TAPPING THE TELEPHONE

POEU
Post Office Engineering Union

Tapping The Telephone

31st July 1980

Printed and Published by the Post Office Engineering Union
Greystoke House, 150 Brunswick Road, London W5 1AW. Tel. 01-998 2981

"TAPPING THE TELEPHONE"

LIST OF CONTENTS — PAGE NO.

INTRODUCTION : THE POEU'S INTEREST 1

THE HISTORICAL BACKGROUND

Previous Enquiries 2
Current Concern 3

IS TAPPING LEGAL?

Arguments About Interception Of Letters 5
Arguments About Interception Of Telephone Calls 6
The Malone Case 7
The European Convention 8

WHO IS TAPPED?

Number And Kinds Of Warrants 10
Criteria For Issuing Warrants 11
Tapping Members Of Parliament 13
Tapping Political And Trade Union Activists 15

HOW IS TAPPING CONDUCTED?

The Warrant Procedure 18
How The Post Office Taps 19
Other Surveillance Techniques 20
The Effect Of New Technology 22

THE CASE FOR AN ENQUIRY

The Omissions Of The White Paper 25
Reservations About The Proposed Monitoring 26
Reasons For An Enquiry 27
Form Of The Enquiry 28

PROPOSALS TO BE PUT TO THE ENQUIRY

Proposals On Interception Of Communications 30
Other Related Proposals 32

PAGE NO.

CONCLUSION : A CASE TO BE ANSWERED 34

ANNEX A - Telephone And Letter Interceptions In England And Wales: Table

ANNEX B - Telephone Interceptions In England And Wales: Graph

ANNEX C - Telephone And Letter Interceptions In Scotland: Table

ANNEX D - Telephone Interceptions In Scotland: Graph

INTRODUCTION: THE POEU'S INTEREST

The interception of communications has been the subject of much public comment in recent months. The 125,000 members of the Post Office Engineering Union are all concerned with the operation of public communications networks, either telecommunications or posts, so that we have a direct occupational interest in the issue of interception.

Our concern is two-fold. First, we take a professional pride in our work of providing public communication services and we would have a principled objection to being associated with any illegal or improper use of the communications networks. Second, we value highly our relationship with the public whom we serve and we do not wish our customers to doubt the integrity of our members.

As long ago as 1966 in our evidence to the Donovan Commission, we said:

> "The Union has always considered that it has a relationship with the public and not merely with the Post Office. Because the telephone service is a well established Government monopoly the Union has consistently and deliberately made public statements over the years drawing attention to aspects of the telephone service which it felt required public or parliamentary consideration."
>
> ("Evidence of the Post Office Engineering Union to the Royal Commission on Trade Unions and Employers' Associations", Page 9).

It is in that spirit that we have produced and are publishing this report.

We wish to make our basic position absolutely clear from the outset. We would not wish to do anything which undermined the security or order of the State. Equally, we would not wish to do anything that challenged the democratic values of our open society or the privacy of the individuals who live in it. It is against these twin criteria that we have examined the various issues raised by the interception of communications and especially telephone tapping.

We have studied the historical background, the legality of tapping, the subjects of tapping and the methods of tapping. Our examination has led us to the firm view that the potential for abuse is now so great that the present safeguards are fundamentally inadequate and new procedures are vitally necessary. Therefore, we reject the Home Secretary's White Paper as an acceptable basis for telephone tapping and we set out a powerful case for a full scale enquiry and outline the proposals that we would wish to put to such an enquiry.

Most of our report is concerned with telephone tapping, since some 95% of POEU members work for the Post Office Telecommunications Business and some 90% of officially authorised interceptions of communications now concern telephones. However, the enquiry which we are seeking should cover interception of the mail and the principles which we are advancing should apply equally to the post.

THE HISTORICAL BACKGROUND

Previous Enquiries

There is evidence that the interception of mail has taken place for some 400 years. From time to time, the practice has been subject to public concern and political debate.

In 1844, there was the most serious agitation which has ever occured on the issue of detaining and opening letters. At that time, it was revealed that the Secretary of State, Sir James Graham, had issued a warrant to open the letters of an Italian revolutionary, Joseph Mazzini, and had communicated some of their contents to the Neapolitan Government.

Following debates in both Houses of Parliament, two Secret Committees were established, one of the House of Commons and one of the House of Lords. Both committees were asked to enquire into the state of the law in respect of the detaining and opening of letters at the General Post Office.

This was the last such enquiry for over a century.

The interception of telephone messages has taken place since the introduction of the telephone, although it was only in 1937 that the Home Secretary and the Postmaster-General decided that such interception should only be conducted on the authority of a warrent from the Secretary of State.

In 1956, there was a public row following revelations about the use made of transcriptions produced as the result of the interception of the telephone of the gang leader, Billy Hill. The Home Secretary, Viscount Tenby, authorised the police to show the transcriptions to the Chairman of the Bar Council, Sir Hartley Shawcross, and subsequently to other members of the Bar Council and the Benchers of Lincoln's Inn who were enquiring into the professional conduct of a barrister called Marrinan.

Criticism of the Marrinan case was headed off by the new Home Secretary, Rab Butler, through the appointment in June 1957 of a Committee of Enquiry chaired by Norman Birkett. The Committee studied carefully the two reports of 1844. It reported in October 1957:

> "Report Of The Committee Of Privy Councillors Appointed To Enquire Into The Interception Of Communications."
>
> (Cmnd.283).

The Committee said that Viscount Tenby had made a "mistaken decision". It concluded:

> "We are satisfied that interception is highly selective and that it is used only where there is good reason to believe that a serious offence or security interest is involved."
>
> (Para.156).

Figures for the number of authorised interceptions were given for the full period 1937-56.

For the next 23 years, whenever public disquiet was expressed about telephone tapping, successive Home Secretaries fell back on the Birkett report. Indeed its continued relevance has been such that in 1977 it was re-printed. All that changed was the price: instead of 1s 9d it now costs 75p. Repeatedly Home Secretaries have refused to provide even the overall number of warrants issued for the tapping of telephones.

Current Concern

The current phase of intense interest in telephone tapping was sparked-off by the judgement in the case of Malone v. the Commissioner of Police for the Metropolis on 28th February 1979. It was fuelled further by an article by Duncan Campbell in the edition of the "New Statesman" dated 1st February 1980, which was actually trailed extensively by David Leigh in a front page article in the "Guardian" on 31st January 1980. This article alleged that the British national telephone tapping service operates from a Post Office building on Ebury Bridge Road, London SW1 and that the facilities contain the capacity to tap 1,000 lines simultaneously.

The POEU had been considering the issues raised by telephone tapping since an approach from one of our Branches about the time of the Malone case. On 31st January 1980, we issued a statement from the General Secretary, Bryan Stanley, which said:

> "The Post Office Engineering Union, which represents the engineering and technical grades in the Post Office Telecommunications Business, is concerned about current statements regarding the interception of telephone communications. Therefore, as recommended by the Shadow Home Secretary, Merlyn Rees in the House of Commons debate on the Blunt affair, we believe that the Government should institute an immediate enquiry into all aspects of telephone tapping. Such an enquiry might be conducted by three Privy Councillors and should result in as full a public report as is consistent with proper security considerations.
>
> The last such enquiry was in 1957. We are convinced that public concern on this sensitive issue now merits a fresh enquiry as a matter of urgency. This enquiry might well establish that the situation has changed signifcantly since the Birkett report of 23 years ago and it would establish that Post Office engineers are not involved."

Others made similar demands for an enquiry and for a time it looked as if one might be established (see, for instance, the "Observer", 9th March 1980). However, instead the Home Secretary, William Whitelaw, contented himself with a White Paper published on 1st April 1980: "The Interception Of Communications In Great Britain" (Cmnd.7873). The White Paper reaffirmed the principles of the Birkett report and offered no new safeguards. Nevertheless, it did supply figures for the number of authorised interceptions from 1958-79.

In an associated statement to the House of Commons, the Home Secretary announced that he would appoint "a senior member of the judiciary" to monitor the procedures for telephone tapping. For some reason, it took two months to find

the man, but on 5th June 1980 he was named as Lord Diplock. Since the White Paper makes no mention of the appointment of a judge and since it took so long to name him, it is likely that the proposal was something of an after-thought, a last minute effort to head off political concern.

The POEU is not willing to let matters rest there. We regard the White Paper as a totally unsatisfactory effort to reassure the public. We repeat our earlier call for a full enquiry and we have sound reasons for doing so.

IS TAPPING LEGAL?

Arguments About Interception Of Letters

It seems astonishing that one should need to question the legality of the interception of communications. After all, the practice has been conducted for centuries and it raises sensitive issues of national security and individual liberty, so most people have taken it for granted that such a practice must have express legal authority. The truth is far more complicated.

Both the Secret Committees of 1844 avoided any discussion of the actual source of the authority upon which the Secretary of State exercised his power to open letters. This is surprising because, in the debates which preceded the setting up of the Committees, the origin of the power had been discussed. Equally, the White Paper of 1980 made no reference whatsoever to the legal authority to tap telephones. This amounts to little less than evasion, since the original need for a statement from the Government was the Malone case where the legal position of tapping was the central issue.

By contrast, the Birkett Committee in 1957 devoted almost a quarter of its report (9 out of 39 pages) to the critical question of the authority of the Secretary of State to intercept communications. A careful reading of the relevant pages reveals a tortuous set of arguments, none of which is wholly satisfactory.

The Birkett Committee opened its examination of the legal question with the incontestible words:

> "The origin of the authority of the Executive to intercept communications is obscure ..." (Para. 9).

Starting with the power of the Secretary of State to issue his warrant for the interception and opening of letters, the Committee examined three arguments.

First, it was argued that the power was an exercise of the prerogative right of the Crown and it would appear that this view was held by the Home Office. However, the Committee noted the telling observation of opponents of this view that:

> "No statutory writer when dealing with the Royal Prerogative mentions this particular power as being a prerogative power" (Para. 23).

Second, it was argued that the power lay in a common law right which was not a part of the Prerogative but which derived from an inherent power in the Crown to protect the realm against the mis-use of postal facilities by ill-disposed persons. However, the Committee undermined this argument with the observation that:

> "No support for this view is to be found in any judicial pronouncement or in any legal textbook" (Para. 28).

Third, it was argued that the power had been in existence from the earliest times:

> "How it arose can only be conjectured because historical records are wanting, but that the power existed and was used permits of no doubt whatsoever" (Para. 30).

On this view, the power was recognised if not expressed in Section 58(1) of the Post Office Act 1953 which reproduced Section 56 of the Post Office Act of 1908 which reproduced Section 25 of the Post Office (Offences) Act 1837 which in turn re-enacted without material amendment Section 40 of the Post Office (Revenue) Act 1710 and before that relevant legislation included the Proclamation of 1663, the Act of 1660 and the Ordinance of 1657 and before that the power can be traced to Orders in Council of 1627 and 1626 and before that is mere conjecture. The crucial point to appreciate about this argument is that, however far back one traces the legislation, none of the statutes contain clauses conferring the power to intercept communications. They simply recognise a power presumed to exist.

At the conclusion of the review of these bewildering arguments, the Committee noted with relief:

> "We recognise that we have no authority ourselves to decide between these conflicting views and to declare the law" (Para. 38).

Arguments About Interception Of Telephone Calls

If then, the origin of the power to intercept the mail is obscure in the extreme, the problem is merely compounded when one considers the power to tap telephones.

If one assumes the power is part of the prerogative right of the Crown (apparently the view of the Home Office), then there is still the previously mentioned objection that no constitutional writer mentions the power as being a prerogative power. There is a further objection that the telephone did not exist when the prerogative power was first taken and exercised. The lawyer overcomes this objection by reference to a court case of 1915 but the laymen who constitute the public will not be so easily assured.

If, alternatively, one assumes that the power to tap is a common law right, then there is still the previously mentioned objection that there is no authoratative legal support for this view.

If one assumes that the power to tap is not a prerogative power and not a common law one either, then one is forced finally to seek statutory authority for it and the Birkett Committee took the view that the only statutory reference to be considered was Section 20 of the Telegraph Act 1868 which states:

> "Any person having official duties connected with the Post Office or acting on behalf of the Postmaster-General, who shall, contrary to his duty, disclose or in any way make known or intercept the contents or any part of the contents of any telegraphic messages or any message intrusted to the Postmaster-General for the purpose

of transmission, shall in England and in Ireland be guilty of a misdemeanour, ... and the Postmaster-General shall make regulations to carry out the intentions of this section, and to prevent the improper use of any person in his employment or acting on his behalf of any knowledge he may acquire of the contents of any telegraphic message".

However, as the Birkett Committee observed:

"It is a little difficult to think that the word "intercept" in Section 20 of the Act of 1868 contemplated the listening in to telephone conversations for the telephone exchange was only instituted in England in 1879 and then there were only seven or eight subscribers" (Para. 46).

At the conclusion of this further set of bewildering arguments about the source of the power to intercept, the Committee noted unconvincingly:

"We favour the view that it rests upon the power plainly recognised by the Post Office statutes as existing before the enactment of the statutes, by whatever name the power is described" (Para. 50).

To summarise an admittedly complex situation: it is not seriously suggested that the interception of communications is actually illegal but no-one can identify a legal or statutory basis for the power.

We have reviewed the legality of the interception of communications at some length because we believe it to be a crucial issue and we are convinced that most members of the public are simply unaware that so totalitarian a power has no express legal authority. We feel sure that, when they appreciate the point, they will be both surprised and deeply disturbed by it.

Even the Birkett Committee recognised that the situation was unsatisfactory:

"If, however, it should be thought that the power to intercept telephone messages was left in an uncertain state that was undesirable it would be for Parliament to consider what steps ought to be taken to remove all uncertainty if the practice is to continue" (Para. 52).

After 23 years, Parliament has taken no steps whatsoever.

The Malone Case

It was this uncertain legal position that was the heart of the previously mentioned case of Malone v. the Commissioner of Police for the Metropolis which lasted from 22nd January - 28th February 1979. It was the first ever court action in this country on the subject of telephone tapping.

James Malone, an antique dealer from Coldharbour, near Dorking, Surrey, discovered that his telephone was tapped because, while standing trial in June 1978 on charges of dishonest handling, he discovered a page in the notebook of Det. Sgt. Peter Ware with a transcript of a telephone call which he had made. After an adjournment, counsel for the Crown confirmed

to the court that the telephone had indeed been tapped.

In the subsequent court case brought privately by Mr Malone, counsel for Mr Malone called for three declarations from the presiding judge:

- that the interception of Mr Malone's telephone by the Metropolitan Police on the Home Secretary's warrant was not lawful under British law

- that the Government's behaviour breached the rights to privacy and respect for correspondence enshrined in the European Convention on Human Rights

- that it was a further breach of the European Convention that Mr Malone had no remedy against the Government in the United Kingdom.

In fact, in the course of the trial, no evidence was given to demonstrate that a warrant had been issued authorising the tapping of Mr Malone's telephone. At the end of the trial, the judge, the Vice-Chancellor, Sir Robert Megarry, gave a 73 page reserved judgement which took two hours, ten minutes to deliver (see "Volume II All England Reports 1979"). He said that the practice in Britain was not one on which "it is possible to feel any pride in English law" and he argued that it "cries out for legislation". Sir Robert ruled that telephone tapping in this country is not illegal but that the system is so open to abuse that it is "abundantly clear" that British practice would be found to be unacceptable by the European Court on Human Rights. However, he insisted that the European Convention was not enforceable in the British courts.

The European Convention

So, if politicians had not previously appreciated the unsatisfactory state of British law on telephone tapping, after the Malone case they had no excuse. Mr Malone has now petitioned the European Commission and this leads us to a brief consideration of the likely outcome of this or a similar case.

The United Kingdom has been a signatory to the European Convention on Human Rights since 1951 and it agreed to the right of individual petition by its citizens in 1966. In exercising this right, Mr Malone is arguing that the British position on telephone tapping breaches two Articles of the Convention, Article 8 on privacy and Article 13 on protection against state interference.

Article 8 states:

"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or

crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Mr Malone is arguing that British practice is in breach of this Article, since there is no express legal authority for tapping and there are inadequate safeguards upon the exercise of the power to tap.

Article 13 states:

"Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

Mr Malone is arguing that there was no way that he could discover with certainty whether or not the tapping of his telephone was the subject of a warrant and, if it was not, there was no remedy for him to use so as to seek compensation against the unlawful invasion of his privacy.

A good indication of the likely outcome of such a British case comes from consideration of the case of Klass and others v. the Federal Republic of Germany when the European Court gave its opinion on 6th September 1978. In this case, the European Court ruled that the signatory states of the European Convention did not have "an unlimited discretion to subject persons within their jurisdiction to secret surveillance", that telephone tapping was acceptable "under exceptional conditions" and that therefore certain minimum safeguards were necessary to protect the rights of the individual under Article 8 of the Convention. It held that the West German system just satisfied the minimum conditions. However, in West Germany interception is covered by legislation, the interception is supervised by a Parliamentary committee, there is a right of complaint against suspected interception and there is a requirement of notification to the victim once surveillance has ceased.

None of these factors applies in Britain and therefore it is almost certain that United Kingdom practice on telephone tapping is in breach of the European Convention. This point was forcefully brought to the attention of the Government by Lord Hooson in a short House of Lords debate on 21st May 1980.

For the British Government to propose no new legislative safeguards in the face of the Klass judgement followed by the Malone case makes our likely breach of the Convention flagrant as well as shameful. It may take Mr Malone or someone like him some years and significant expense to prove the point, but we earnestly hope that public opinion will force the Government and Parliament to act well in advance of such a politically embarassing episode.

WHO IS TAPPED?

Number And Kinds Of Warrant

There has been repeated and often rather wild speculation about the number of warrants issued for the tapping of telephones.

Only last year, someone as interested and relatively informed as Duncan Campbell wrote: "Such scanty evidence as is available points to at least 1500 or more official tapping warrants a year - almost a 10-fold growth since Birkett - and that of course does not include other methods used to get around normal procedures." ("New Statesman",9th February 1980). An even more recent estimate was even higher: "According to political sources the Home Secretary five years or so ago was authorising about 800 tappings a year. More recently the figure has risen to 2,000-3,000 a year." ("Sunday Times", 3rd February 1980).

In fact, we now know that for Great Britain (the territorial scope of the Birkett report and the White Paper) the latest figure (1979) for the number of warrants to tap telephones is 467 or about one-third of the Campbell estimate and about one-sixth of the highest "Sunday Times" estimate. Even allowing for the knowledge that some warrants cover organisations rather than individuals and the possibility that the published figures for any one year are merely new warrants instead of existing ones, it is still clear that the level of authorised tapping has been frequently and massively over-estimated.

Nevertheless, it has grown significantly over the period since the Birkett Committee reported - some 260% for England and Wales, much more for Scotland, and (if we knew the figures) almost certainly considerably more for Northern Ireland. Furthermore, all this says nothing about the scale of tapping without a warrant.

Annual statistics for authorised interceptions over the past 40 years are now available. The actual figures on warrants for telephone tapping in England and Wales are set out in Annex A and these are expressed graphically in Annex B. The actual figures on warrants for telephone tapping in Scotland are set out in Annex C and these are set out graphically in Annex D. These figures are drawn from the Birkett report and the White Paper and it will be noted that there are some gaps.

Another problem is that there is no break-down of these figures by the organisations granted the warrants. The Birkett report did make a very broad analysis of interceptions granted to the Police, Customs, Post Office and Security Service on the one hand and those concerned with drugs, lotteries and obscene publications on the other, but the White Paper does not even contain this kind of break-down.

Nevertheless, since different kinds of warrant are renewed for different periods - one month for the Police, two months for the Customs and Excise and six months for the Security Service (White Paper, para.11) - it is possible to make a rough estimate of the proportion granted for security purposes.

Duncan Campbell has calculated it as follows:

"The White Paper in a separate table, included figures for the number of warrants signed and in operation at the end of three sample years. These figures may be compared with the total number of warrants signed during the year:

Year	Signed During Year	In force at 31st. Dec.
1958	129	95
1968	333	155
1978	428	214

Since a normal warrant lasts only two months, the number of warrants said to be in operation at the years' end is astonishingly high. Since warrants for taps by the Special Branch and MI5 are normally renewed for six months at a time, the likely explanation is that most of the warrants go to those two agencies, and that many warrants are more or less permanent. On the basis of simple assumptions and some simple maths (warrants issued evenly through the year, and say, once) the proportion of 'security' warrants may be calculated. For 1968 and 1978, the proportion is about 75 per cent." ("New Statesman", 11th April 1980).

Of course, all this concerns only the taps officially authorised by warrant of the Home Secretary and does not include any official tapping without a warrant or unofficial tapping.

Criteria For Issuing Warrants

Officially the selection of individuals to be tapped is an extremely careful process involving strict criteria.

As far as interception of communications by the Police is concerned, the Birkett Committee set out in para.64 of its report the three conditions that must be satisfied before a warrant can be issued:

"(a) The offence must be really serious.

(b) Normal methods of investigation must have been tried and failed, or must, from the nature of things, be unlikely to succeed if tried.

(c) There must be good reason to think that an interception would result in a conviction."

As for the definition of "serious crime", it was said in para.65 that the Home Office regarded such crime as "offences for which a man with no previous record could reasonably be expected to be sentenced to three years' imprisonment, or offences of lesser gravity in which a large number of people were involved."

The recent White Paper repeated these criteria almost word for word but in para.4 "serious crime" was given a slightly but significantly wider definition: "an offence for which a man with no previous record could reasonably be expected to be sentenced to three years' imprisonment or an offence of lesser gravity in which either a large number of people is involved or there is good reason to apprehend the use of violence." The new element is violence.

No doubt some big time criminals are the subject of telephone tapping under the application of these criteria: the 1980 White Paper mentions the Great Train Robbery and other sources testify to the use of taps in Operation Julie (although it would appear that not all of these were the subject of warrants). However, on other occasions, it is not clear that the seriousness of the crimes really justified the invasion of privacy.

More concern has been expressed over "offences of lesser gravity" (that is, those attracting less than three years imprisonment) which might result in tapping, since numbers of people do not of themselves constitute seriousness and the reference to violence is totally unqualified as to severity. We are concerned that the formulation currently operated by the Home Office can be taken to include political meetings and demonstrations and trade union industrial action.

Besides these problems of interpretation, there is an additional point that the Home Office is dependent entirely on the evidence of the Police that normal methods have failed and that a conviction is likely to result.

As far as the interception of communications by the Customs and Excise is concerned, the definition of "serious crime" upon which the Home Office acts when considering the issue of warrants is that set out in para.66 of the Birkett report: "The case involves a substantial and continuing fraud which would seriously damage the revenue or the economy of the country if it went unchecked."

This formulation is repeated exactly in para.5 of the White Paper but it is pointed out that warrants under this head are now issued primarily in cases involving a systematic importation of illegal drugs (later identified as especially cocaine and heroin).

As far as the interception of communications by the Security Service is concerned, the principles governing the issue of warrants are set out in para. 6 of the White Paper:

> "(a) There must be a major subversive, terrorist or espionage activity that is likely to injure the national interest;
>
> (b) The material likely to be obtained by interception must be of direct use in compiling the information that is necessary to the Security Service in carrying out the tasks laid upon it by the Directive given to its Director General (the text of which was given in para. 238 of Lord Denning's Report in 1963, Cmnd 2152);
>
> (c) Normal methods of investigation must have been tried and failed, or must, from the nature of things, be unlikely to succeed if tried."

This formulation differs from that expressed in paras.67 and 68 of the Birkett report in two understandable ways (the use of the additional term "terrorist" and the reference to the Directive) but it omits the significant admission set out in para.68 of the Birkett report:

> "The same provison applies to the Security Service as to the Customs and Police about the failure of normal means of detection. But less stress is laid on the need to secure convictions, since the Security Service is primarily concerned with safeguarding the State and keeping itself informed about dangers to

its security. Besides securing convictions, the Security Service has the duty to keep up to date its information covering espionage and subversion and to inform Ministers and Departments of State about security matters that concern them."

Here again there are real problems of interpretation, since the definition of subversion is a notoriously political one that has been known to vary from time to time and from Minister to Minister. Furthermore, as with other kinds of warrants, the Home Office is dependent totally on the applicant agency for the information which it uses to decide on the issue of a warrant. However, where the agency is the Security Service, the problem is considerably more acute, since the 'need to know' principle is applied to Ministers and Civil Servants and the previously mentioned Directive (issued by Sir David Maxwell-Fyfe, then Home Secretary, in 1951) excludes Ministers from knowing the details of cases involving security and subversion.

Tapping Members Of Parliament

The strict application of the above criteria should lead to official telephone tapping being confined to criminals, subversives, terrorists and spies but considerable interest has been expressed in whether the telephones of Members of Parliament are tapped.

Two things can be said with reasonable certainty.

First, as far as the interception of communications is concerned, "a Member of Parliament is not to be distinguished from an ordinary member of the public." (Birkett report, para. 124) and therefore there is no reason why MPs telephones should not be tapped if application of the criteria suggests that it should. It seems that the only situation in which this might not be the case is if the communications being intercepted were held to be in connection with a Parliamentary proceeding but, since this term seems never to have been precisely defined, it could mean virtually any matter or no matter.

Second, the responsibility for this state of affairs lies with MPs themselves, although they have their long-time predecessors to thank for the situation. In 1735, the House of Commons approved a resolution (quoted in para.124 of the Birkett report) which seems to be a clear recognition by the House of the right of the Secretary of State to intercept MPs' mail. The Birkett Committee noted: "So far as we know this recognition has never subsequently been rescinded or modified." (para.125) and: "No question seems ever to have arisen in the House on the specific question of the interception of a Member's telephone conversation. Subject to any decision by the House on this point, it appears probable that the rulings concerning letters would extend by analogy to telephones." (para.127).

So the telephones of MPs can legally be tapped but the question remains as to whether they have been.

On 17th November 1966, the then Prime Minister, Harold Wilson, told the House of Commons:

".....I feel it right to inform the House that there is no tapping of the telephones of hon. Members, nor has there been since this Government came into office....

There was to be no tapping of the telephones of Members of Parliament. That was our decision and that is our

policy. But if there was any development of a kind which required a change in the general policy, I would, at such moment as seemed compatible with the security of the country, on my own initiative make a statement in the House about it." ("Official Report", 17th November 1966, Col.635-9).

In the famous Duncan Campbell article on telephone tapping, he wrote: "According to the tapping-centre employee who gave us some of the most detailed information, there was no MP's telephone being tapped during the Sixties. Thus, the assurances given by Harold Wilson in 1964 [sic] appear to have been honoured." ("New Stateman", 1st February 1980).

On 16th July 1970, the succeeding Prime Minister, Edward Heath, repeated the Wilson assurance that MPs' telephones would not be tapped "only with the proviso that the security of the State must be maintained". The then Prime Minister, James Callaghan, repeated the position on 26th May 1977 and the present Prime Minister, Margaret Thatcher, reiterated it on 27th July 1979.

However, many MPs have had occasion to believe that their telephones were being tapped. The evidence is necessarily circumstantial.

In 1950, Sir Tufton Beamish believed that his telephone conversation with someone in the War Office was intercepted ("The History And Practice Of The Political Police In Britain", Page 207).

Between August 1961 and January 1962, 15 Labour MPs were investigated by MI5 (at the request of Hugh Gaitskell, George Brown and Patrick Gordon Walker) and the techniques involved "telephone tapping, shadowing, opening of mail, examination of bank accounts, and other methods used by Intelligence Services." ("Daily Express", 28th June 1968; further details "Inside Story", Pages 22-23).

It would appear that up to October 1964 Conservative Ministers authorised the opening of mail and the tapping of telephones of an unspecified number of MPs. When questioned in the House of Commons, the succeeding Prime Minister, Harold Wilson, said: "When we came into office naturally I found out what was going on. I felt that the system of the previous Government in which MPs telephones were being tapped should be changed." ("Daily Telegraph", 12th April 1967).

It has been alleged that in 1974 Judith Hart, then a Minister, was tapped although she herself has never claimed this ("Sunday Times", 3rd February 1980).

In Northern Ireland, politicians such as Gerry Fitt and Ian Paisley appear to take it for granted that their telephones are tapped ("Guardian", 11th July 1978).

It was recently reported that MPs convinced that their telephones have been tapped include Neil Kinnock, a member of the Shadow Cabinet, and former Junior Ministers Michael Meacher and Bob Cryer ("Observer", 3rd February 1980).

Of course, some of these incidents could have involved tapping but of the telephone of the person to whom the MP was speaking at that time which would fulfill the terms of successive Prime Ministers' statements.

However, it would seem that the Prime Minister himself is not above surveillance. In the Summer of 1977, there was much concern over Chapman Pincher's suggestion in the "Daily Express" that Harold Wilson had been under electronic surveillance during a part of his time in 10 Downing Street and in his office at the House of Commons. This suggestion was re-asserted but revised by Pincher in Chapter 3 of "Inside Story" where he implies that the surveillance was in fact non-electronic. In either event, this is not actual telephone tapping but it does achieve precisely the same effect and more and it cannot possibly have been authorised by a Minister.

Still higher than the Prime Minister, it has been suggested that King Edward VIII's telephone was tapped on the instructions of the then Prime Minister, Stanley Baldwin, during and immediately before the Abdication crisis of 1936 ("Daily Telegraph", 20th November 1978).

Tapping Political And Trade Union Activists

MPs are not the only ones to fear that their legal activities are the subject of interception of communications. The same is true of many political trade union and pressure group activists especially those on the Left. This was the fear behind the Proposition passed by the POEU Annual Conference in June 1980:

> "To oppose by all means at their disposal the widespread and growing use of telephone tapping, by Government and its agencies to further the political ambitions that they have."

Again the evidence is anecdotal but disturbing.

Papers now removed from the Public Records Office show that during the General Strike of 1926, Ernest Bevin, then leader of the Transport & General Workers Union, had his telephone tapped ("Sunday Times", 3rd February 1980).

In "The History And Practice Of The Political Police In Britain", Tony Bunyan mentions a number of possible cases. These include eight members of the Executive Committee of the Associated Society of Locomotive Engineers and Firemen (Page 182), the office of the "Railway Gazette" (Pages 207-208), members of the Campaign for Nuclear Disarmament (Page 209) and an activist in the National Council for Civil Liberties (Page 209).

During the 1969-72 Stop The Seventy Tours Campaign, Peter Hain believed that his telephone was tapped on occasions ("Sunday Times", 3rd February 1980).

It has been alleged that telephones in Transport House, then the Headquarters for the Labour Party and still the Headquarters of the Transport & General Workers Union, were tapped for long periods in 1972 ("Times", 4th October 1974).

In 1976, Frank Field, then Director of the Child Poverty Action Group, believed that his telephone was being tapped as part of the Police investigation into the leak of Cabinet papers concerning child benefit ("Morning Star", 30th July 1976).

In early 1977, the National Council for Civil Liberties was given fairly reliable information that its telephone was being tapped as a result of its campaign against the deportation of Philip Agee and Mark Hosenball ("Privacy Report", Page 67).

In 1978, Jack Dromey, a leading member of the Grunwick Strike Committee, suspected that his telephone was tapped ("Sunday Times", 3rd February 1980).

Apparently a massive surveillance operation was mounted on certain participants in the Lancaster House talks on the future of Zimbabwe-Rhodesia ("Sunday Times", 3rd February 1980).

Earlier this year, the Iron & Steel Trades Confederation claimed that Police tapped telephones at their Rotherham office during the steel strike ("Times", 4th February 1980).

Most recently, Arthur Scargill, the President of the Yorkshire area of the National Union of Mineworkers, suspected so strongly that there was tapping of the telephones in both the area NUM Headquarters in Barnsley and his home nearby that he wrote to the Home Secretary on the matter but the Home Office refused to confirm or deny the suspicion ("Guardian", 1st July 1980).

Duncan Campbell has written: "Home and office numbers of union leaders and others involved in major industrial disputes are frequently, even routinely, tapped: MI5 appear to take the view that ministers have no 'need to know' about the details of surveillance operations." ("New Statesman", 1st February 1980).

Many journalists too are convinced that on occasions their homes and offices have been tapped and Anne McHardy, the Northern Ireland correspondent of the "Guardian", claims to have proof in her case ("Guardian", 11th July 1978).

Three points need to be made.

First, there is a good deal of alarmism in allegations concerning telephone tapping and we have no wish to add to it; equally, there is a measure of paranoia about the subject in some quarters and we do not wish to share in it. If more than a fraction of all the allegations about tapping were true, then it would require a vast surveillance operation which we doubt exists.

In many cases, the sole evidence adduced to support a suggestion of tapping is something like noises on the line, dead lines, interruption of calls or frequent wrong numbers and we know enough about the technical operation of the British telecommunications network to know that unfortunately all of these phenomena are capable of a purely straightforward explanation. In fact, we assume that any official agency tapping a telephone would ensure that reception on that line was reasonably clear and consistent. The other kind of evidence offered is warning, interrogatory or hostile voices on the line. However, we assume that most official tapping is too professional for interceptors to reveal their presence in the manner sometimes suggested.

Second, not withstanding our desire to avoid alarmism and paranoia, we do believe that there is some truth in the allegations that telephone tapping is used to monitor the legal actions of political and trade union activists. The problem for the individual subscriber is that it is virtually impossible for him actually to prove that his telephone is being tapped, but it is not so difficult for Post Office engineers on occasions to come across clear evidence.

We are convinced that the practice of official telephone tapping extends beyond those categories set out in the Government's White Paper

and includes political organisations and individuals as well as trade unions and trade unionists. However, we have no way of knowing the actual extent of such tapping or whether it is authorised by warrant or otherwise or not authorised at all. If warrants have been issued, we cannot imagine how such cases can be felt to be involved with criminal or espionage activities. On the other hand, if (as we think more likely) warrants are not involved, then this challenges the whole principle of effective control of official tapping by the Home Secretary.

Third, wherever the truth lies it will not be discovered under the prevailing blankets of suffocating secrecy. It cannot be in the overall best interests of the Police that they, who ultimately depend on public respect and support for their successful operation, should be suspected - no doubt often wrongly - of such invasion of privacy. Equally individuals who are disturbed about the possibility that their telephones are tapped are entitled to authoritative reassurance that this is not the case where it can reasonably be given.

Therefore, we believe a full enquiry is necessary with terms of reference which allow the investigation of particular cases and the opportunity for Post Office engineers and others to give evidence free of the threat of prosecution. Once that enquiry is complete and recent and current practices have been established, there needs to be a mechanism whereby in the future specific allegations can be properly investigated. We return to these themes at a later stage of the report.

HOW IS TAPPING CONDUCTED?

The Warrant Procedure

As far as telephone taps officially authorised by warrant are concerned, the procedure commences with a formal application to the Secretary of State.

The procedure is summarised in para. 9 of the White Paper:

> "Applications for warrants are sent by the police, by Customs and Excise and by the Security Service to the Home Office (the Scottish Home and Health Department for police and Customs and Excise warrants in Scotland). Applications are made in writing and must contain a statement of the purpose for which interception is requested and of the facts and circumstances which support the request. Every application is submitted to the Permanent Under-Secretary of State at the Home Office or the Secretary, Scottish Home and Health Department (or, in their absence, nominated deputies) who, if he is satisfied that the application meets the required criteria, submits it to the Secretary of State for approval and signature of a warrant. In a case of exceptional urgency, if the Secretary of State is not immediately available to sign a warrant he may be asked to give authority orally, by telephone; a warrant is signed and issued at the earliest possible time thereafter."

We know Home Secretaries to be honourable and hard working men who take their responsibility for interception of communications very seriously and examine applications for warrants most conscientiously. Nevertheless we find the existing procedures disturbing for four main reasons.

First, the Home Secretary has limited time. As well as examining individually each application for interception of communications, he has to consider individually all the more problematical immigration cases, all the most serious parole cases and all detention orders under the Prevention of Terrorism Act. On top of this, he has all his Departmental responsibilities, his Cabinet work, his Parliamentary duties and his constituency - case load. With the best will in the world (and we do not doubt that the will is there), it is impossible practically for one man to give the proper measure of scrutiny to an average of nine or ten applications a week.

Second, the Home Secretary has limited advice. On a matter such as the interception of communications, he will not consult more than a tiny handful of Home Office officials and he will not consult his Political Advisor, his Junior Ministers, his Cabinet colleagues or his Parliamentary Private Secretary or other MPs. Consequently, he is over-dependent on the information and advice supplied to him by his professional security advisors who, while obviously competent in their fields, have a limited political perspective and restricted practical knowledge of political and trade union activity.

Third, the Home Secretary does not have total control. Para. 10 of the White Paper admits that warrants may cover an organisation rather than an individual (although this seems contrary to the recommendation in para. 56 of the Birkett report) and that in some cases authority to change warrants may be delegated to the Permanent Under-Secretary of State. Furthermore, the Home Secretary has no control over tapping which may be authorised by the Prime Minister or the Secretary to the Cabinet or by the Foreign Secretary or the Defence Secretary (see "Inside Story", page 144). No Minister has control over official tapping which is performed without the need for a warrant.

Fourth, there is no Parliamentary accountability. The Home Secretary is exercising a power on behalf of the state, not himself, and, as with the exercise of any power by any Minister, a democratic society requires that there should be a measure of accountability to Parliament. The sensitive nature of this power is such that the accountability cannot be as open and detailed as in most other cases but the present absence of any accountability whatsoever is disturbing and unacceptable.

As well as telephone taps officially authorised by warrant, there is 'official' tapping which does not require a warrant. This derives from an 'institutional' relationship between the police (or CID and Special Branch) and the Post Office and the arrangement is set out in a Home Office circular of 1969 (cited by L H Leigh in "Police Powers In England And Wales", Page 215).

A senior official at Post Office Headquarters can authorise tapping in certain cases without the need for a warrant and it is understood that in 1978 15 police requests for interception concerning serious criminal cases were made and the information was provided in six cases. Additionally, in urgent cases local telephone managers have the authority to allow the police to listen in on calls.

How easy it is for the police to intercept calls without a warrant must be a matter for conjecture but, on page 161 of the (now unavailable) book "Operation Julie", the head of the operation, Inspector Dick Lee, explains how he avoided routine police channels and persuaded an unnamed organisation to tap a suspect's telephone.

How The Post Office Taps

Most official tapping - whether authorised by warrant or not - is carried out on behalf of the relevant agency by specially selected Post Office personnel. These personnel voluteer for the task and are drawn from grades represented by a number of trade unions (including of course the POEU). During their time on tapping duties, they are under the operational control of the Home Office.

These men are unknown to their other Post Office colleagues and operate out of their sight and in most cases without their support. The ordinary Post Office engineer has nothing whatsoever to do with telephone tapping and has the same mixed feelings about the practice as most members of the community.

The actual mechanics of telephone tapping cannot be described in detail, but most members of the public would be amazed and concerned by the range and sophistication of surveillance technology which now exists, although we hasten to add that most of the techniques are not used by the Post Office and only a tiny proportion of the population are actively at risk from the application of the techniques.

The essential point to grasp is that technically a telephone conversation can be intercepted at virtually any point in the link between subscriber and subscriber. (Optical fibre cable - which is now being introduced in small quantities in the British telecommunications network and is used in some military applications - cannot be tapped but, even with this, at some point the pulses of light have to be converted into electrical signals and at this point tapping is possible).

In practice, most parts of the transmission line plant would not be used for tapping purposes, since in many cases tapping circuits would present formidable technical and practical problems and interfering with a cabinet, pillar or distribution point in the local network would be too open to public view and too liable to discovery by Post Office engineers on normal duties. Therefore most tapping takes place in the local telephone exchange or in the customer's premises.

In the case of official tapping, virtually all of it is liable to be based on the exchange since, compared to a home or office, access is easy and detection is unlikely. It is likely that such official tapping is based on the main distribution frame (MDF) where each individual circuit is wired across by means of a jumper wire.

The main points to note about this procedure are that it is possible to gain easy access to the exchange outside normal hours and work in reasonable comfort with little chance of being observed, the basic technical operation is simple and quick, it is easy to pass the tap to the monitoring centre (which may be any distance away) via a trunk or junction circuit by the use of one jumper, no attention is drawn to an extra jumper since there are already so many, and there is little prospect of discovery by staff on conventional duties.

Other Surveillance Techniques

The techniques which can be used to intercept or overhear a telephone call or a conversation in the room of the telephone include the following:

(1) A conventional tap on a telephone line which may be a metallic contact or an induction device which picks up the pulses in the line - these draw an almost undetectable amount of electricity from the telephone wire and give no betraying noises.

(2) An 'infinity transmitter' which is a device inserted into a telephone handset which, when activated by dialling the number and giving an ultrasonic note on the last digit, prevents the telephone ringing and transmits over the dialler's line all the sounds in the room where the telephone is situated whether the handset is on or off the telephone - this can be installed in a matter of minutes.

(3) An induction device to pick up telephone conversations from the stray magnetic field of the telephone itself - this must be within about four feet of the telephone.

(4) A microphone using a wired link, the wired link either being specially laid or using an existing pair of wires or a single insulated wire - the range and sensitivity is unlimited depending on the size of the microphone.

(5) A microphone using a radio link with a transmitter - the sensitivity is great although the transmission range is limited.

(6) An electronic stethoscope of high amplification with wall-listening microphone and socket for connecting pin-hole microphones or the spike-mike for inserting into plaster walls - this requires access to adjoining walls.

(7) A directional microphone concentrating a beam of sound from a distance on to a sensitive microphone and so hearing across intervening noises - the range is only about 25 yards.

(8) Reflection of a laser beam off a window-pane or an object in a room to pick up the vibrations generated by the speaker - this is a recent development.

(Note: much of this information is taken from the Younger Report on Privacy, Cmnd. 5012, Page 155).

Many of these techniques are used by the police and the security service. No warrants are needed to employ bugs in a police investigation (in the Metropolitan Police, bugging is normally authorised by a Deputy Commissioner). Substantial use was made of bugging in the sieges at Spaghetti House, Balcombe Street and the Iranian Embassy.

Furthermore, most of these techniques are practised by those organisations and individuals concerned with industrial espionage or private investigation. The laws against their use are few and weak. There are only three laws in Britain that relate to private surveillance. They are the Wireless and Telegraph Acts 1949 and 1967 and the Theft Act 1968. The Wireless and Telegraph Acts make it necessary to have a licence for all radio transmitters and forbid listening to non-public broadcasts. Licences for radio transmitters are very rarely granted and there are an average of about 80 prosecutions a year under these Acts, but they are usually against pirate radios and hardly ever against those using bugs. Under the Theft Act, a person can be prosecuted for stealing electricity for the operation of a tap, but this is not a serious limitation on professional investigators and in any event the constraint can be avoided by using battery-powered bugs and other methods. Another serious problem is

that there is no registration or regulation of private security firms and investigators in this country.

The result is that private bugging and efforts at de-bugging are now big business. Equipment is easily available and last year an American company, Communication Control Systems, actually opened a London shop selling a wide variety of specialised devices. The shop is called Counterspy and is located at Park Street in Mayfair.

Besides these taps and bugs, all of which are operated as covert operations, there are a couple of other additional invasions of privacy of telephone communication which are practised (in the main quite properly) by the Post Office:

(1) Service observation - This involves the Post Office making random monitoring of calls to test the quality of service. It is understood that some 300,000 calls are monitored every week by 600 observers throughout the country and around 10,000 of these are said to be monitored from beginning to end ("New Statesman", 9th February 1979). Of course this practice is necessary to ensure good service but it is nevertheless an infringement of privacy.

(2) Meter Check Printer No. 2A - This is a device for recording on paper tape the number, destination and duration of any calls made from a particular telephone, although there is no record of the content of the calls. Its main use is to check the accuracy of telephone bills where the customer disputes them, but it has been used to obtain information to assist police enquiries (see "Operation Julie"). Estimates of the number of such meters range as high as 18,000 ("Rights", August 1978).

The Effect Of New Technology

All this demonstrates vividly that telephone conversations are open to many kinds of interception or surveillance and the advance of technology is ensuring that the threat is growing. Even the White Paper admitted that "one of the reasons for the present concern about interception is the fear that technological changes have made it easier to intercept telephones" (Para.25), yet it made no attempt to deal with the point.

One kind of technological advance that is relevant is the production of smaller, more sophisticated and (in some cases) cheaper and more obtainable bugs and other surveillance devices as a result of the development of micro-electronics.

Another development is computerised voice recognition. Duncan Campbell scared many people when he wrote:

> "The equipment at Ebury Bridge Road was designed by GCHQ, the government's code-and-cypher centre at Cheltenham. This has access to the latest US know-how, including computerised voice recognition techniques. According to one tapping centre employee, voice-recognition operations have reached an advanced stage - given the availability of good-quality lines - and by 1978 speech on many lines could be transcribed automatically and printed-out almost 'on demand'." ("New Statesman", 1st February 1980).

However, the consensus in the electronics industry is that this capability simply does not exist at present:

> "One British ex-army source, now doing consultancy work in narrow band communications and speech processing, said that none of the authorities with whom he had come into contact had even hinted that direct transcription was possible. He even cast doubt on the possibility of accurate voice identification which would be certain enough for the purposes described in the report" ("Electronics Weekly", 13th February 1980).

Nevertheless, the capability of automatic transcription of voice messages is certainly being developed:

> "Experts who dismissed the idea of an automatic machine which could transcribe phone calls were shaken this week when IBM revealed details of advanced work on natural language speech recognition. IBM researcher Fred Jelinek, head of the team at IBM's top laboratory in the US, described an automatic dictation machine which has already reached the point where it can transcribe the vast majority of English language words from continuously spoken input" ("Computing", 17th April 1980).

Still another important development - and much the most important in the sense that eventually it will affect all telephone subscribers - is the progressive introduction by the Post Office Telecommunications Business (and its successor British Telecommunications) of a new generation of switching equipment known as System X. The first System X exchange is due to open in July 1980 at Baynard House in London (this is a junction tandem exchange). Then the first local System X exchange will open at the end of the year at Woodbridge in Suffolk.

In May 1979, the POEU published a detailed review of the plans of the Post Office Telecommunications Business in a study entitled "The Modernisation Of Telecommunications". Pages 17-23 describe the exchange modernisation programme and the future deployment of System X. We explained then the nature of the system:

> "System X (TXD) is a family of new systems using microelectronic technology, integrated digital switching and transmission and stored programme (software) control. The system is designed to be modular, enabling each switching system to be assembled from a range of basic modules, and evolutionary, enabling continuous development and improvement".

Some concern - which we share - has been expressed about the enhanced capacity of a computer-controlled exchange like System X to monitor what should be private telephone communications.

Malcolm Peltu, former editor of "Computer Weekly", has written:

> "The new System X computerised telephone exchanges do not, a Post Office spokesman said last week, make telephone tapping any easier. This may be true in the sense that it is already easy enough to tap lines given the will (and, let's hope, the warrant). System X however, does increase the potential use, scope and efficiency of telecommunications surveillance and to deny this is to deny some

of the clever features of the system. One of the earliest services System X will provide to the public is the ability to bring more than two people into a conversation wherever they are located. If this is possible at the customer's request, the same capability could clearly bring a silent "mole" into a conversation. System X is essentially a computer controlled by software programs; it is a relatively easy matter to modify the software to provide comprehensive and detailed monitoring of the destination and duration of all calls" ("New Scientist", 24th April 1980).

Duncan Campbell has expressed similar views:

"A new generation of British telephone exchanges, known as 'System X', is about to come into service. This, if not regulated, can be turned into a tool of mass-surveillance far more readily than our present cumbersome electro-mechanical exchanges - and there is another shrouded department of the Post Office which appears to be working on just that project. In today's exchanges, large cables enter from the street, spray out onto distribution frames and are connected to long racks of switching equipment. Everything is highly visible, and comprehensible even to uninstructed eyes. Every aspect of System X's operation will be concealed inside miniature electronic devices. Its overall operations will be controlled by inaccessible computers, themselves subordinate to regional control centres. Complex facilities for channelling calls through exchanges will anyway be required, and adding a few programmes to monitor 'target' lines will be simple. No dangerously visible extra wires will be required to be attached during semi-clandestine visits: there will be no warning lights, and rather fewer people around each exchange to notice what may be going on" ("New Scientist", 1st February 1980).

This is a matter which the POEU has taken up with the Post Office. It has been admitted by the Post Office that stored programme control exchanges change the method by which the routing and control of calls is brought about and that it will be easier for individuals to gain access to customer lines from a remote point. However, we have been assured that access to control areas of software will be limited strictly by protection protocols. Nevertheless, it is obvious that official tappers would have access to these protocols.

We intend to press this matter further with Post Office management. Ultimately, however, it is not simply the POEU which must be assured but the general public and the kind of enquiry into telephone tapping which we have in mind would cover this issue.

THE CASE FOR AN ENQUIRY

The Omissions Of The White Paper

As the first stage of our case for a full enquiry into telephone tapping, we intend to establish the serious inadequacies of the White Paper, "The Interception Of Communications In Great Britain" (Cmnd.7873), and the statement to the House of Commons on 1st April 1980 and of the associated appointment of a judge to perform a monitoring role.

At a mere seven pages of text for a price of £1, the White Paper is hardly value for money. It adds little to the Birkett report and indeed on many occasions it simply repeats Birkett.

We believe that the White Paper contains three major areas of omission.

First, the White Paper omitted some of the basic statistics on the interception of communications:

a) Although it purports to bring up-to-date the Birkett report, the figures for the number of Home Secretary warrants for both telephones and letters in the year 1957 are inexplicably missing and the figures for the number of Secretary for State for Scotland warrants for both telephones and letters for the entire period 1957-66 are missing as well (this omission is noted but not explained).

b) Even when figures are given, it is not made clear whether the number of interception warrants is cumulative or not. This particular point was picked up by Clement Freud after the Commons statement when he asked: "... whether the number of interception orders listed in the White Paper are cumulative - that is to say, those currently in force - or is the number given simply that of the new orders that have been published?" ("Official Report", 1st April 1980, Col.212). But the Home Secretary did not deal with the question.

c) Although Birkett broke down the figures for each year into the two broad categories Police, Customs, Post Office and Security on the one hand and drugs, lotteries, and obscene publications on the other, there is no break-down whatsoever in the recent White Paper. Again this point was picked up by Clement Freud after the Commons statement when he asked: "Will he consider subdividing the number of interceptions into those instigated by the Police, those by Customs and Excise officials and those by the security forces?" ("Official Report", 1st April 1980, Col.212). But pointedly the Home Secretary did not answer this question either.

d) Even when some kind of statistical analysis is given, it is suspect. Para. 22 of the White Paper suggests that interception of communications led to the seizure or played an essential part in the case of 62% of the heroin and 56% of the cocaine seized in 1978. However, David Clark has written that, "the claim....is demonstrably untrue" since "as far as heroin seizures are concerned Mr. Whitelaw was talking nonsense" ("New Statesman", 2nd May 1980). Apparently in 1978 Customs had an all-time one-off record seizure of a large consignment of heroin following vigilance by Customs Officers.

Second, the White Paper omitted any substantive reference to Northern Ireland. This omission was understandable if regrettable in the case of the Birkett report, since in 1957 Northern Ireland had its own Government and Parliament, but since 1972 Northern Ireland has been governed by direct rule from Whitehall and Westminster. Commenting on the omission of Northern Ireland from the White Paper, the previous Home Secretary, Merlyn Rees, said: "I believe that it would be the height of folly to give numbers of any kind about Northern Ireland - much as I am assured of them - because terrorism is established in Northern Ireland in a way that we do not experience in the rest of the United Kingdom." ("Official Report", 1st April 1980, Col.209-210). However, on the same occasion, James Kilfedder, a Northern Ireland MP noted for his anti-terrorism views, stated:

> "Because of the evil terrorist campaign that has been waged in Northern Ireland for the past 10 years or more, it is naturally assumed that a far greater number of telephone tappings will take place in the Province in proportion to the rest of the United Kingdom, but that does not justify the Home Secretary's refusal to give the figures. Is the right hon.Gentleman aware that his refusal to do so and his refusal to extend judicial monitoring to Ulster, will create greater concern in Northern Ireland where many believe that phone tapping, conducted by the Army, takes place and extends to those who are not engaged in criminal or terrorist activities?" ("Official Report", 1st April 1980, Col. 218).

In these circumstances, the situation in Northern Ireland must be reviewed. Certainly the POEU's Union Regional Council for Northern Ireland has expressed particular concern that the ordinary Post Office engineer be cleared of any involvement in the practice of tapping telephones on behalf of the Army or the Police.

Third, the White Paper omitted any reference to surveillance of communications conducted by official organisations other than the Police, Customs and Excise and the Security Services. Principal among these is Government Communications Headquarters (GCHQ). According to Duncan Campbell, GCHQ designed the Post Office tapping centre in Chelsea, provided much of the Centre's equipment and receives much of its intelligence ("New Stateman", 1st February 1980) and GCHQ or the Americans' National Security Agency (NSA) intercept on a routine basis much international telecommunications traffic, that is radio, telegrams, telex and telephone ("New Statesman", 2nd February 1979). However, other agencies believed to be involved in tapping but not covered by the White Paper include the Foreign Office (that is, Military or Defence Intelligence 6) and the Ministry of Defence (that is, Service Intelligence).

Reservations About The Proposed Monitoring

Associated with the publication of the White Paper came the announcement of the intention to appoint a "senior member of the judiciary" with the following terms of reference:

> "To review on a continuing basis the purposes, procedures, conditions and safeguards governing the interception of communications on behalf of the Police, H.M. Customs and Excise and the Security Service as set out in Cmnd Paper 7873; and to report to the Prime Minister." ("Official Report", 1st April 1980, Col.208).

Subsequently, Lord Diplock was appointed to the position.

We do not regard the appointment of a judge on the basis announced as anything like an adequate safeguard in the circumstances. We have five main reservations.

First, Lord Diplock is an able and distinguished judge,but a man of 73 who has been Chairman of the Security Commission for nine years cannot be seen to have the required measure of independence from the Home Office and the Security Services to perform the task to the evident satisfaction of Parliament, the press and the public.

Second, it would appear that the judge will not have the power to investigate the detailed circumstances of particular cases and in any event it it difficult to see how such a senior member of the judiciary will have the time to monitor in sufficient detail the operation of a system of telephone tapping said officially to involve some 400-500 warrants a year (or an average of around ten a week).

Third, the judge's terms of reference only cover interceptions authorised on the warrant of the Home Secretary and the Secretary of State for Scotland and do not include interceptions authorised by other Secretaries of State (particularly the one for Northern Ireland) or interception by State agencies which have not received express authorisation (such as GCHQ).

Fourth, although the judge's first report will be published, his subsequent reports will be secret with Parliament being informed only of the findings of a general nature or of any changes in arrangements, so that secrecy will continue to prevail.

Fifth, there is no involvement of Parliament in the monitoring process (beyond being the recipient of occasional statements at the absolute discretion of the Home Secretary) and therefore there is still no real political accountability over what is essentially an exercise of political judgement by the Home Secretary.

Reasons For An Enquiry

It is because of these serious omissions in the Government's White Paper and the grave reservations over the announced role of the judge that we must press our case for a full enquiry. We believe that there are four main reasons why a fresh enquiry is vitally necessary 23 years after the Birkett report.

First, the level of telephone tapping has increased significantly as evidenced by the Government's own statistics in its White Paper. The Home Secretary has said that there has simply been a "modest overall increase" ("Official Report", 1st April 1980, Col.206). However, the increase in warrants for telephone tapping in England, Wales and Scotland from 1958-75 was from 129 to 468, a rise of some 260% although the figures have fallen a little in recent years.

Second, there have been many changes in technology over the past quarter of a century and many believe that current and coming technology makes telephone tapping easier and less detectable and therefore its abuse more likely. The

principle changes are on the one hand the introduction of semi-electronic exchanges (TXE2, TXE4 and TXE4A) followed by fully electronic exchanges using stored programme control (System X) and on the other hand the use of micro-electronics to produce small and sophisticated bugging and surveillance devices.

Third, there is an urgent need to review practice concerning all forms of interception of communications, whether authorised or unauthorised, whether using tapping techniques or not. In 1957 the Birkett report devoted a mere 108 words to the subject of unauthorised tapping and wrote something which could never be said today: "All the evidence we heard was to the effect that there is, and has been, no tapping of telephones by unauthorised persons in this country" (Para.129). In 1972, Chapter 19 of the Younger report on Privacy (Cmnd.5012) dealt with some aspects of the problem but it was a partial study and one now somewhat out-dated technologically.

Fourth, there is growing public concern about the extent of the interception of communications by various agencies in various forms and the community is entitled to have its anxiety taken seriously and answered comprehensively. As Patrick Gordon Walker noted in his reservation to the Birkett report, "One of the factors determining the evolution of policy in regard to the interception of communications has been the state of public opinion towards the exercise of this power" (Para.173). He went on to argue that: "Public repugnance to the interception of communications has,it seems to me, increased and there should therefore be a further restriction upon the use of this power....." (Para.174). Demonstrably, this is even more true today than it was 23 years ago.

We believe that individually these arguments are persuasive and that collectively they are compelling.

Form Of The Enquiry

We believe that we have identified major weaknesses in the current position of the Government on the interception of communications and that we have advanced powerful arguments as to the need for a new enquiry. We turn now to the kind of enquiry which we have in mind.

It must not simply be 'another Birkett'. The terms of reference of the Birkett Committee centred on "the exercise by the Secretary of State of the executive power to intercept communications" (Para.1). The Committee was not required to look at interception other than that authorised by warrant and it was not asked to consider the situation in Northern Ireland. We want to see an enquiry into all forms of interception of communications throughout the United Kingdom, that is whether authorised by warrant or not, whether conducted by State agencies or private organisations and individuals, whether involving actual tapping or other forms of surveillance.

The composition of such an enquiry is a delicate matter. Clearly the subject material of the enquiry will be one of great sensitivity: the Committee will need to look at the operational practices of the Police, Customs and Excise and the Security Services and it will need to inform itself of the technical details of the public telecommunications network and of available surveillance equipment. Therefore, though we would have liked a broad based Committee, we feel that the Committee should consist exclusively of Privy Councillors (like the Birkett Committee), although we feel strongly that the Committee should use professional advisors (who should be positively vetted) for advice on the operation of the Security Services and the nature of telecommunications technology.

The conduct of the enquiry is another difficult matter. To an extent, it is probably best left to the Committee of enquiry itself, but we would hope that the Government or Parliament in establishing the enquiry would indicate its strongly felt wish that, consistent with the needs of national security, as much as possible of the hearings of the enquiry should be in public and as much as possible of the evidence should be published or reflected in the text of the published report.

PROPOSALS TO BE PUT TO THE ENQUIRY

Proposals On Interception Of Communications

There are no easy answers to the serious problems which we have described in this report. Striking the correct balance between the needs of national security and the right to individual privacy is an onerous and difficult task. It will be for the enquiry which we have advocated to recommend detailed proposals, but we feel that we should conclude our report by outlining the broad principles which we believe should constitute a more acceptable framework for telephone tapping in this country.

First, there must be legislation to provide an express legal authority for the official interception of communications. We accept the need for mail to be opened and telephones to be tapped on limited occasions by specified authorities. We feel sure that most competent professional criminals and spies will be too cautious and clever to write letters or make telephone calls revealing details of their criminal activities or espionage but nevertheless, if authorised tapping was not allowed, it could only encourage the wrongdoer. However, we believe that the present lack of an express legal provision for official interception which we have described is unacceptable in a democratic society and a breach of the terms of the European Convention on Human Rights by which the United Kingdom is formally bound.

In the Parliamentary session 1980/81, there will be a major Bill on the Post Office and the opportunity could be taken to use this Bill to amend the relevant parts of previous Post Office Bills (such as Section 58 of the Post Office Act 1953) to provide the express legal authority which we are seeking. It is a 'once in a decade or so' chance and, if the Government does not take it, then MPs should move the necessary amendments at Committee Stage.

Second, there should be stricter criteria for the issue of warrants for the interception of communications and the criteria should be specified in the legislation. In the case of warrants requested by the police, we have expressed our doubts about whether the definition of "serious crime" is sufficiently demanding and our special concern about the inclusion of "offences of lesser gravity". In the case of warrants requested by the security service, we have expressed our particular anxiety about the meaning of "subversive".

In 1957, Patrick Gordon Walker produced a reservation to the Birkett Report in which he argued that "the purposes for which warrants are issued should in future be judged by new and stricter standards" (Para. 170). His reservation was not accepted by the Government of the day or indeed subsequent Governments and, since the Birkett Report, the criteria used have been widened rather than narrowed. Although we would not support the precise formulations advocated by Mr Gordon Walker, we believe that his general approach was much more in accord with public feeling then and even more so now.

Third, there needs to be an independent check upon the judgement of the Home Secretary in deciding upon applications for a warrant or alternatively, the decisions should be taken elsewhere. We have described the reasons why we are so disturbed by the present dependence for the

operation of the system ultimately on one man and some alternative solutions are possible.

One could require the Home Secretary to justify his decisions to independent persons. For instance, in West Germany the Minister's actions are supervised by a board of five Parliamentarians appointed by the Bundestag and in the USA the Attorney General has to convince a seven man secret court. Alternatively, one could place the responsibility for authorising warrants in the hands of magistrates or, more likely, a High Court judge.

Fourth, there should be annual published reports to Parliament detailing the numbers of interceptions authorised in the previous year and commenting on the effectiveness of the interceptions and any changes in policy or procedure. We believe that the present lack of any meaningful kind of political accountability for the interception of communications is fundamentally wrong and that the minimum requirement is that all MPs know the broad picture as it unfolds from year to year.

Of course, it will be argued that publication of these statistics would undermine the effectiveness of the operation, but that argument was undermined by the publication of figures by the Birkett Committee and it was abolished by the publication of figures by the present Home Secretary. We agree with the Sunday leader writer who wrote:

> "The benefits of fuller disclosure, including annual details of numbers and categories of taps, far outweigh the disadvantages that additional publicity would bring" ("Observer", 4th March 1979).

Fifth, there should be a requirement to notify a person whose mail has been opened or whose telephone conversation has been intercepted once doing so would not assist criminal activity or weaken national security. In West Germany, victims of official surveillance must be notified once it has been terminated (unless this would jeopardise future operations) and they then have the right to challenge the legality of the surveillance in criminal proceedings and to bring actions for damages. In the USA, in some circumstances citizens can discover whether their communications have been intercepted by the careful use of the Privacy Act 1974.

Such a requirement would act as a major discipline on the exercise of the power of interception, so that the innocent would be better protected. On the other hand, the information that their communications have been intercepted would act as a powerful deterrent to many criminals and spies.

Sixth, there should be an opportunity for any person suspecting the interception of his mail or telephone conversations to have his suspicions investigated and confirmed or denied. In West Germany, anyone who suspects that he is a victim of unlawful surveillance can apply to the constitutional court that is empowered to investigate his complaint. We could apply a similar approach to this country.

Of course it will be argued that this would assist criminals or spies but it is difficult to see how this would be the case in practice. If the response was confirmation of interception, this would not frustrate further the objectives of interception since the subject already suspected interception and presumably modified his behaviour accordingly. If the response was denial, this would carry no guarantee that there would not be

interception in the future and anyone suitable for interception would have drawn attention to this fact by making the original approach.

We recognise that these six proposals represent a radical departure from current procedure and practice, but we believe sincerely that they can be brought into effect without damage to the nation's security or assistance to criminals in our society. It is clear that we can learn by studying the situation on the interception of communications in other democracies. The United States must be the scene of more serious espionage activity and large-scale crime than any country in the western world and West Germany has the combined threat of East German agents and political terrorists, yet both these countries manage to operate more enlightened and liberal systems than our own.

While we believe that our proposals do not undermine the effectiveness of the proper operations of the police and the security service, we accept that neither do they assist directly such effectiveness (except in so far as they enhance public support for the agencies so aiding indirectly their work). However, if the safeguards which we have proposed were introduced, then we would accept a reconsideration of the traditional practice whereby the results of interceptions of communications are never used in evidence by the prosecution in criminal proceedings. Such material is admissable in law and on many occasions would assist conviction of the guilty.

Other Related Proposals

Our review of the threats to the privacy of telephone calls has identified problems much wider than those associated with the interception of communications by the Home Secretary. There are the difficulties associated with tapping and bugging by private investigators who have ready access to sophisticated devices and whose activities are hardly circumscribed at all by the present law.

It is not as if these problems have not been recognised and publicised before. Almost a decade ago now, the Younger Committee on Privacy examined the area and made a series of recommendations on which no Government has acted. We take this opportunity to declare our support for, and our wish that the Government will legislate on, the relevant recommendations in the Younger Report, especially:

- Control over the type of person engaging in private detective work should be secured by a system of licencing aimed simply at excluding persons known to be unsuitable and infringement of the conditions should involve the withdrawal of a licence with criminal penalties for pursuing the work unlicenced. (Paras. 451-454).

- It should be unlawful to use an electronic or optical device for the purpose of rendering ineffective, as protection against being overheard or observed, circumstances in which, were it not for the use of the device another person would be justified in believing that he had protected himself from surveillance whether by overhearing or observation. (Para. 560).

- Unlawful surveillance by device should, where it is done surreptitiously, be an offence punishable by imprisonment or fine and triable both summarily and on indictment. (Paras. 562-563).

- There should be a new tort of unlawful surveillance by device for which damages can be awarded as for other torts or orders for an injunction can be made. (Para. 565).

Two further requirements are necessary to tackle comprehensively the disturbing situation which we have detailed in this report. We need a reduction in secrecy and an extension of human rights in our society.

Less secrecy, especially as it affects discussion of the interception of communications and related issues, requires a fundamental revision of the Official Secrets Act and the enactment of a Freedom Of Information Act (proposals which the POEU advocated in a memorandum to the Home Secretary on 9th October 1979), review of the D-notice system and especially the D-notices 10 and 11 (a review which in fact the Commons Select Committee on Defence has initiated), a new willingness by the Prime Minister and the Home Secretary to answer Parlimentary Questions on aspects of official and unlawful interception of communications, and a more relaxed approach to public discussion of the role of the police and the security and secret services in a modern democratic society.

An extension of human rights would be assisted by the implementation of the previously mentioned Younger Committee recommendations on technical surveillance devices, but technology changes so fast that specific legislative provisions will never be adequate, so additionally we need to create a general statutory right of privacy (as recommended in the two Minority Reports to the Younger Report) and to incorporate into our domestic law the provisions of the European Convention on Human Rights (so providing Britain with a kind of Bill of Rights which is enforceable in our own courts but recognises the ultimate sovereignty of Parliament).

CONCLUSION : A CASE TO BE ANSWERED

We do not claim that this report contains anything particularly revelational or new. However, we do believe that it represents one of the fullest and most considered public statements on telephone tapping since the Birkett Report of 23 years ago. Furthermore, we hope that the special professional position of the POEU entitles us to command the interest and attention of politicians and public on this controversial subject. For these reasons, we hope that this report will be read widely and that the arguments that it advances will prove persuasive.

The report will be used within the POEU as a basis for further discussion on telephone tapping. It is being issued to the press and it is being made available for purchase by members of the general public.

The report is being submitted to:

- The Home Secretary as a response to his White Paper "The Interception Of Communications In Great Britain"
- Members of Parliament as part of our campaign for the holding of a full enquiry
- The Labour Party as evidence for its Study Group on the Security Services
- The Socialist Group of the European Parliament which is investigating telephone tapping in EEC countries.

We invite POEU Branches and all other concerned organisations and individuals to support the POEU's call for a full enquiry into telephone tapping by writing to their local Member of Parliament and to:

Rt. Hon. William Whitelaw MP,
Home Secretary,
Home Office,
50 Queen Anne's Gate,
LONDON.
SW1H 9AT

ANNEX A

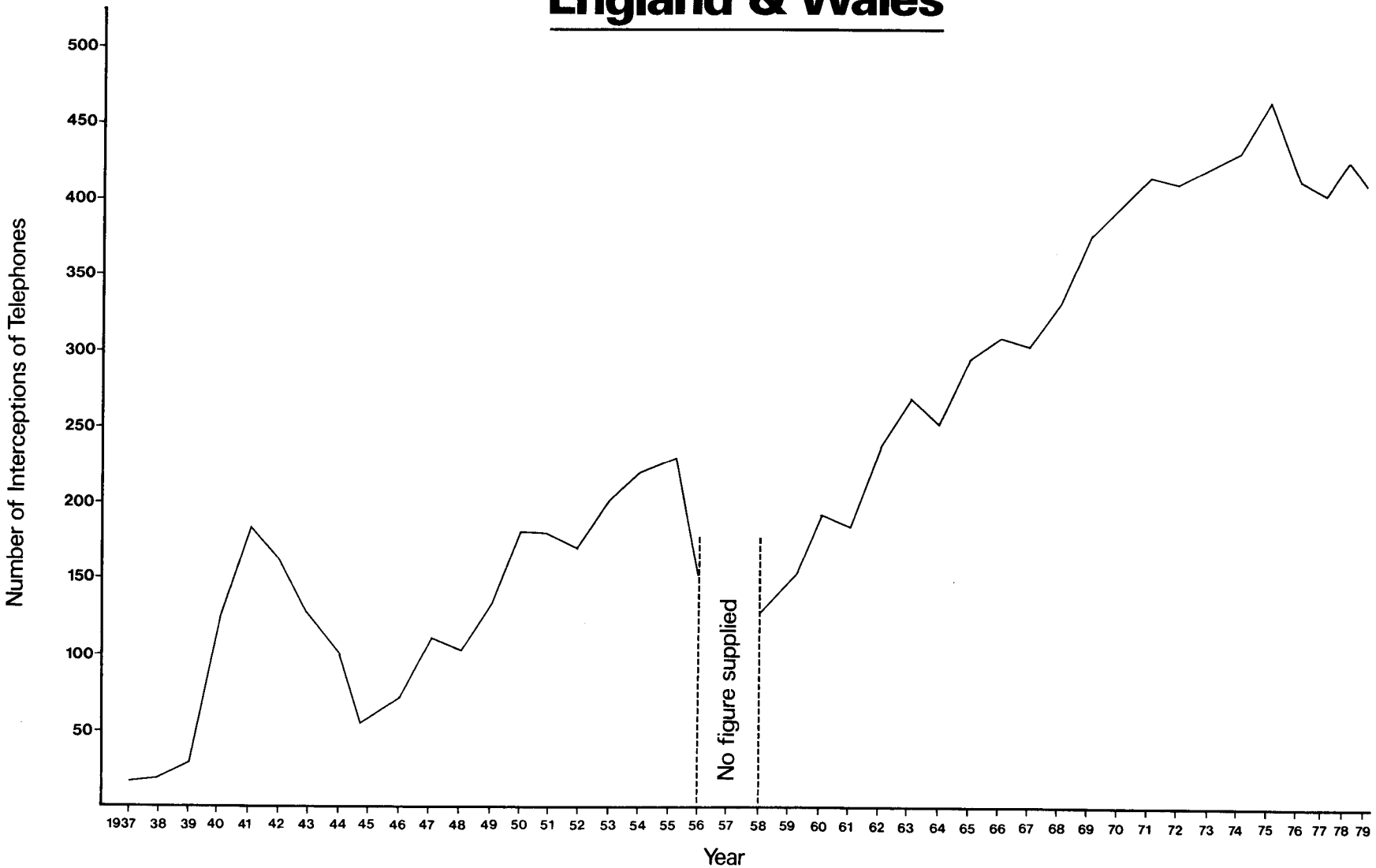
TELEPHONE AND LETTER INTERCEPTIONS IN ENGLAND & WALES

YEAR	TELEPHONES	LETTERS	TOTAL
1937	17	556	573
1938	20	710	730
1939	29	973	1002
1940	125	1557	1682
1941	180	862	1042
1942	164	514	678
1943	126	329	455
1944	102	213	315
1945	56	90	146
1946	73	139	212
1947	110	190	300
1948	103	870	973
1949	133	641	774
1950	179	356	535
1951	177	486	663
1952	173	462	635
1953	202	459	661
1954	222	227	449
1955	241	205	446
1956	159	183	342
1957	N/A	N/A	N/A
1958	129	109	238
1959	159	101	260
1960	195	110	305
1961	183	75	258
1962	242	96	338
1963	270	128	398
1964	253	120	373
1965	299	93	392 *
1966	318	139	457
1967	307	92	399
1968	333	83	416
1969	377	93	470
1970	395	104	499
1971	418	86	504
1972	413	95	508
1973	424	73	497
1974	436	93	529
1975	468	93	561
1976	410	62	472
1977	407	84	491
1978	428	44	472
1979	411	52	463

* This figure is wrongly given as 382 in Cmnd. 7873

ANNEX B

England & Wales

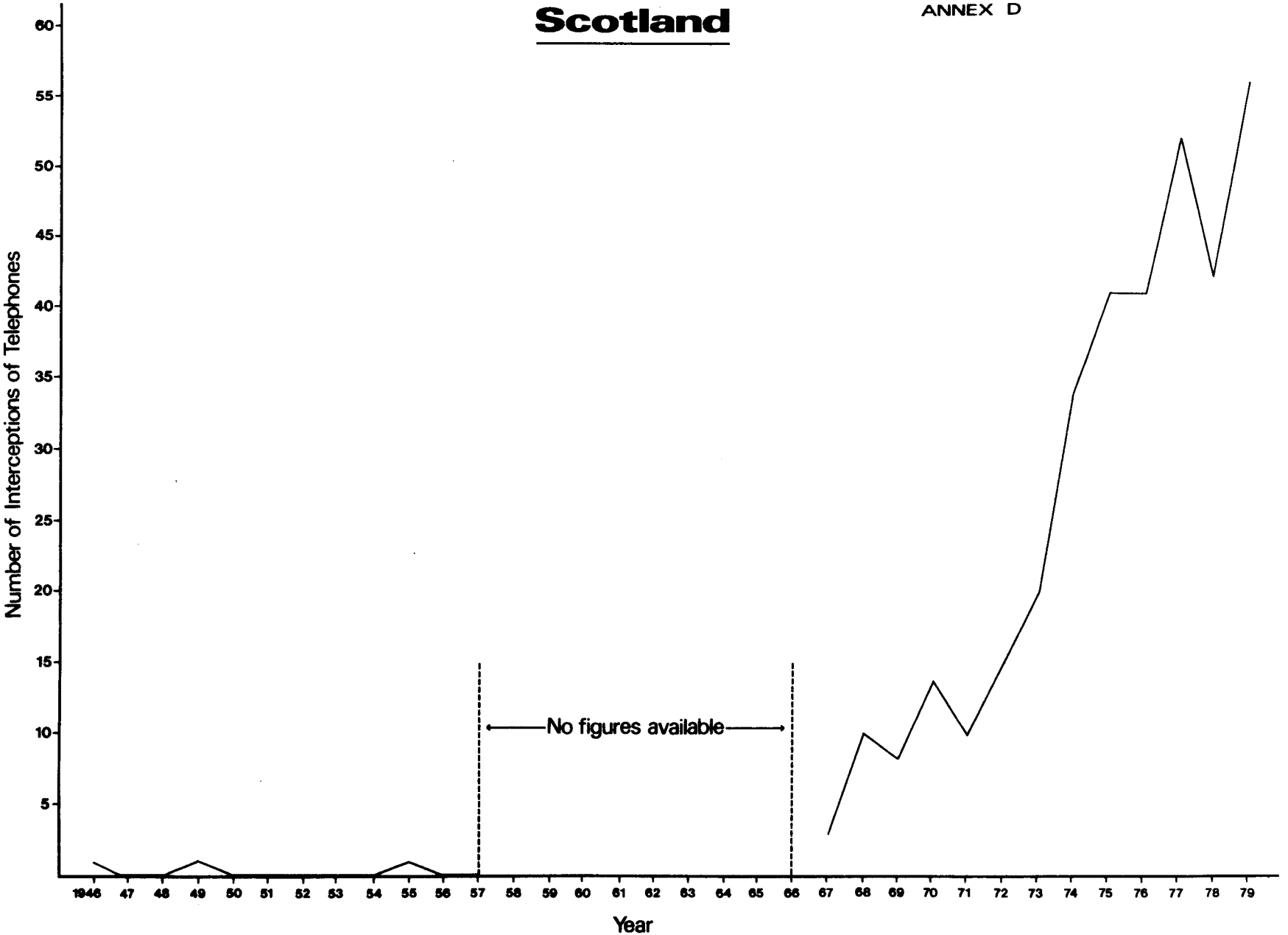


ANNEX C

TELEPHONE AND LETTER INTERCEPTIONS IN SCOTLAND

YEAR	TELEPHONES	LETTERS	TOTAL
1946	1	0	1
1947	0	22	22
1948	0	9	9
1949	1	3	4
1950	0	4	4
1951	0	6	6
1952	0	7	7
1953	0	0	0
1954	0	0	0
1955	1	0	1
1956	0	0	0
1957	N/A	N/A	N/A
1958	N/A	N/A	N/A
1959	N/A	N/A	N/A
1960	N/A	N/A	N/A
1961	N/A	N/A	N/A
1962	N/A	N/A	N/A
1963	N/A	N/A	N/A
1964	N/A	N/A	N/A
1965	N/A	N/A	N/A
1966	N/A	N/A	N/A
1967	3	0	3
1968	10	0	10
1969	8	0	8
1970	14	0	14
1971	10	2	12
1972	15	0	15
1973	20	0	20
1974	33	5	38
1975	41	0	41
1976	41	0	41
1977	52	3	55
1978	42	0	42
1979	56	0	56

ANNEX D


Scotland
Number of Interceptions of Telephones
60
55
50
45
40
35
30
25
20
15
10
5
No figures available
1946 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79
Year

Other Publications

Two other publications are available from:

Post Office Engineering Union,
150 Brunswick Road,
London W5 1AW

These are:

* "The Modernisation Of Telecommunications" (£1 plus 25p p&p) - this describes the whole modernisation programme of the Post Office Telecommunications Business over the next decade and assesses the impact on POEU members (there are special annexes on electronic mail, electronic funds transfer, the electronic office and the electronic home).

* "Optical Fibre Technology" (£1 post free) - this describes what optical fibre is and what it does and sets out details of its use in the British telecommunications network and elsewhere.

