LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Response by Liberty to Home Office consultation paper: *Interception of Communications in the United Kingdom*

Response by Liberty to Home Office consultation paper: *Interception of Communications in the United Kingdom*

Contents

Response by Liberty to Home Office consultation paper: *Interception of Communications in the United Kingdom*

1 Introduction

This is Liberty's response to the Home Office consultation paper, "Interception of Communications in the United Kingdom", Cm 4368,issued on 22 June 1999.[1]

Liberty has a long-standing interest in interception of communications. Policy-making and executive practice in this area, as with other aspects of clandestine intelligence-gathering and investigation, tends to involve a sharp clash between the rights of the citizen and the perceived interests of the wider community. The legislator faces the difficult task of striking the proper balance in a democracy between, on the one side, the legitimate aim of protecting society from genuine threats to its integrity and, on the other, the need to preserve the very values - the rule of law, respect for individual liberty, abhorrence of arbitrary or unjustified official interference with citizens' rights - that make a democratic society worth protecting.

The inevitably secretive nature of interception amplifies the risk of abuse of citizens' rights and is a key reason why all the greater care is needed to ensure that law-making is informed, above all, by a principled approach to the balancing exercise.

For that reason this response, as well as addressing the detail of the Government's present proposals, explains as a matter of principle - in particular from the standpoint of the legal principles developed under the European Convention on Human Rights, about to become binding on our domestic institutions as a result of the Human Rights Act 1998 - the approach which we consider appropriate in formulating legal rules about interception.

This response contains practical proposals which we think Government and Parliament will find helpful in enabling the right balance to be struck. They are practical not least because the implementation of the Human Rights Act is set to lead to a profound shift in the culture of legal and constitutional thought over the next few years. Practices which the public and, significantly, the judiciary have so far tolerated, or considered themselves powerless to censure, are likely increasingly to be recognised as unacceptable in a modern democracy.

The existing matrix of legislation dealing with interception and related forms of surveillance - the Interception of Communications Act 1985 ("IOCA"), the Security Service Act 1989 (as amended), the Intelligence Services Act 1994 and the Police Act 1997 - came into being under a Government with deeply illiberal instincts. The proposals which gave rise to that legislation were rightly criticised in numerous respects by the Labour and Liberal Democrat opposition and were the subject of many attempts at amendment. We would invite this Government to take the opportunity of new legislation to revisit and reform the existing flawed regime for interception and related practices.

We hope that the case made in this response will be accepted as a contribution to the important process of ensuring that this sensitive part of the statute book retains its effectiveness while acquiring - and keeping - a clean bill of health, in the eyes of public opinion and the courts, once the Human Rights Act is in force.

---

[1] Liberty would like to thank Gordon Nardell for his assistance in the preparation of this submission.

2 General observations

The contemporary legislation in this area was prompted in part by litigation at Strasbourg which revealed the failure of traditional British constitutional thinking to meet modern standards of protection of civil liberties. Placing on a statutory footing executive activity which was previously "lawful" in domestic law only because of the absence of legal rules expressly prohibiting it was to that extent a step forward.

But the principle that, where civil liberties are concerned, the executive must point to a law positively entitling it to act provides only a threshold of legitimacy. More important is the balance struck by the substantive content of that law. Civil liberties in the United Kingdom have traditionally been "residual" - whatever remains after the law's restrictions have run their course. But in every legal system which embraces the express protection of human rights, it is axiomatic that the starting point is not restrictions but rights: it is for the state to demonstrate not only that a particular restriction on rights pursues a legitimate aim, but that it is necessary, reasonable and proportionate in all the circumstances.

We freely accept that the existing legislation and the proposals pursue aims that are capable of providing legitimate reasons for interfering with citizens' privacy interests. A society free from major threats to public safety and well-being is essential for the exercise of fundamental rights and freedoms. But we consider that the extent and nature of the interference allowed under the present framework reflects a philosophy that regards the demands of administrative convenience and expediency as paramount and grudgingly tempers them with few and inadequate gestures towards rights.

Liberty's core concerns about the scheme of IOCA and the legislation modelled on it are well-known. The criteria for authorising interception are objectionably vague and overbroad. The absence of prior judicial sanction, coupled with the restrained and secretive machinery for supervision and complaints handling, means that the legislation fails to offer the safeguards necessary to ensure that intrusion into the field of individual rights is, and is seen to be, strictly proportionate to the legitimate needs of the agencies concerned.

The mere fact that the context is one of combatting serious social evils does not in itself justify derogation from the principle that the law should allow interference with citizens' rights only to the extent demonstrably necessary to attain its purpose. Indeed, the more serious the subject-matter of an allegation or suspicion against the subject, the greater the need for effective safeguards to prevent abuse. Though the need for operational secrecy presents practical difficulties, it also amplifies the risk of improper or excessive interference. The challenge for the legislator is to devise ways of dealing with these problems that impinge on accepted standards of protection of rights as little as possible.

We welcome the shift in philosophy already apparent in Government proposals in parallel areas. The draft Electronic Communications Bill ("ECB"), for example, partially restores to the supervision of clandestine surveillance some of the judicial qualities lacking from the Tribunal system established by IOCA. The shift is modest, and we consider it should go much further (see below). But it is a step in the right direction which we hope the Government will build upon in its review of interception legislation.

3 Scope: subject-matter of proposed powers

This heading deals with points appearing in Chapters 3, 4, 5 and 10 of the Consultation Paper.

3.1 General

Liberty has no objection in principle to extension of the interception regime to new technologies and practices (paras. 3.4-3.14; see also the *private systems* and *communications data* sub-headings below). The corollary to that is the importance of recognising that interception of these methods of communication raises issues of civil liberty just as compellingly as more traditional activity such as

tapping of fixed public telephone lines and opening of items carried by the Post Office. The European Court of Human Rights recognises the Convention as a "living instrument", moving with the times in the protection it offers. We are pleased to see that this much is accepted by the Government (Consultation Paper, para. 4.5).

3.2 Private systems

Paras. 3.8, 3.9 and 4.6 of the Consultation Paper address this area. We agree that where a state agency seeks to intercept a communication, the question whether the network is technically "public" or "private" at the point of interception should make no difference to the content of the law regulating that activity.

However, there is a difficulty in relation to interception by employers. That is because the Human Rights Act binds every public authority (s. 6). Bodies which are "obvious" public authorities are bound to respect Article 8 in all their activities, including their relations with employees. Other bodies may qualify as public authorities for some purposes, and depending on the circumstances may or may not act as public authorities in the course of their employment relations (s. 6(3)(b) and (5)). Where a body is bound by the Act in its capacity as employer, we consider that Article 8 is likely to subject it to requirements comparable to those applicable to a state agency.

Hence where an employee has a reasonable expectation of privacy in making communications (which will be a question of fact), a public authority employer risks violating Article 8 unless the interception is expressly permitted by law and is proportionate.

We regard that as right in principle. While legitimate business purposes may form legitimate aims for interception, continuous or indiscriminate monitoring and absence of proper safeguards would be disproportionate. Parliament's enactment of the Public Interest Disclosure Act is just one illustration of the vital role that confidential communications by employees can play.

Even in relation to an employer which is not regarded as a public authority, it is implicit in the *Halford* judgment that the UK may, as part of the notion of "respect" in Article 8(1), be under a positive obligation to provide protection against routine or unregulated monitoring. So the courts themselves may in future impose on private employers much the same duties in relation to monitoring as public sector employers will owe directly under Article 8.

We consider that legislation should therefore provide a framework for protection of employees' communications over private systems, without technical distinctions based on the "public" or "private" status of the employer.

3.3 Communications data

As part of its "living instrument" approach, the European Court has developed the scope of the activity caught by Article 8 well beyond the confines of physically intrusive surveillance and direct interception of communications. Any clandestine gathering and retention by the state of information about the individual's activities and private relations with others raises issues of "private life", as does the exercise of compulsory powers in relation to transaction records and other personal documents.

It follows that it is mistaken to suggest that access to data represents a "lower level" of intrusion than interception (Consultation Paper, paras. 10.1, 10.2). It is hard to see any cogent basis for distinguishing in principle between (say) the bank statements seized in the *Funke* case and itemised billing information obtained without the subject's knowledge under the powers proposed in Chapter 10. The state's obtaining access to these private transactions raises the concerns, and the need for strong safeguards, forcefully expressed by Browne-Wilkinson in *Marcel*. The European Court in *Malone* found a violation of Article 8 in relation to telephone metering data as well as interception proper.

We therefore urge the Government to accept that the grounds on which access to this material may be sought, and the authorisation and supervision procedures applicable, should be no less strict than those we propose (see below) in relation to interception proper. Those safeguards are additional to the data protection principles, which rightly apply to the use and disposition of the information obtained (Consultation Paper, para. 10.7).

3.4 The position of Communication Service Providers

We are troubled by the proposal that CSPs should be compelled to take reasonable steps to ensure that their system is capable of being intercepted if this prevents the development of more secure and private communications.

The specific question of what would be "reasonable" assistance in an interception case should be open for consideration by the Tribunal on an application by the CSP. It would be wholly wrong for the executive to have the last word. The warrant should expressly indicate the CSP's right to apply to the Tribunal.

It would be unsatisfactory for OFTEL to have an adjudicating role, as apparently proposed at para. 5.6 of the Consultation Paper. OFTEL is a body in the nature of a non-ministerial government department. It signally lacks the independence needed in this context.

4 Scope: grounds for interception

The present proposal is for no change to the purposes, set out in IOCA s. 2(2), for which interception warrants may be granted. They are:

(i) the interests of national security,
(ii) preventing or detecting serious crime, and
(iii) safeguarding the economic well-being of the UK.

We have serious concerns about the inclusion of heads (i) and (iii) and about the definition of "serious crime" in head (ii).

4.1 National security and economic well-being

These are extraordinarily vague concepts. Neither is defined in IOCA. The cumulation of these categories with "serious crime" indicates that Parliament intended them to include activity which does not constitute serious crime (or indeed any crime at all: it is difficult to think of activity that is capable of threatening the security or economic well-being of the nation as *not* "serious").

We consider that in the overwhelming majority of cases, "serious crime" will be the only necessary and defensible category in which to place activity of a kind judged so menacing to society as to justify interference with fundamental rights of the citizen. In the field of national security, a range of crimes of espionage, terrorism and conspiracy cover an enormous range of harmful conduct. In the field of "economic well-being" offences covering fraud, evasion of fiscal and customs regulation, insider dealing, false accounting, counterfeiting and so forth prohibit an equally broad range of objectionable activity. If Parliament has not judged an activity sufficiently grave or insidious to justify bringing it within the criminal law, then it should not generally be regarded as a legitimate basis for interception or surveillance.

The criminal law brings with it the principle that the prohibited activity must be properly defined. By contrast it is wholly wrong, and inimical to the requirements of certainty and predictability that lie at the heart of the rule of law, that a person's liability to an invasion of privacy by the executive should turn on the application of ill-defined concepts whose meaning, as the law stands, depends not on the rigours of judicial interpretation but on little more than the subjective assessment of the executive itself.

We recognise that, exceptionally, activity may properly be regarded as closely analogous to serious crime but for technical reasons fall outside the strict ambit of the criminal law. Examples might include activities carried on under the cloak of diplomatic immunity, or activity connected with commission of acts abroad over which the UK courts lack jurisdiction or which are not clearly offences under the law of the territory in question. The solution may be to adjust the definition of "serious crime", or alternatively to retain a separate category but to ensure that it is considerably narrower and more precise than the present heads of national security and economic well-being.

4.2 Serious crime

Our first concern lies with the alternative, rather than cumulative, formulation of the definition in IOCA s. 10. Crime is "serious" if the first limb of the definition is satisfied (offence involving violence, substantial financial gain or common purpose) even if the second condition (likelihood of three years' or more imprisonment on first conviction) is not.

In our view the likely sentence for an offence is always a relevant indicator of its seriousness. A crime should not be considered sufficiently serious to justify interception if it would be regarded by the courts themselves as not sufficiently serious, in all the circumstances, to merit a substantial term of imprisonment. One result of the present definition is that interception risks becoming a routine option for investigations into certain kinds of offence - for example, revenue or customs offences where "substantial financial gain" will almost always be the suspect's purpose - even though a particular suspect might not be expected to receive a custodial sentence.

The conditions should therefore be made cumulative, not alternative.

Our second concern is with the "common purpose" head. We are not persuaded that the mere fact that common purpose or large numbers are involved in activity inherently aggravates an offence to the point where interception and surveillance become legitimate *for that reason*. The emphasis on common purpose increases the risk that the net of surveillance extends indiscriminately to participants in legitimate collective activity - industrial action, organised protest and so on. Even if unlawful conduct occurs in the course of collective activity, it may in itself be trivial in nature; and indeed may not involve the interception subject as a participant in crime at all. It is worth recalling that the European Court has recognised that an innocent party to a communication which is intercepted for reasons connected with the other party has a potential complaint under Article 8. Interception against a person under the common purpose head simply on the basis of an association with others would similarly give rise to a complaint that the interference with privacy was not necessary or proportionate.

The common purpose head should be removed from the definition.

5 Authorisation procedures

This heading responds to Chapter 7 of the Consultation Paper. The Government proposes no substantial change to the present arrangements.

5.1 Judicial authorisation

We are strongly of the view that the procedure for *executive* authorisation of interception is fundamentally objectionable. The case-law of the European Court of Human Rights emphasises that prior *judicial* sanction is the preferable safeguard for the citizen's Article 8 rights in the investigative context. In the debates in the House of Lords on the Bill for the Police Act 1997, Lord Browne-Wilkinson was among several speakers strongly critical of the proposal that executive rather than judicial authorisation should apply to surveillance under what became Part III of the Act.

The position under IOCA and its offspring (including Part III of the 1997 Act) compares unfavourably with the framework for obtaining sensitive material in the course of ordinary criminal investigations. Under Schedule 1 to the Police and Criminal Evidence Act 1984, "special procedure material" (including journalistic material and other material held in confidence), the necessary authority must be given by a circuit judge. In the case of information held by a party other than a suspect - where, for example, access is sought to unpublished press photographs - the procedure is on notice.

As far as the "serious crime" ground for interception is concerned, we see no reason why the safeguards for the suspect in relation to attempts to obtain material by interception should not be at least as rigorous as those applicable to *routine* crime under PACE. Nor is there any compelling justification for executive, rather than judicial, authorisation in the case of the national security and economic well-being grounds. Indeed it is precisely because of the open-textured nature of those concepts that requests for authority on those grounds ought in principle to be examined by a judge rather than a politician or (under Part III of the 1997 Act) a police officer. Judicial involvement under PACE is designed to maintain public confidence in the operation of the system. The need to achieve that is all the stronger in relation to clandestine surveillance by central government agencies.

Given that the focus of IOCA interception is on *serious* crime, and by analogy on similarly grave conduct under the national security and economic well-being heads, it is appropriate that requests for authorisation should involve a High Court judge.

Our recommendation is therefore for a procedure under which a request for an interception warrant should be made in writing to a High Court judge in private. The judge should give brief reasons for granting or refusing a warrant.

5.2 Information held by third parties: on notice procedure

The on notice PACE procedure was introduced as a necessary safeguard for important rights. Requests by the police for press disclosure of journalistic material raise issues under Article 10 of the Convention. The judge provides vital independent scrutiny of the request and is well-placed to strike the proper balance between the interests of the investigation on the one hand and the public interest in maintaining the freedom of the press on the other. In many cases privacy interests are also at issue, in the shape of the relationship between journalists and those who provide them with information.

By analogy with the PACE position, an application on notice would be appropriate where communications data are sought from a CSP. There should be a simple procedure, similar to the practice on applications under Schedule 1 to PACE, for a request to be served on the CSP and then considered at a private hearing before a High Court judge. We would not object to there being an alternative procedure without notice in exceptional cases of genuine urgency. In those cases the warrant should be of very short duration and followed by an application on notice at the earliest opportunity.

5.3 The test to be applied

Section 2(3) of IOCA requires the Secretary of State to consider the availability of alternative means of obtaining the relevant information before granting authorisation. By contrast, the access conditions in

paragraph 2 of Schedule 1 to PACE require the judge to be satisfied that other methods have either been tried unsuccessfully or have not been tried because they were bound to fail. We think that a strong condition of that kind properly reflects a proportionate approach: merely requiring the relevant authority to "consider the availability" of other means is too loose a test because it permits the grant of a warrant even where other means might well be adequate. A strong condition should therefore apply in interception cases.

5.4 Duration and modification

An initial duration of three months is not in itself objectionable provided that is the maximum rather than the norm. The judge should consider in each case the period for which the warrant is genuinely needed. Renewal might properly be dealt with on written application to the judge, but the judge should have a discretion to require an application for renewal to be made at a private hearing.

We agree that it is sensible for there to be an administrative power to make minor or technical variations, for example to reflect a change in the subject's telephone number. The warrant should expressly state the scope of the minor amendments of this kind that can be made. Beyond that, applications for modification should be made in writing to the judge, again with a power to require a hearing at the judge's discretion.

6 Supervision and remedies

The Consultation Paper proposes retention of the present system of bipartite supervision by a Commissioner and a Tribunal. We consider that system seriously inadequate.

6.1 The Tribunal

We consider that in place of each of the statutory regimes which follow (Broadly) the IOCA model, the legislation should establish a Tribunal with power, on application by an individual, to review the substantive merits of authorisation of the interception, surveillance or other measures in question. It should not be confined to the narrow ground of the validity of a warrant.

That is particularly so for this reason. In many cases the measure in question will affect not only the individual's Convention rights but interest under the ordinary law which the Convention recognises as "civil rights" within Article 6. The individual seeking redress for an interference with those rights is entitled to have access to a body meeting the requirements of a court. That implies that the Tribunal must not only meet the requirements of independence and impartiality but must be in a position to determine the merits of the decision to impose the measure in question. Although we recommend a judicial procedure for prior authorisation, that procedure of course cannot comply with Article 6 since it will (necessarily) have taken place without notice to the affected individual. So the Tribunal, in conducting its after-the-event investigation, must have "full jurisdiction" to revisit the matters considered when authorisation was granted.

The present Tribunal procedures fall far short of the requirements of fairness and transparency. Even taking into account the inevitable need for a degree of secrecy to protect sources of information and methods of intelligence-gathering, the present regime is indefensible. The shortcomings of the present closed process amplify our objection to the breadth of vagueness of the national security and economic well-being grounds: since the Tribunal neither hears argument nor gives reasons for its decisions, it is impossible to subject the authorities' contentions about the range of activity encompassed within these concepts to adversarial critique, or to know what meaning the Tribunal gives them. Yet the threshold question whether any of the grounds for authorisation was established in a particular case is surely central to any adequate remedial or supervisory process.

Although the former European Commission of Human Rights in *Christie* recognised the restricted opportunity for review which the present Tribunal offers, it found no violation of Article 8. However, the Court's more recent jurisprudence reflects an increasing willingness to view with considerable circumspection arguments that the fairness of proceedings may be compromised on national security grounds: see in particular the Court's *Tinnelly and McElduff* v. *UK* judgment of 10 July 1998. Although that decision concerned Article 6 rather than Article 8, the court's Article 6 jurisprudence has long been a source of inspiration for the procedural requirements attached to substantive Convention rights, including rights under Article 8; and, as already mentioned a party's "civil rights" may well additionally be at issue in the interception and surveillance context.

We consider that both the enlargement of the scope of the Tribunal's reviewing function, and observance of higher standards of openness and equality of arms, could readily be achieved without compromising the proper operational requirements of the agencies. The material presented by the agency in support of its case could be presented in summary form, with documents of particular sensitivity either withheld or supplied with parts deleted, and the identity of operational personnel or sources of information likewise withheld if need be. The proceedings could be held in private. The Tribunal might hear exceptionally sensitive evidence in the absence of the complainant and his or her representative and, on their return, indicate the gist of that evidence sufficiently to enable the complainant to know what case has to be met. The Tribunal's decision could be carefully framed to avoid disclosing information which ought not to be revealed and could if necessary provide abbreviated reasons for its findings.

The European Court of Human Rights acknowledged in *Tinnelly* (in this respect following the approach of the European Court of Justice in *Johnston* v. *Chief Constable of the RUC*) that such departures from the usual standards of judicial proceedings may be perfectly permissible where necessary. What is not acceptable is the wholesale abandonment of those standards in every case. The proper course is for the legislation to enable the making of rules of procedure which permit the Tribunal, in its discretion, to strike the right balance between secrecy and transparency in dealing with the various aspects of the proceedings in each case.

The draft ECB takes a small step in this direction. Schedule 2 envisages hearings with legal representation and evidence; it enables the making of rules of procedure dealing with admissibility, the mode and burden of proof, and the circumstances in which a complainant and his or her legal representative may be excluded.

Paragraph 6 of that Schedule provides for appointment of a "special representative" to attend parts of the hearing from which the complainant and his or her representative are excluded. That echoes arrangements in the appeals which now lie against "public good" deportations under the Special Immigration Appeals Commission Act, introduced in the wake of the European Court's insistence in its *Chahal* judgment that the Article 13 right to an effective remedy was violated by the absence of adequate judicial machinery for review of those cases.

To these examples can be added the practice followed in the employment tribunals in Northern Ireland in the wake of the *Johnston* case in adopting the necessary techniques to avoid compromising national security while at the same time ensuring that the citizen obtains a fair hearing. That is the theme common to all these examples and to our proposals for the Tribunal in the present context.

We should say that of the various techniques mentioned here, we think that the appointment of a "special representative" is not a desirable route. In place of the rather incongruous fiction of a "representative" who, as para. 6(3) of Schedule 2 to the draft ECB makes clear is "not responsible to the person whose interests" he or she represents, we would prefer the more direct course of the Tribunal itself summarising for the complainant the gist of the material received in his or her absence.

Proof by a complainant that interception or surveillance has occurred is inevitably difficult in this area. The authorities invariably prefer not to admit to such activity. No doubt that is what the reference to

mode and burden of proof in para. 6 of Schedule 2 to the draft ECB gestures at. The European Court and Commission have developed a pragmatic test of "reasonable likelihood". Adoption of that test in Tribunal proceedings would be a broadly acceptable solution assuming it were not possible to eliminate the problem. In our view, though, the problem could easily be removed: we see no compelling reason why the subject of interception should not as a general rule (and subject only to necessary exceptions agreed on a case by case basis by the Tribunal or authorising judge) simply be told about the interception after it has ceased. That practice works satisfactorily elsewhere (in Germany, for example).

The decisions of the Tribunal proposed under the ECB will be appealable to the High Court on a point of law. The same should apply in the fields of surveillance and interception.

Finally, the Tribunal machinery should be accessible to a person who is not as such the subject of an authorisation but who is a party to intercepted communications. Because such a person is a "victim" for the purpose of an Article 8 complaint, in the absence of a right to complain to the Tribunal the courts are likely to fashion remedies of their own, dealt with in ordinary proceedings less suited to determination of issues in this area than the specialised Tribunal environment we propose.

6.2 The Commissioner

The Commissioner does not purport to act as a judicial authority, and provided the Tribunal acquires the necessary powers and procedural safeguards we would be broadly content with the Commissioner's present constitution. We consider that the ability of the Tribunal to call on the Commissioner to assist it is valuable provided the Commissioner's role is confined to investigation of factual matters. The Tribunal should not be influenced by the Commissioner's *opinions* on the very issues it is called upon to determine.

7 Use of material in evidence

Chapter 8 of the Consultation Paper invites comment on s. 9 IOCA.

This is a complicated and troublesome provision. The Commission decision in *Preston* ignores a very real inequality between the parties. The investigating and prosecuting authorities have complete access to any intercept material and may use it to pursue lines of inquiry, within and outside the trial process, which are not open to the defence. Once the Human Rights Act is in force, the UK courts are unlikely to follow *Preston*, particularly in view of dicta of the House of Lords in *Sultan Khan*. There is the prospect that an unamended s. 9 would either be substantially re-interpreted or declared incompatible with Article 6.

If and only if authorisation of interception is judicial rather than administrative we would accept the amendment of the protection set out in section 9. Absent that vital safeguard, we are of the view that intercept material should not be admissible in evidence. This does not prevent the authorities using the intercept material as the basis for lines of ordinary investigation with a view to obtaining admissible evidence.

If no change is made, fairness (and Article 6) requires that the material should generally be disclosed to the defence so that it is equally enabled to make appropriate inquiries of its own.

Subject to judicial control of warrants we recommend replacement of s. 9 with a simple provision to the following effect:

- Intercept material obtained in breach of the legislation should simply be inadmissible. In the context of criminal proceedings that is a more focused deterrent, and one every bit as potent, as the risk of conviction of an offence of unlawful interception.

- Where lawful intercept material forms any part of the prosecution case, it should be open to cross-examination, if necessary subject to proper conditions (such as those we suggest in relation to Tribunal proceedings) to ensure secrecy or anonymity where, and to the extent, that is genuinely necessary. The quality and reliability of that part of the evidence can then be fairly and fully considered by the jury.

- Lawful intercept material unused by the prosecution should be disclosable as unused material in the ordinary way, subject only to proper exceptions conditions to ensure necessary secrecy etc. (much as the current practice in the case of material obtained from informers).

Summary of recommendations

Scope: subject-matter of proposed powers

- **Private systems:** the legislative framework should not make technical distinctions based on the 'public' or 'private' status of the employer.

- **Communications data:** the grounds on which access to this material may be sought, and the authorisation and supervision procedures applicable, should be no less strict than those we propose below in relation to interception proper.

- **CSPs (1):** Concern that compelling CSPs to make systems subject to interference will make them communication less secure and less private.

- **CSPs (2)**: OFTEL's lack of independence renders it unsuitable for an adjudicating role

Scope: grounds for interception

- **National security and economic well-being:** in almost all cases, 'serious crime' will be the only necessary and defensible category. Where, exceptionally, seriously harmful activity may fall outside strict ambit of the criminal law then the solution may be to adjust the definition of serious crime, or to retain a separate category far more precise than 'national security' and 'economic well being'.

- **Serious crime (1):** the formulation in IOCA s10 should be cumulative rather than alternative.

- **Serious crime (2):** the 'common purpose' head should be removed from the definition.

Authorisation procedures

- **Judicial authorisation:** under the 'serious crime' ground for interception, safeguards should be at least as rigorous as those applied to routine crime under PACE. Requests for authorisation should be made in writing to a High Court judge in private.

- **Information held by third parties - on notice procedure:** by analogy with PACE, an application on notice would be appropriate where communications data are sought from a CSP. A simple procedure similar to that in PACE Schedule 1 should be applied, with a request served on the CSP and then considered at a private hearing before a High Court judge.

- **The test to be applied:** a strong condition of the kind in PACE Schedule 1 para 2, requiring the judge to be satisfied that other methods have failed or have not been tried because they were bound to fail, should be applied instead of the requirement that the relevant authority 'consider the availability' of other means.

Supervision and remedies

- **The Tribunal (1) :** the scope of the Tribunal should not be confined to the narrow ground of the validity of the warrant.A Tribunal should be established with power to review the substantive merits of authorisation of interception, surveillance or other measures. In conducting 'after the event' investigation the Tribunal must have full jurisdiction to revisit the matters considered when authorisation was granted.

- **The Tribunal (2):** enlargement of the scope of the Tribunal's reviewing function, and observance of higher standards of openness and equality of arms, could be achieved without compromising the proper operational requirements of the agencies. The legislation should enable the making of rules of procedure which permit the Tribunal to strike the right balance between secrecy and transparency.

- **The Tribunal (3):** the subject of interception should be told about it after it has ceased, a practice which works satisfactorily elsewhere (in Germany, for example).

Use of material in evidence

- **IOCA s9** should be replaced with a simpler provision to the following effect: interception material obtained in breach of the legislation should be inadmissible; where lawful interception material forms part of the prosecution case it shouldbe open to cross examination (if necessary, subject to conditions to ensure secrecy and anonymity); lawful intercept material unused by the prosecution should be disclosable as unused material in the ordinary way. Implicit in this recommendation is that the authorisation of interception will be judicial rather than administrative. Without this safeguard, intercept material should not be admissible in evidence.

Liberty, August 1999