigator, might stumble upon 995-47 by

accident), they would be enabled to dial free calls. This money saving device disappeared earlier this year, when the code became needed for new subscribers on that exchange and the engineer had to take it out. Two devices to avoid payment were displayed at the trial. One, known as a black box or non-charge facility, is simply a battery and two simple components that can be fitted to any telephone and prevent the exchange from realising that the called telephone has been



The Post Office goes to great, but ansuccessful, lengths to keep its secrets. The centre door (31-32 High Holborn) is the unmarked entrance to the Kingsway exchange, London's largest traunk exchange, located in two deep level bomb shelters under Chancery Lane underground station. answered---thus no charge is made to the caller.

The other was more amusing—a 2p piece on a length of thread. Its student owner had not known that it could be used for telephones, but a zealous executive engineer studied the problem and showed the court how, with a little legerdemain, it could be retrieved from the reject slot of the coinbox.

Telephone tapping?

As might be expected in Watergate year, allegations of telephone tapping were well to the fore, and several Post Office methods were exposed. The first, and simplest, is a printermeter, which makes an automatic record of whom you call, for how long, and the exact time and date of the call. The second is the misuse of special test circuits to listen in to any call. The operator or monitor merely has to dial your number on

An Old Bailey anniversary

This year is the 20th anniversary of another Old Bailey telephone conspiracy trial. In that year, a Mayfair chemical company director and two friends were accused of making automatic trunk calls around Britain—almost 10 years before STD was introduced. And all for a single charge of an old penny.

Their method was known as the Toll A drop-back, named after Toll A, an exchange near St Paul's which routes calls between London and nearby non-London exchanges. The trick was to disi a number, such as Dartford 21111, which was then not allocated. Then, the received rest would be "flashed" (depressed for '2, a second). This would act in a rather similar way to the "clear forward" on the a.c. system. The caller would be left with an open line into the Toll A exchange.

The user could then dial a code, 018, which would take him on to what was then the first trunk (long distance) exchange in Britain. Once again with a list of trunk codes which he would have compiled by experimentation, he could dial around Britain. The advantages of these methods in 1953 was immense. The delays on trunk calls through the trunk operator; could often be several hours, and the quality very poor.

The method is still available. One of the defendants in last month's trial was alleged to have made experiments by using a Toil A dropback. He had dialled Caterham 41111, a number not in use. Then by flashing, he could dial through the Toil A exchange, and out through exchanges around London to some point where he would be able to dial up onto the trunk network.

In May, a London chemiatry student pleaded guilty to making calls to the US utilising Toll A dropback via exchanges in Surrey where trunk accesses had been fitted at the time. He was fined £70 plus £10 costs and ordered to pay the Post Office £350 for last revenue. New Scientist 13 December 1973

these special circuits, and listen for as long as he likes. The intended use for such circuits to interrupt a call to tell you that someone is trying to call you from abroad, for instance

The third is the euphemistically named "Call Check Circuit"—this can be attached to any phone in the country—and is undetect able. It can be used with a tape recorder the record all incoming and outgoing calls. Identifiable only by the type number painted on it, 60345, it is now fitted as standard equipment.

The British Post Office is not the only organisation with pranksters prowling through their system. In the USA, the vast telephone network has been blighted for some years by the phenomenon. For technical reasons, the Bell system is far more open to the possessor of the Blue Box, as a bleeper is known across the Atlantic. Forty years ago world telephone technologies diverged. The Bell system, which owns almost all of North America's 140 million telephones, started to use the crossbar system, while Britain stuck to the Strowger method, invented by a Kansas City undertaker in the 1890s. The effect of crossbar on the trunk network was to enable the same codes that are used for the nationwide dialling system to be used for the internal codes of the system, resulting in far greater reliability and faster operation. It also uses a multifrequency signalling system, using frequencies between 700 Hz and 1700 Hz Because of the identical codes usage. US phreaks are spared the hard work of compiling and using special trunk codes as in Britain.

The phreaks first appeared on the US scene in the early 1960s, when a group of MIT students were found to have conducted a late night dialling experiment on the Defense Department's secret network. They were rewarded with jobs when they explained their system to Bell investigators. The attitude was a little different a few year later when blind Joe Engressia, sometimes acclaimed as the "King of the Phone Phreaks" was discovered merrily whistling down the line to fix up free calls round the world for his school friends. As a result of his widely-publicised prosecution, many individuals who had been working in the dark, alone, across the continent rang in to Blind Joe. The new technology spread rapidly through the underground and names like Captain Crunch and the Midnight Skulker became commonplace on illegally procured trunks. The name "phone phreak" identified the enthusiasts with the common underground usage of freak as someone who was cool and used drugs.

Since then, the telephone system has been a battleground between the phreaks and the Telcos (as the telephone comparies nickname themselves). Abbie Hoffman's Yippies, the Youth International Party, gave birth to a Phreak division whose monthly, The Party Line, publishes details of the latest and best in Anti-Telco hardware. It has recently diversified into using high-power magnets on parking meters in order to stay longer cheaper. In June 1972, Ramparts carried a set of step by step instructions on how to build

New Scientist 13 December 1973



Some optimists think that the North Sea is a bottomless well, with sufficient high grade energy to supply all the country's needs.

Some pessimists think that it's probably another proverbial bubble: that existing supplies will quickly be used up: that there's little future in it.

Neither has the right answer.

To be honest there is no certain answer. But natural gas is certainly vital to Britain's well-being. Here are some facts.

In only six years British Gas has already obtained sufficient supplies to:

Convert over nine million customers to natural

gas. This has involved converting over twenty eight million appliances.

To increase its sales by nearly three hundred per cent.

To increase its share of the domestic central heating market to more than three million households.

Further, the amount of additional gas available from the new Frigg gas field alone by 1978 could amount to as much as the total gas distributed by the whole of the British gas industry just 10 years earlier.

How much is there down there?

Nobody knows for sure.

But though natural gas cannot solve *all* our energy problems it is already playing a key role in our economy – a role that will become even more important with the advent of significant new supplies of natural gas from 1976 onwards.

So that British Gas will have an even more vital role to play. Our Vital industry