HOME OFFICE CONSULTATION ON THE INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM

BT VIEW

General

1. BT agrees that it is timely to update the current Interception of Communications Act 1985 to take account of changes in the market and to extend the law to cover non-PTO networks and the recording of communications in the course of lawful business practice.

2. We welcome the intention to retain the existing safeguards contained in the Act to ensure only authorised interception takes place and that there is independent judicial oversight of the process.

3. Our further observations and concerns are outlined below and answers to the questions raised in the Consultation are annexed.

Meeting the New Obligations – Securing Confidence

4. Under the proposals, many more organisations will become subject to IOCA for the first time. The legislation should, as far as possible, make due allowance for continued change in communications services whilst providing the level of certainty in application and impact that communication service providers need, to minimise any adverse impact on their businesses. Clarification of definitions such as Communications Service Provider (CSP) or a mechanism for 'downstream' clarification of, for instance, "reasonableness" will be important to secure confidence in the revised Act.

5. The mechanism for deciding what is a "reasonable intercept capability" will be a key factor in meeting the concerns of Communications Service Providers (CSPs) regarding compliance. Whilst Oftel has considerable experience in telecommunications matters, we do not believe that it alone is necessarily the most appropriate body to lead on the practical implementation of the revised Act. We believe there is a case for adapting the recent proposals for an Electronic Trust Services organisation to include compliance with the revised IOCA. Alternatively an independent body, representing <u>all</u> parties should be established.

6. As a matter of principle, a common set of requirements should apply to all CSPs to ensure fair and effective implementation of the legislation. We accept that the means of achieving those requirements may vary between CSPs, but variation, for example, in the size of such organisations is not in itself a valid justification for discriminatory application of the rules.

7. Wherever possible, requirements should be based on international standards to maximise fair and effective global application and minimise costs, and to ensure that technical solutions are available in a timely, efficient and effective manner.

Provision of Communications Data

8. We recognise the merit in placing the provision of data on a secure legislative footing to protect both the individual and the organisations required to provide the data. We do however have a number of concerns regarding implementation.

   - Use of data within and between CSPs must continue to be allowed for the combating of crime such as fraud.

   - There should be no provisions requiring CSPs to collect, store or manipulate data for the Law Enforcement Agencies (LEAs) other than that gained in the normal course of business.

   - There should be checks and balances allowed for in the legislation to ensure the reasonable implementation of the obligations, adequate monitoring of the operation of the process and a route of appeal in the event of disagreements.

Monitoring for Business Purposes

9. It will be important to businesses, CSPs and PTOs to ensure that legitimate monitoring is not unintentionally prohibited by the new legislation particularly as new and unforeseen services come into existence. There is already a need for instance with regard to e-mails as well as voice calls

Use of Intercept Material

10. BT concurs with the analysis in the consultation document that the evidential use of intercept material would be difficult to establish and of doubtful long term net benefit. However, if such a change was implemented, due consideration would need to be given to the additional cost of providing intercept material that would be acceptable in court, whether this would be justified and who should bear the cost. A further important consideration would be to ensure the personal safety of any employees involved in security sensitive cases such as those involving terrorists.

Security

11. Consideration will need to be given to the security of intercept systems. This may prove to be a more difficult issue for the operators of smaller systems.

Annex follows

Crawford Stewart
BT Regulatory Affairs Department

Tel: 0171 728 4109
Fax: 0171 236 3457
e-mail: crawford.stewart@bt.com

ANNEX

HOME OFFICE QUESTIONS FOR PROVIDERS OF COMMUNICATION SERVICES

1. **Please describe the nature of the market you operate in and a general indication of the size and nature of your customer base.**

   BT is experiencing major change, in an industry that is changing the way people live and work around the world. BT is transforming itself from a UK telecommunications company into a global communications company. "Telecommunications" is now, we believe, too narrow a word to sum up the wide range of things we do and want to do. We have grown from a national telecommunications operator, dealing mainly in fixed-voice telephone calls, to a global communications company with operations that span the world, and services that, in addition to fixed-voice telephony, include the Internet, mobile and data communications, and business systems and solutions.

   Data

   Data communications, which covers almost all network traffic that is not voice – including e-mail, the Internet, electronic commerce, and files sent from computer to computer – is growing at more than 30 per cent per year. Data has overtaken voice communication over BT's networks, a phenomenon often referred to as the

   Investment in our networks

   In 1998/99, we launched the UK's largest and most advanced data network. And we have earmarked £5 billion for future investment in data and multimedia services.

   Concert

   BT is already a world-leader in the growth area of global managed services through Concert Communications, which has 40 per cent of the *Fortune* top 500 companies as customers. And Concert is to become a key part of BT's contribution to the global venture we are forming with AT&T.

   Liberalised markets worldwide

   Our growth in the recently-liberalised markets worldwide has continued. In the European market, which is growing by ten per cent per year, we currently have more licences than any other operator. In 1998/99, our European ventures increased their customer numbers by more than 150 per cent to over nine million. In Asia Pacific, we have made carefully targeted investments in high-growth companies.

   Mobility

   The market for mobile communications is growing at 20 per cent per year and our mobile operations now have more than 14 million customers worldwide.

   Business systems

   And, in the market for business systems, BT's Syncordia Solutions, which manages networks for corporate clients, and Syntegra, which designs integrated business systems, together grew by more than 20 per cent in 1998/99.

(*Extract from BT 1999 Annual Report and Accounts*)

2. **Does your company fall within the scope of IOCA 1985, and if so do you compete with UK companies upon whom there is currently no intercept requirement?**

   As a PTO BT runs public networks that fall within the ambit of IOCA 1985. These carry voice, data and internet services amongst others. BT competes with other PTOs and service providers – many of the latter are not normally subject to the Act.

3. **If you are not subject to IOCA 1985, do you compete with companies who are?**

   See 2 above.

4. **Do you already have the capability to monitor your network where necessary for fault diagnosis or other purposes? How much additional work do you consider would be required to ensure that communications passing over your network are capable of being intercepted? What cost is involved, the nature and the scale of the cost and would it be a one-off or recurring cost?**

   BT already complies with the requirements of IOCA 1985 and monitors its networks for operational reasons in a similar way to most other operators. The additional cost involved in meeting the proposed new requirements will depend on the actual nature of the information required to be intercepted. The use of standardised solutions would help to reduce costs. There are no standardised solutions yet for data networks and their applications. The security aspects of implementing such solutions also require further consideration. In a widespread competitive, global environment, the maximum standardisation should be employed to reduce costs.

   A clearer understanding of likely cost impacts can probably be best determined in dialogue with Government. The conclusions from this could then inform further consultation following this initial exercise. BT has indeed been discussing this issue further with the Home Office. It will of course be important to ensure that the interception or provision of certain types of data does not place an unreasonable burden on CSPs and BT welcomes the concept of only requiring compliance with what is a ‘reasonable’ requirement.

5. **Compliance costs aside, can you identify any impacts these proposals will have upon your business?**

   BT believes the extension of IOCA to non-PTO networks is important both in ensuring law enforcement authorities have the tools necessary to fight crime and ensuring that PTOs are not put at a competitive disadvantage to other CSPs.

6. **If you operate internationally, how do the proposed requirements compare with those placed upon you in other countries? Would it be helpful to have more consistency internationally?**

   As the Information Society takes on a global nature international harmonisation is of growing importance and would undoubtedly be of benefit. However the reality of different cultures and legal systems means that this will of necessity be a gradual process and should not be imposed to the detriment of the UK. Such developments are probably best left up to the competent interest groups, such as the EU Police Co-operation Working Group with the assistance of ETSI.

7. **While implementing these measures, how can the Government best support you to minimise the impact on your business?**

   Obligations that would require retrospective redesign of networks and systems should be avoided wherever possible. Practical requirements and standards should be made clear and stable from an early stage. The costs to all parties of executing a warrant should be an explicit factor when the relevant authority considers the case for each request.

8. **Do you have any suggestions for improvements to the proposals for a framework to achieve a "reasonable intercept capability" (paras 5.3 – 5.5)?**

   We believe consideration should be given to the following:

   - A common set of requirements should apply to all CSPs to ensure fair and effective implementation of the legislation. We accept that the means of achieving those requirements may vary between CSPs, but variation, for example, in the size of such organisations is not in itself a valid justification for discriminatory application of the rules.

   - The organisation chosen to advise on the implementation of the scheme and what it is "reasonable" should be demonstrably independent, have the necessary expertise and be representative of all the main interest groups. Given the specialist nature of the issue it may be worth considering setting up a new body to fulfil this role. Alternatively there may be an opportunity to extend the functions of the proposed self-regulatory scheme for Electronic Trust Services. This has a number of attractions:

Flexibility:	the ability to adapt to changing technologies;
Responsiveness:	the capability to react quickly to opportunities and concerns

Cost effectiveness:	for government, industry and users;
Representation:	from a broad range of stakeholders to establish effective criteria.
Sanctions:	ensuring compliance without criminal sanctions

9. **What sanctions, if any, do you think would be appropriate where a CSP failed to provide a reasonable intercept capability or assistance when required by warrant? Would such sanctions assist in ensuring a level commercial playing field for comparable CSPs?**

   As suggested above, the most realistic form of sanction may be via an independent self-regulatory body where, as with Trust Services, there appears to be no easy legislative solution. This solution would obviously require further work within the communications industry, but an early indication of likely government support would be helpful.

10. **If you are a small – medium sized business can you comment on the ways that compliance to these proposals would be difficult or impossible?**

    N/A

11. **Are you content for your replies to these questions to be published? YES/NO**

    Yes.

END OF ANNEX