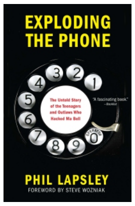


Exploding The Phone

www.explodingthephone.com

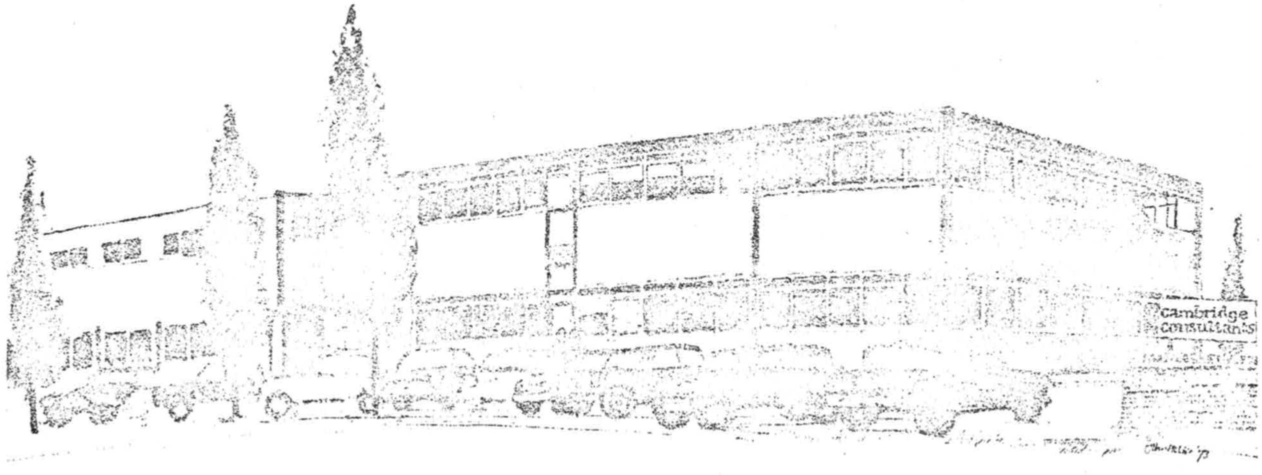
Bibliographic Cover Sheet

db340

Title	**Phone Phreaking**
Publication	*Interface magazine*
Date	1974-04-00
Author(s)	Brookfield, Mike
V/I/P	Vol. 8, No. 1, p. 8
Abstract	Overview of British phreaking.
Keywords	subscriber toll dialing (STD); British phreaking; British Post Office (BPO); blue box; AC9 signaling system; MF2 signaling system
Notes	Article is 2 pages; our copy includes a copy of the Table of Contents page. This article was reprinted in "Undercurrents" a few months later.
See also	db341
Source	Alan Rubinstein

interface

Volume 8 No. 1 April 1974



Contents

Interface is the house journal of Cambridge Consultants Ltd. All correspondence, MSS etc should be addressed to:
The Editor, Interface,
Cambridge Consultants Ltd., Bar Hill, Cambridge.

Editors : Hugo Davenport and Pat Preston
Art Editor: Ken Vail

Printed by: Cambridge Instantprint

Editorial

Over the past year a number of readers have commented on the introspective nature of *Interface* contributions, especially the non-technical articles and quotes. The Editors hereby acknowledge those comments but feel impelled to point out that a house journal must be inherently introspective to some extent. The question is merely that of degree.

The current Editorial feeling is that *Interface* reflects the ambience of CCL and while this is so the current almost non-existent Editorial policy will continue to be followed. As a concession, however, the Editor will try to avoid lavishing praise on the elegant shoulders of the Editrix (partly, it must be admitted, in deference to her own feelings on the matter).

Away from these introspections.

It's interesting to observe the development of public consciousness in the National Press. Take two examples : Pollution and The Fuel Crisis. Both these issues hit the headlines in the national dailies for the first time last year. What, the reader may ask himself, is so significant in that? Well, the significance is that both were being widely discussed in only slightly less universal periodicals, e.g. New Scientist and Scientific American, over two years previously. Assuming that fuel, pollution and other technological issues are important to the public it seems a pity that they are publicised only on the eve of disaster, as it were. On the other hand there is little point in alarming the public unless some material advantage ensues (i.e. starting a resources conservation/utilisation programme at an earlier date than would otherwise be the case), and it is difficult to imagine any government making long range plans which extend beyond the next election date in the absence of desperately compelling reasons. Let's hope that really long range planning is a habit developed by government and industry alike.

'PHONE PHREAKING

Mike Brookfield

Have you met the author?

Mike Brookfield graduated in physics at Hull University before furthering his studies in solid state physics at Sussex University where he obtained an M.Sc. He worked for 4 years in the Optics Research Group at the British Aircraft Corporation before undertaking a second M.Sc. at Reading University in applied optics. This was followed by a 3 year post in optical design at Watsone, Barnet before joining CCL in 1973.

Telephones are interesting, and fun to play with. People whose hobby is playing with telephones are known as 'phone phreaks' in the USA, a term which is not very popular in this country. The polite term 'telephone enthusiast' is sometimes used instead.

Anyone interested in amateur radio can go to his local library and find a shelf of books telling him how to annoy his neighbours by interfering with their television pictures. Unlike such normal hobbies it is not so easy to find information on the subject of 'phone phreaking. When I first became interested in telephones I was more or less on my own and I spent a lot of time trying to find other telephone enthusiasts. This was an interesting exercise, full of odd surprises. On one occasion I spent a lot of time tracking down rumours of one individual who turned out to be no other than myself. Some people get interested in telephones simply by meeting established 'phone phreaks. I feel that one misses something by this.

To understand what 'phone phreaking is all about one needs to know a little about telephone systems.

The British Telephone System

Telephone exchanges in the UK are arranged in a hierachical structure based on about 40 zone switching centres, 350 group switching centres and about 6,000 minor exchanges. Each group switching centre (GSC) is a member of a zone and its zone switching centre is its primary route to the trunk network. Similarly, each of the minor exchanges has a GSC as its parent.

In addition to this basic structure there are further circuits, GSC to GSC, minor to minor exchange and so on, provided that there is a sufficient demand to justify them.

Until the introduction of Subscriber Trunk Dialling (STD) in 1959, telephone operators handled all trunk traffic. By this time most of the network was automatic in the sense that one originating operator could complete a call by dialling, over the trunk network, codes which routed the call from one centre to another.

Following the introduction of STD, the responsibility for the setting up of the call was placed upon the subscriber. Now the most costly part of a telephone system is the provision and maintenance of circuits between exchanges and this dictates the philosophy behind the working of the system.

The STD equipment dials calls over the trunk network automatically and in this way replaces the local operator. The equipment is full of safeguards which ensure that, either by accident or misuse, a subscriber does not waste time on trunk circuits. For example, a subscriber cannot let a call ring indefinitely : he will be automatically disconnected after about 3 or 4 minutes.

Most of the automatic switching equipment in the U.K. is based upon the older type of electromechanical switching known as the Strowger (or step by step) system. This type of equipment responds directly to the impulses set up as one dials. As a result, there is a very close relationship between the codes dialled and the way in which the call is routed.

If one looks at the dialling code booklet issued to subscribers one will find that it is divided into two parts. The first gives dialling codes for 'local' calls and the main part of the booklet gives the dialling codes for trunk calls. These local codes operate Strowger switching equipment. If one studies the local dialling codes published for a few neighbouring exchanges it is possible to break them down into their component routings. It is then possible to string them together to reach distances of up to about 70 miles. It is through discovering this that many people, myself included, first became interested in telephones. This stringing together of local codes is known as 'chaining' and is of restricted interest since the lines are unamplified and of low quality.

The STD codes consist of the digit zero followed by a three digit 'area code' and, in the case of minor exchanges, further routing digits. The initial zero connects a subscriber to the STD routing equipment. The next three digits bear no relation to the routing digits actually needed to set up the call and are the same all over the country. They were allocated as a mnemonic in the days when telephone dials had letters on them.

The heart of the STD equipment is a register translator (RT). This splits off the area code and translates it into the appropriate routing digits, indeed the same ones that an operator would dial. Meanwhile the remaining dialled digits are stored in a register. The equipment first pulses out the routing digits got from the translator and follows them with the digits stored in the register, these being the final routing digits (for minor exchanges) and the called number. Having done this the equipment switches through the speech path and the register translator releases itself in preparation for the next call leaving control to a piece of equipment called a register access relay set. This piece of control equipment has obtained the appropriate metering rate for the call from the translator, and when the call is answered it steps the subscribers meter at this rate.

Trunk Access

Theoretically, the only way that a subscriber has of obtaining a trunk circuit is either via the local operator or through the STD equipment. Neither of these methods allows one to explore the telephone network which is what the 'phone phreak wants to do. In practice there are other ways of gaining access to the trunk network. For a variety of reasons there are ways of dialling from the local codes, to which a subscriber has proper access, onto trunk routes. One way in which this can happen is occasionally a local route can terminate at a GSC with the same status as an incoming trunk route. When this happens one may dial the appropriate local code followed by the digit '1' and gain access to the trunk circuits at the distant GSC.

Another type of trunk access arises when post office engineers within an exchange wire up their own irregular circuits. A variety of techniques are used to conceal this type of circuit. One of these came to light last year in Bristol as a result of a Post Office prosecution. One dialled 173 and received a continuous 'number unobtainable' tone (as one should, it is a spare code). However, if one waited for 30 seconds, this would switch through to Bristol trunks.

One person who was prosecuted was apparently running an air charter company and making all his telephone calls abroad free of charge.

A more common type of concealment occurs when, instead of waiting as above, one had to dial a further code, most commonly a digit zero. If more than one such digit is required then the access becomes difficult to find.

In spite of such attempts at concealment a large list of these was compiled. To explore the trunk network using one of these one would use the 'chaining' method to the nearest exchange providing such a trunk access. If one was lucky one's own exchange would possess one.

As a result of recent publicity the Post Office has tightened up on its own internal security and now only relatively few of these accesses are left. Fortunately, there is a more powerful way of gaining access to trunks and this involves simulating the control signals that are used on trunk routes. To explain how this can be done it is necessary to describe first the principles of telephone signalling.

Telephone Signalling Systems

Dial pulses, which originate at the subscriber telephone on dialling, periodically interrupt the DC path between the telephone and the exchange. This is known as loop disconnect signalling and is also used over local links between exchanges. It is not suitable for signalling over longer links because the pulses get distorted, or over microwave links where there. is no DC path. Over the majority of trunk routes a type of signalling known as AC9 is used. This employs a single signalling frequency of 2280 Hz which is within the audio pass band of the circuit. Digits are transmitted as impulses of this frequency sent at dial pulse speed (10 pulses per second). Control signals are also at 2280Hz. For example, on completion of a call a continuous tone at this frequency is sent to clear down the circuit.

The STD system as already described is inadequate in many ways. It is capable of providing only relatively simple translations and this is why subscribers who have STD cannot dial all of the exchanges on the automatic trunk network. Further, if congestion is met on any of the links within a routing then the call will fail whereas an operator would either redial or try an alternative routing. It was decided from the outset that it would be uneconomical to extend the planned STD system to cope with these problems and so a different approach known as 'transit working' was planned. Accordingly, a completely independent trunk network is being built and is now gradually coming into operation. This is known as the trunk transit network.

In the transit mode the area code is examined by the originating RT as before but instead of producing a complete set of routing digits it simply seizes the first free circuit to the most likely exchange capable of handling that call. If there are no free circuits then it tries its next choice of exchange. This distant switching centre then requests the original area code and upon receipt of this from the originating RT it will set up the next link in the same way. The intermediate RT is then released and plays no further part in the connection of the call. This process continues until the call reaches its required destination whereupon the distant RT sends back a signal to initiate the transfer of the contents of the originating register to the final register and the call is then established as before.

The area code has to be repeated by the originating RT to each of the intermediate switching centres and a slow signalling system such as AC9 is unsuitable. A high speed signalling system is therefore used and is known as SSMF2. This uses a combination of two frequencies out of a total of six to represent digits.

A digit may be sent in 160 milliseconds, compared to a maximum of 1 second when using AC9. Signals in the backward direction are needed, for example to request the area code, and these are based on a further six frequencies. Supervisory signals are again at 2280Hz in most cases, these including the forward clear for example.

The Blue Box

It has been seen that the control signals employed within the inland trunk network are audio signals within the passband of the telephone circuit. Armed therefore with a set of audio oscillators and some means of playing combinations of these into one's telephone one can imitate these signals. A device capable of doing this is known as a 'blue box' in the USA and as a 'bleeper' in this country. With such a device the entire telephone system of the world, is then at your command.

To imitate signalling system AC9 all that one needs is a single oscillator running at 2280Hz and a method of interrupting this at dial pulse speed. A second telephone dial is a simple and convenient method. In practice one would start by dialling an ordinary STD call and then, before the call is answered, send a short burst of tone. This 'clears down' the call and one is left with an outgoing trunk route. This first link is not released because the telephone is still 'off the hook' and the D.C. holding conditions are still applied at the local GSC. A second burst of tone will then re-seize in the sense that the switching equipment is reconnected at the distant GSC in preparation for the receipt of routing digits. These are sent using the auxiliary telephone dial just as if one was an operator or was using a trunk access.

Simulation of the MF2 signals requires, of course, six oscillators and the procedure is more complicated. However, one does not need to know any internal trunk routing digits.

Once one has unrestricted access to the trunk network in this way it is possible to gain access to the international circuits as well. Over these circuits different signalling systems are employed and these too are normally in-band systems. More sophisticated 'blue boxes' allow one to simulate these as well and one can go even further and simulate the signalling used internally in other countries. This will be the subject of a further article.

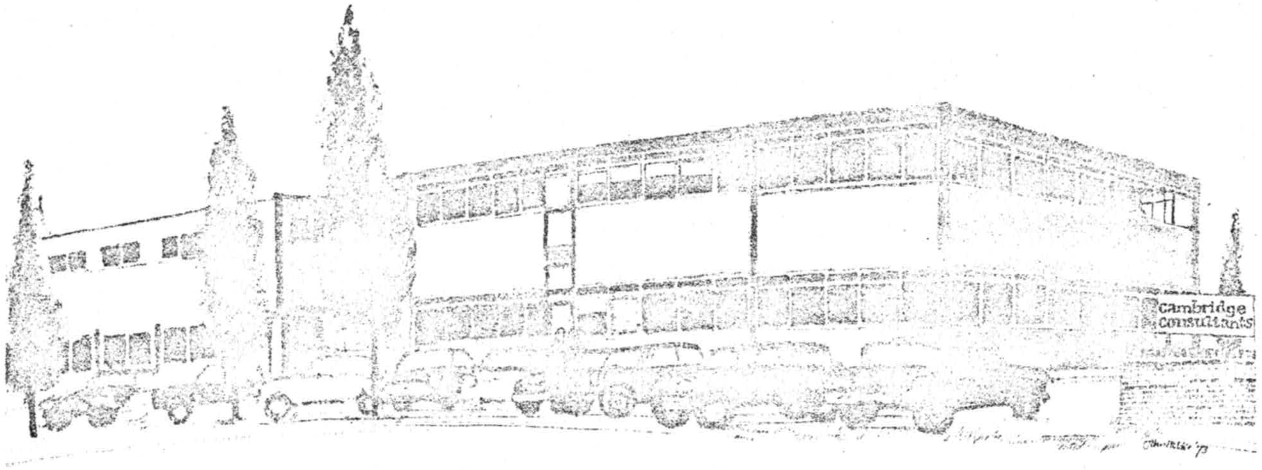
Having acquired a 'blue box' the way one explores the network is very much a question of personal taste and people tend to specialise as in any hobby. To start with, most 'blue box' owners just play around and enjoy the novelty of having the world at their fingertips. Calls to various information services are popular as are calls to international operators, who are very friendly. It is a pleasant diversion on a winter evening to discuss surfing with the Honolulu operator or to chat about the weather with the Sydney operator.

One type of circuit that is quite popular is the conference call whereby a number of enthusiasts are connected together : here the conversation often tends towards 'phone phreaking. This type of circuit arises either by accident or by design. One example of the 'accidental conference' was Londonderry. One of its dependent exchanges got demolished by a bomb and all circuits from Londonderry to this exchange were connected together onto a recorded announcement. This recorded announcement became disconnected and a conference was born. Conferences also occur on an international scale and are very popular in America, where they are sometimes very sophisticated.

So far nothing has been said about the legality (or otherwise) of 'phone phreaking. Using a blue box one can make a 'phone call to virtually anywhere in the world at the cost of a local call or even free of charge. To make a 'phone call to somebody in this way is clearly fraudulent and if caught you would face prosecution. On the other hand, to use a 'blue box' for the purpose of exploring or studying the telephone system the situation is by no means so clear. When using an AC9 simulator, the very first forward clear causes the equipment to start metering the

interface

Volume 8 No. 1 April 1974



Contents

Interface is the house journal of Cambridge Consultants Ltd. All correspondence, MSS etc should be addressed to:
The Editor, Interface,
Cambridge Consultants Ltd., Bar Hill, Cambridge.

Editors : Hugo Davenport and Pat Preston
Art Editor: Ken Vail

Printed by: Cambridge Instantprint

Editorial

Over the past year a number of readers have commented on the introspective nature of *Interface* contributions, especially the non-technical articles and quotes. The Editors hereby acknowledge those comments but feel impelled to point out that a house journal must be inherently introspective to some extent. The question is merely that of degree.

The current Editorial feeling is that *Interface* reflects the ambience of CCL and while this is so the current almost non-existent Editorial policy will continue to be followed. As a concession, however, the Editor will try to avoid lavishing praise on the elegant shoulders of the Editrix (partly, it must be admitted, in deference to her own feelings on the matter).

Away from these introspections.

It's interesting to observe the development of public consciousness in the National Press. Take two examples : Pollution and The Fuel Crisis. Both these issues hit the headlines in the national dailies for the first time last year. What, the reader may ask himself, is so significant in that? Well, the significance is that both were being widely discussed in only slightly less universal periodicals, e.g. New Scientist and Scientific American, over two years previously. Assuming that fuel, pollution and other technological issues are important to the public it seems a pity that they are publicised only on the eve of disaster, as it were. On the other hand there is little point in alarming the public unless some material advantage ensues (i.e. starting a resources conservation/utilisation programme at an earlier date than would otherwise be the case), and it is difficult to imagine any government making long range plans which extend beyond the next election date in the absence of desperately compelling reasons. Let's hope that really long range planning is a habit developed by government and industry alike.