

Lawful Business Practice Regulations Information

This document provides the following information concerning the Lawful Business Practice Regulations. Please note that in view of the time that has elapsed since these regulations were introduced some of the information that has been reproduced may be slightly incomplete:

1. Regulatory Impact Assessment: Pages 2-12
2. Notes for Business: Pages 13-16
3. Conclusion: Page 17
4. Consultation Responses: Pages 18-50
5. Summary: page 51
6. Statutory Instruments: Pages 52-55
7. Legislation Background: Pages 56-57
8. Questions For Consultees and Issues Pages 58-62
9. How To Respond: Pages 63-64
10. Key Issues Raised In The Consultation: Pages 65-70
11. Outline Of The Original Proposals: Page 71
12. Outline Of The Final Regulations: Page 72
13. Legislative Overview: Page 73

1. REGULATORY IMPACT ASSESSMENT

PURPOSE AND INTENDED EFFECT OF THE MEASURE

Issue and Objective

Issue

The Regulation of Investigatory Powers Act 2000 prohibits the interception of communications made by means of a public or private telecoms system without consent. However, Section 4(2) of the Act allows the Secretary of State to make "Lawful Business Practice" Regulations to authorise businesses to intercept communications on their own private systems without consent for certain purposes.

Objective

Businesses need to intercept communications for a variety of legitimate purposes such as keeping essential records of transactions and ensuring the operation of their systems. The objective of the regulations is to ensure that businesses will be able to continue to make interceptions for essential purposes once the Regulation of Investigatory Powers Act comes into force. However, it is also important to ensure that the regulatory framework governing interception provides sufficient protection for the confidentiality of communications and individuals' right to privacy.

Article 5.1 of the Telecoms Data Protection Directive requires Member States to ensure the confidentiality of communications made by means of a public telecoms system (which includes the beginning or end of such a communication on a private system). Articles 5.2 and 14.1 establish the extent to which Member States can make an exception to this rule. The Lawful Business Practice Regulations can only exempt business from the requirement to gain consent to the extent permitted by the Directive. The Regulations must also not go further than permitted by the European Convention of Human Rights and the Human Rights Act 1998.

Risk Assessment

The Regulation of Investigatory Powers Act establishes new legal constraints on the interception of communications. The purpose of the Lawful Business Practice Regulations is to ensure that legitimate business activities are not unfairly hindered as a consequence of the Act.

OPTIONS

Options available

Four main options have been identified:

Option A (Not to make any regulations.) Not to make any regulations authorising businesses to intercept communications without consent.

Option B (Regulations allowing essential interceptions; business to inform staff and third parties.) To make regulations which allow businesses to intercept communications without consent for evidentiary and operational purposes providing that they make all reasonable efforts to inform both staff and third parties of interceptions

Option C (Regulations allowing interceptions for essential and quality control purposes; businesses to inform staff.) To make regulations which allow businesses to intercept communications without consent for evidentiary, operational, and quality control purposes providing that they make all reasonable efforts to inform staff of interceptions.

Option D (Regulations authorising all interceptions; businesses not required to inform staff or third parties.) To make regulations which allow businesses to intercept without consent for any purpose without needing to inform staff or third parties of interceptions.

Issues of equity or fairness

It is important that the regulations strike a fair balance between, on the one hand, facilitating legitimate business practices and, on the other hand, ensuring that individuals' confidentiality and privacy are adequately protected.

BENEFITS - Identify the Benefits

Benefits for Business

The benefit of the regulations is that they will allow businesses to intercept communications without consent for certain purposes. This will facilitate business practices by avoiding, in certain cases, the costs and difficulties involved in gaining consent. The Regulations will provide business with the legal certainty they need to derive full benefit from modern communications technology and to develop innovative ways of handling information.

Benefits for Employees and Consumers

The regulations will establish the purposes for which businesses can intercept without consent and the conditions that businesses will have to meet before doing so. They therefore fit into the framework of legislation designed to ensure that individuals' right to privacy is respected.

Quantity and Value

Option A (Not to make any regulations.)

Benefits for Business

This option would provide no benefit to business because it would not allow interception for any purposes without consent. It would seriously hinder essential business practices such as keeping records of transactions and ensuring the operation of communications systems.

Benefits for Employees and Consumers

This option would ensure a very high degree of protection for the confidentiality of communications by requiring consent to be gained before an interception could take place. However, consumers would suffer from lower standards of service because of the disruption caused to legitimate business practices such as maintaining the effective operation of systems and procedures and monitoring for quality control. This option would also inhibit business from making interceptions for the purpose of protecting staff from abuse or harassment.

Option B (Regulations allowing essential interceptions; business to inform staff and third parties.)

Benefits for Business

This option would facilitate essential business practices by allowing interceptions without consent for purposes such as keeping records and ensuring the operation of communications systems. However, businesses would need to modify their practices and procedures in order to inform staff and third parties of interceptions. They would also need to modify their procedures in order to gain consent for interceptions for purposes outside the scope of the regulations such as staff training, quality control, marketing and market research.

Benefits for Employees and Consumers

This option would result in a high level of consumer awareness of businesses' practices regarding interception. However, some of the costs of informing third parties of interceptions would inevitably be passed on to customers.

Consumers might suffer lower standards of service because the Regulations would not allow businesses to intercept without consent for purposes of quality control. Employees might also suffer if the Regulations had a negative impact on their training.

Option C (Regulations allowing interceptions for essential and quality control purposes; businesses to inform staff.)

Benefits for Business

This option would facilitate legitimate business practices by allowing interceptions without consent for purposes such as keeping records, ensuring the operation of communications systems and monitoring calls to ensure a high level of service.

Businesses would not need to restructure their procedures in order to inform third parties of interceptions or in order to gain consent for interceptions for quality control purposes. However, if they did not do so already, businesses would need to ensure that staff were aware that interceptions might take place. They would also need to gain consent before intercepting for purposes outside the scope of the regulations such as marketing or market research.

Benefits for Employees and Consumers

This option would ensure that businesses informed employees that interceptions might take place. This would help to ensure that employees understood what level of privacy they could expect when making personal communications on their employers' systems. This option would avoid placing significant burdens on business that might be passed on to the consumer. Customers would benefit because businesses would be able to monitor communications in order ensure high standards of service.

Option D (Regulations authorising all interceptions; businesses not required to inform staff or third parties)

Benefits for Business

This option would not change the legal position of businesses regarding interception before the entry into force of the RIP Act. It would allow businesses to continue intercepting communications on their networks for any purposes as at present.

Benefits for Employees and Consumers

This option would do nothing to limit the purposes for which businesses might intercept without consent and it would not require businesses to inform either staff or consumers that interceptions might take place. This option would be in breach of the Telecoms Data Protection Directive and would risk breach of the European Convention of Human Rights and the Human Rights Act 1998. It would fail to provide adequate protection for the confidentiality of communications and it would allow businesses excessively wide scope to intercept without consent.

COMPLIANCE COSTS FOR A "TYPICAL" BUSINESS

Business Sectors Affected

These proposals have a bearing on the activities of a wide range of businesses. The financial services industry, in particular, needs to be able to record evidence of telephone transactions. The operators of call centres need to be able to monitor communications in order to ensure a high quality of service. Businesses need to intercept emails in order to check for viruses and protect against attack as well as to conduct routine activities such as accessing email accounts in the absence of staff. It would be extremely difficult, if not impossible, to reach an accurate estimate of the total number of businesses affected - or potentially affected - by the Regulations. This is because of the sheer range of businesses

that need to intercept for routine operational purposes such as checking for viruses or accessing emails in staff absence.

The call centre industry, in particular, would be affected by any change to current practices of call monitoring for quality control purposes. In 1999, there were 2150 major call centres in the UK with 20 or more telephone operators. There were also 4200 smaller centres with 3-19 telephone operators. These numbers are expected to increase significantly in 2000-2001. The Financial Services industry, in particular, would be affected by any change to current practices regarding the recording of telephone transactions. The Financial Services Authority estimates that there are currently 22,000 financial services organisations operating in the UK.

Compliance Costs for a "typical" business

Option A (Not to make any regulations.)

Businesses would need to overhaul their procedures in order to gain the consent of correspondents before making any interceptions.

This option would impose extremely heavy costs on a wide range of businesses. It would not be possible to arrive at an exact estimate of costs because of the variety of businesses affected to varying degrees. However, it is worth noting that this option would inhibit businesses from making essential interceptions for purposes such as scanning for viruses and ensuring the operation of their email systems. As such, it would affect the majority of businesses that operate modern communications systems.

This option would also inhibit businesses from conducting transactions by telephone. The financial services industry, in particular, would need to put in place procedures to gain consent for recording before conducting telephone transactions.

Option A would impose overwhelming practical difficulties for a large number of businesses. The consultation exercise suggested that some businesses would relocate operations outside the UK if the regulatory environment inhibited interceptions without consent for essential operational purposes.

Option B (Regulations allowing essential interceptions; business to inform staff and third parties)

If they did not do so already, businesses would need to modify their procedures to ensure that staff and third parties were aware that interceptions for purposes authorised under the regulations might take place. Businesses would need to modify their procedures to ensure that they gained consent before making an interception for purposes outside the scope of the regulations such as quality control, staff training, marketing and market research. The consultation exercise revealed that a large number of businesses were very concerned about the costs of informing third parties. One major British company suggested that the costs of installing new equipment and procedures in order to inform callers of interceptions might amount to £100,000.

The consultation also revealed that businesses were concerned about the costs of needing to gain consent for interceptions for quality control purposes. A national call-centre with 2000 telephone operators suggested that the costs of reorganising procedures in order to gain consent before monitoring calls for quality control purposes would be £800,000 per annum. Around 400,000 call centre and other telephone operators in the UK might be affected. We could, therefore, estimate that the total costs of having to gain consent for quality control monitoring might be £160 million.

Option C (Regulations allowing interceptions for essential and quality control purposes; businesses to inform staff.)

Businesses would need to modify their procedures to ensure that staff were aware that interceptions for purposes authorised under the regulations might take place.

Businesses would need to modify their procedures to ensure that they gained consent before making interceptions for purposes outside the scope of the regulations such as marketing and research. The consultation exercise did not reveal that businesses were generally concerned about the costs of informing staff that interceptions might take place. Both British Chambers of Commerce and the Federation of Small Business indicated that they did not believe this requirement would impose a significant burden on business. One large service company estimated that it would cost £15 per employee to run training meetings to inform staff of its interception practices. However, the DTI believes that in most cases this would be a matter for routine communications between employers and staff and would not involve significant costs. A small number of respondents argued that businesses ought to be able to monitor communications without consent for marketing and

market research purposes. However, the majority of respondents agreed that businesses ought to gain consent before intercepting for these purposes. The DTI believes that in the majority of cases, businesses will be able to conduct these operations without needing to intercept communications.

Option D (Regulations authorising all interceptions; businesses not required to inform staff or third parties)

This option would impose no costs. Businesses would not need to change their current practices in any way. However, this option would be in breach of the Telecoms Data Protection Directive and would risk breach of the European Convention of Human Rights and the Human Rights Act 1998.

Total Compliance Costs

It would be very difficult to make an accurate estimate of the total compliance costs of each option. The Regulations affect - or potentially affect - a wide range of businesses in a variety of ways. However, it is possible to weigh the cost burden of each option in relation to the others:

Option A (Not to make any regulations.)

This option would impose extremely heavy costs. A wide variety of businesses would need to overhaul essential, routine procedures such as checking emails for viruses and checking email accounts in the absence of staff.

Option B (Regulations allowing essential interceptions; business to inform staff and third parties)

This option would impose significant costs for a large number of businesses by requiring them to restructure procedures to inform correspondents that interceptions take place. It would also impose significant costs for call centres and other businesses that intercept for quality control purposes. These businesses would need to restructure their procedures to gain consent before monitoring for quality control.

Option C (Regulations allowing interceptions for essential and quality control purposes; businesses to inform staff.) This option would not impose significant costs on many businesses. It would require a large number of businesses to inform staff of interception practices. However, this could be done without considerable expense. Businesses that intercept without consent for marketing purposes might also need to review their practices.

Option D (Regulations authorising all interceptions; businesses not required to inform staff or third parties) This option would not impose any costs. However, it would be in breach of the Telecoms Data Protection Directive.

CONSULTATION WITH SMALL BUSINESS

The DTI has held meetings with the British Chamber of Commerce and the Federation of Small Businesses in order to ensure that the regulations take account of the needs of small to medium sized enterprises. We have also developed the proposals in close consultation with our own Small Business Service. These discussions made clear that small businesses might incur significant costs if they were required to inform third parties before making routine interceptions. They also made clear that some small businesses, like larger companies, need to monitor communications in order to ensure high quality of service. There was no indication that small businesses would incur significant costs as a result of having to inform staff that interceptions might take place. The DTI's consultation paper invited small firms to comment on the cost implications of the regulations on their business. A few small firms and two regional Chambers of Commerce responded to the consultation. They made clear that small businesses need to intercept for routine purposes such as ensuring the operation of their systems and keeping adequate records. However, none of the respondents was able to give a precise estimate of the costs complying with the regulations.

OTHER COSTS

None.

RESULTS OF CONSULTATIONS

The DTI conducted a public consultation exercise on the draft regulations from 1 August to 15 September 2000. Its proposals were based on Option B. It received over 80 consultation responses from businesses, charities, representative organisations and private individuals. During the same period, we held a large number of informal discussions with representative organisations including the Confederation of British Industry, the British Chamber of Commerce, the Information Security Forum, the Alliance for Electronic Business, the London Stock Exchange, the Financial Services Authority and the parliamentary lobby group EURIM. A summary of consultation responses and a

Response to Consultation have been published on the DTI website at <http://www.dti.gov.uk/cii/regulation.html> . These provide a detailed account of the issues raised by consultees and the steps we intend to take to address them. Businesses expressed concern about the compliance costs of informing third parties of interceptions and gaining consent for interceptions for quality control and staff training. Two respondents were able to provide an estimate of the costs of compliance with these requirements. We have quoted their estimates in Section 5 above.

SUMMARY AND RECOMMENDATIONS

Option A (Not to make any regulations)

This option would restrict to an unreasonable extent business practices regarding interception. It would inhibit a wide range of essential business practices such as keeping records of transactions and ensuring the operation of modern communications systems. It might lead to some companies relocating outside the UK.

Option B (Regulations allowing essential interceptions; business to inform staff and third parties)

This option would allow businesses to make essential interceptions without consent. However, the requirement to inform third parties of interceptions would impose significant costs. The requirement to gain consent for interceptions for quality control would also impose costs and might in some cases have an adverse effect on service standards.

Option C (Regulations allowing interceptions for essential and quality control purposes; businesses to inform staff.)

This option would allow businesses to make interceptions for essential evidentiary and operational purposes without consent. It would also allow businesses to intercept without consent in order to monitor service standards. It would require businesses to inform staff but not third parties that interceptions might take place.

The consultation exercise indicates that this option would allow businesses to continue legitimate practices without being burdened with significant additional costs. The requirement to inform employees of interceptions would minimise the danger of personal calls being monitored without their knowledge. The provision for businesses to monitor communications for quality control would help to ensure high service standards for the benefit of consumers.

Option D (Regulations authorising all interceptions; businesses not required to inform staff or third parties)

This option would be in breach of the Telecoms Data Protection Directive.

Conclusion

Option C is the recommended approach. This will allow businesses to continue legitimate business practices without needing to overhaul equipment or procedures. However, it will require businesses to gain consent before interceptions for non-essential purposes such as marketing and market research. It will safeguard privacy by ensuring that staff are aware of their employers' practices regarding interception.

ENFORCEMENT, SANCTIONS, MONITORING AND REVIEW

Section 1(3) of the Regulation of Investigatory Powers Act 2000 will introduce a tort of unlawful interception on a private telecoms system by the operator of that system. The effect of this is that if a business unlawfully intercepts communications on its own network, individuals who suffer a loss as result of the interception will be able to sue for damages. The regulations will not in themselves be enforceable. They will not impose an obligation on business but will reduce the need to gain consent for interceptions under section 3(1) of the Regulation of Investigatory Powers Act. The DTI intends to review the Regulations after twelve months from their entry into force or, if later, after the adoption of the revised Telecoms Data Protection Directive proposed to the EU Council by the EC Commission in July 2000.

REGULATORY QUALITY

Declaration. I have read the Regulatory Impact Assessment and I am satisfied that the balance between cost and benefit is the right one in the circumstances.

PATRICIA HEWITT

(Minister for Small Business and E. Commerce)

2. NOTES FOR BUSINESS

1. Introduction

The Regulation of Investigatory Powers Act 2000 establishes a new legal framework to govern the interception of communications. It sets the rules regarding activities such as recording, monitoring or diverting communications in the course of their transmission over a public or private telecoms system. The Act brings the interception activities of private businesses on their telecoms systems within the scope of regulation. If a business intercepts a communication on its system without legal authority, the sender or the recipient of the communication will be able to obtain an injunction or, if they can show that they suffered a loss as a result of the interception, sue for damages.

The Act establishes the circumstances in which it is lawful to intercept communications. It authorises interception in cases where the interceptor has reasonable grounds to believe that both the sender and intended recipient have consented. It also provides for the Secretary of State to make "Lawful Business Practice" Regulations setting out the circumstances in which businesses can lawfully intercept communications without consent. The Lawful Business Practice Regulations will allow businesses to intercept without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use, and ensuring the operation of their telecoms systems. Businesses will not need to gain consent before intercepting for these purposes although they will need to inform their staff that interceptions may take place. The new rules will come into force on 24 October 2000. These notes set out the purposes for which businesses will be able to intercept without consent under the regulations and the steps they should take to inform staff of these practices. The notes also set out some of the circumstances in which businesses would need to gain consent for interceptions and some of the steps they might take to ensure that this is achieved.

2. Purpose of these notes

These notes represent no more than the views of the DTI on the meaning of Part I of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. They are not exhaustive and have no legal force. They will not necessarily have any bearing on how the

courts interpret the new legislation. Businesses will need to consult the Act and the Regulations in order to ensure that their activities do not breach the new interception rules. They may need to take legal advice to ensure compliance.

3. Interceptions authorised under the Lawful Business Practice Regulations

The Regulations authorise businesses to monitor or record communications on their telecoms systems without consent for the following purposes:

A. To establish the existence of facts relevant to the business e.g. keeping records of transactions and other communications in cases where it is necessary or desirable to know the specific facts of the conversation.

B. To ascertain compliance with regulatory or self regulatory practices or procedures relevant to the business eg. monitoring as a means to check that the business is complying with regulatory or self regulatory rules or guidelines.

C. To ascertain or demonstrate standards which are or ought to be achieved by persons using the telecoms system e.g. monitoring for purposes of quality control or staff training.

D. To prevent or detect crime e.g. monitoring or recording to detect fraud or corruption.

E. To investigate or detect the unauthorised use of their telecoms systems e.g. monitoring to ensure that employees do not breach company rules regarding use of the telecoms system.

F. To ensure the effective operation of the system e.g. monitoring for viruses or other threats to the system; automated processes such as caching or load distribution. The Regulations also authorise businesses to monitor (but not record) without consent in the following cases:

G. For the purpose of determining whether or not they are communications relevant to the business e.g. checking email accounts to access business communications in staff absence.

H. In the case of communications to a confidential anonymous counselling or support helpline e.g. monitoring calls to confidential, welfare helplines in order to protect or support helpline staff.

4. Requirement to inform staff of interceptions made under the Regulations

If businesses intend to make interceptions without consent for the purposes authorised under the regulations, they are required to make all reasonable efforts to inform every person who may use their telecoms system that communications may be intercepted. e.g. Businesses could place a note in staff contracts or in other readily available literature informing staff that interceptions may take place. The persons who use a system are the people who make direct use of it. Someone who calls from outside, or who receives a call outside, using another system is not a user of the system on which the interception is made.

5. Interceptions outside the scope of the Regulations

If businesses wish to make interceptions for purposes outside the scope of the regulations, they will need to gain consent of the sender and the intended recipient of the communication. e.g. Interceptions for purposes such as marketing or market research; e.g. Interceptions for any other purposes that fall outside the list in Section 3 above.

6. Gaining consent for an interception outside the scope of the Regulations

The Regulation of Investigatory Powers Act authorises interceptions in cases where the interceptor has reasonable grounds to believe that he has the consent of both the sender and the intended recipient of the communication. If businesses need to intercept communications for purposes outside the scope of the Regulations, they could take a number of steps to ensure that they gain the consent of staff and outsiders:

e.g. the business could insert a clause in staff contracts by which employees consent to calls being monitored or recorded;

e.g. the call operator could ask outsiders at the start of a call whether they consented to their call being monitored or recorded;

e.g. the business could begin calls with a recorded message stating that calls might be monitored or recorded unless outsiders requested otherwise.

We believe that, as a minimum, a business would need to give outsiders a clear opportunity to refuse consent to interception and to be able to continue with the call.

7. Warning: The Data Protection Act 1998

Anybody who intercepts a communication will need to be sure that their actions are authorised under the Regulation of Investigatory Powers Act and comply with the requirements of the Data Protection Act 1998. The Lawful Business Practice Regulations make an exception to the rule established in the Regulation of Investigatory Powers Act that consent is needed before an interception can take place. If a business intercepted a communication in accordance with the Regulations, it would not risk civil liability under the Regulation of Investigatory Powers Act for unlawful interception. However, businesses should be aware that any interception which involves obtaining, recording or otherwise processing personal data by means of automated equipment (for example recording calls or filtering emails) also falls within the scope of the Data Protection Act 1998. So too does the holding or processing of personal data after the interception has taken place.

8. Further Information

For more information about the Lawful Business Practice Regulations visit the main pages on the DTI website

3. CONCLUSION

The Government is confident that the Lawful Business Practice Regulations will allow business to conduct most important monitoring or recording activities without needing to restructure practices and without undergoing significant costs. The Regulations should offer business the greatest possible scope for maximising the advantages of new ways of working with phone, email and other electronic communications, consistent with a high degree of privacy for the users of communications services. As such, they will contribute to the Government's aim of making the UK the best place for e-commerce by encouraging modern markets and confident consumers. The Lawful Business Practice Regulations and Section 1(3) of the Regulation of Investigatory Powers Act will come into force on 24 October 2000. The DTI intends to review the Regulations after twelve months from their entry into force or, if later, after the adoption of the revised Telecoms Data Protection Directive proposed to the EU Council by the EC Commission in July 2000.

4. CONSULTATION RESPONSES

Introduction

The DTI received 80 non-confidential responses to its consultation on the draft Lawful Business Practice Regulations. This document provides a list of the organisations and individuals who responded and a short summary of each consultation response.

The Consultation Paper for the draft Regulations invited respondents to provide their own non-confidential summary of comments for publication on the DTI website. Wherever possible, we have reproduced the summaries provided by consultees. In cases where consultees did not provide their own summary, the DTI has highlighted what it considers to be the most important comments in their responses.

List of Respondents to the Consultation

Aikin Driver Partnership
Alliance for Electronic Business
Association for Payment Clearing Services
Association of Chartered Certified Accountants
Birmingham Chamber of Commerce and Industry
British Airports Authority
British Bankers' Association
British Computer Society
British Petroleum
British Telecom
Mr M. F. Chenoweth
Clifford Chance
Colt Telecom
Computer Weekly
Consumer Congress
Corporation of London
Department of Social Security

Mr C. Dilloway
Direct Marketing Association
DLA (solicitors)
E Centre UK (draft response)
Peter Edwards (a Cornish Housing Association)
Mr E. Emecz
EURIM
Employment Lawyers Association
Faculty of Advocates
Federation of Small Business
Finance and Leasing Association
Financial Law Panel
Financial Services Authority
Forestry Commission
IBM
Independent Healthcare Association
Information Security Forum
Institute of Chartered Accountants of Scotland
Institute of Directors
Institute of the Management of Information Systems
Justice (Human Rights Organisation)
KPNQuest
Law Society of Scotland
Level 3 Communications
Dr C. H. Lindsey
LINX
London Investment Banking Association
London Underground
Manufacturing, Science and Finance Union
Magnetic North Software Ltd
Mortgage Group Ltd
National Crime Squad
National Electricity Consumers' Council

National Federation of Consumer Groups

National Union of Journalists

Natural Environment Research Council

Nestor Healthcare Group

Newspaper Society

Norwich Union

TG Pollard & Sons (solicitors)

Portsmouth and SE Hampshire Chamber of Commerce and Industry

Post Office

Premium Rate Association

Reuters

J Sainsbury plc

Samaritans

S4C

Scope

Scottish Advisory Committee on Telecommunications

Small Business Service

South East Employers

Standard Life

Telecoms Managers' Association

Telephone Helplines Association

Tensor plc

Thompsons Solicitors

Trades Union Congress

Trading Standards Institute

UK Information Security Forum

United Kingdom Education and Research Networking Association

University & Colleges Information Systems Association

U.S. Marine & Industrial Pump Repair

Vodafone

Aikin Driver Partnership (Employment Law Advisory Service)

Personal use of telecoms systems should be determined by the employer. Ofcom advice should be removed. The employer should be entitled to access to any communication without consent where the communication relates or appears to relate to the business or where the system has been provided for business purposes only. The employer will be aware that this is the case but there is less certainty that the correspondent will be aware. The correspondent will be aware if the employer has taken steps to bring this to his attention or if the mode of communication makes this obvious such as an email address including a business name. Consideration should be given to including in the regulations some marker which could be attached to telephone and other addresses which would indicate business only or subject to business intercept and recording. The correspondent should have to prove that reasonable steps had not been taken.

Alliance for Electronic Business

The regulations are too narrow in scope. The Regulation of Investigatory Powers Act and the regulations would, taken together, deny business day to day access to their own correspondence in the form of email or voicemail.

The regulations should authorise all interceptions relating to legitimate business activity such as monitoring, archiving and accessing relevant communications with the exception of specifically excluded practices.

The regulations should allow interceptions without consent for purposes such as quality control or staff training. For many types of electronic communication, it would be very difficult, even impossible, to gain consent for interceptions.

The combined impact of the Regulation of Investigatory Powers Act and the Regulations is likely to be significant. This will apply both to direct and indirect costs, and inconvenience as business has to adapt its procedures to permit the access it has been accustomed to in the past.

Association for Payment Clearing Services

APACS members have indicated broad support for the regulations and for the development of industry guidelines on interception in the financial services industry.

Association of Chartered Certified Accountants

The ACCA agrees with the scope of the regulations and that businesses should gain consent before intercepting communications for purposes such as staff training or quality control.

The regulations should only permit interceptions in cases where the purposes for the interception could not be achieved by other means.

Wide ranging regulations might lead to conflict with article 8(2) of the Convention on Human Rights. A general authorisation for employers to intercept without consent on the grounds of unauthorised use would be excessive on privacy grounds.

The cost burden of the regulations would not necessarily be significant.

Birmingham Chamber of Commerce and Industry (BCI)

On the whole, bearing in mind the constraints of the Telecommunications Data Protection Directive, those BCI members who responded to the consultation exercise are in agreement with the DTI's proposal, in relation to the draft Regulations on Lawful Business Practice regarding the Interception of Communications.

Generally, it is believed that allowing businesses to intercept communications without consent for essential evidentiary purposes is the right way forward, and it is not unreasonable that they should have grounds for believing that both correspondents and employees have consented to the interception, for the purposes of quality control, staff training and general marketing. Marketing research however, should perhaps be subject to more explicit consent of callers, before intercepting such communications.

In relation to guidelines, the BCI would urge the Government to "think small first" by developing guidelines that are specifically written for the convenient use of small businesses.

In conclusion, there is no doubt that there must be a balance between protecting the confidentiality of communication and the right to privacy, and the needs of businesses in respect of taking measures to prevent, investigate and detect criminal offences and unauthorised use of communications systems. The BCI is of the opinion that the draft Regulations on Lawful Business Practice regarding the Interception of Communications, do go some way towards ensuring that employers' interests are protected.

British Airports Authority

The government should advertise the circumstances under which calls may be recorded and there should be a general presumption that any call falling into these categories will be recorded.

In order to comply with the regulations, businesses may need to buy voice processing equipment at a cost of £30,000- £100,000. Businesses with such equipment may need to modify or reprogram it. The cost of advertising to one's customer base will vary from company to company.

Recorded messages would also extend the length of calls and the cost to the consumer.

British Bankers' Association

Monitoring/recording for training, quality control purposes, etc is routine in major call centres. "Quality control" can be used to ensure compliance. For example, in call centres staff are assessed on a number of criteria, including whether they adhere to certain elements of a script. Such adherence can be critical where it includes fair obtaining and disclosure notices, as necessary under the Data Protection Act. In addition institutions are required to comply with industry codes, for example the Banking Code. Expert dealing with customer complaints is important. A recorded conversation is there as an audit trail in respect of communication between bank and customer; it may also be used to teach staff, for example, in how to better deal with a customers complaint.

The Regulations need to stand-alone and provide the necessary clarity and legal certainty.

British Computer Society

The Data Protection Commissioner should be fully involved in implementing the Regulations and her formal powers should be extended accordingly. She should also be involved in the development of industry guidelines.

British Petroleum

The regulations need to cover instances where businesses have a legitimate need to access emails and recordings. It is inevitable that personal communications are occasionally intercepted. The regulations should allow interceptions for quality control. BP

agrees with the drafting approach but believes the regulations need to be complemented by industry guidelines. It does not believe that the regulations will impose significant costs.

British Telecom

The regulations should authorise interceptions for a wide range of evidentiary purposes including internal disciplinary investigations, ensuring compliance with internal procedures, staff training and market research. The regulations should allow businesses to check staff emails in their absence and in the course of internal disciplinary investigations. The regulations should make sure that businesses can intercept communications in order to protect against viruses or other harmful content.

It would be very difficult to inform all parties of interceptions or, in the case of interception activities outside the regulations, to gain consent. In certain circumstances these requirements would lead to significant costs. It is inappropriate to require businesses to inform callers when intercepting communication in order to detect crime.

As they stand, the regulations would impose major constraints and excessive costs.

M. F. Chenoweth (Private Individual)

The draft Regulations treat interception as a casual matter. Private communications should not be intercepted unless a crime is being committed.

Clifford Chance

The Telecoms Data Protection Directive fails to take account of business realities and technological developments. The Government should abandon implementation of Article 5 by 24 October and instead take the opportunity to influence the new draft Directive.

The scope of the regulations should be as wide as possible. The regulations should allow businesses to intercept all communications which take place during the course of a business's activities. The regulations must explicitly authorise interception for the purpose of determining whether a communication relates to the business. The regulations should allow interceptions without consent for a wide range of evidentiary purposes as well as for market research, marketing, staff training, quality control, disciplinary activities, investigating misconduct, access to communications in the absence of staff. The requirement to inform callers of interceptions is unworkable and should be removed.

Colt Telecom

The interception of communication without consent should be allowed for a wide range of legitimate business practices including staff training and quality control provided that certain defined steps have been taken by the interceptor to inform the correspondents to the communication that monitoring is taking place;

There is a need to define further what is meant by (a) "reasonable efforts" to be made by an interceptor in order to inform every person to whom or by whom the communication is made that it will or may be intercepted and (b) "reasonable grounds" to believe that every person is aware that communications are or may be intercepted;

There is a need to issue guidance notes in relation to the steps to be taken by employers to comply with the Regulations, particularly in relation to the use of e-mails. Such guidance notes should be drafted in consultation with all interested parties in the industry.

Computer Weekly

A number of IT Directors contributed to the Computer Weekly response. They expressed concern that businesses must be allowed full access to the communications that travel over their systems. Communications over a business's system should be considered to be the business's property. It is often impossible to distinguish between personal and business communications.

Consumer Congress

The regulations will give business an unfair advantage in disputes with consumers. Consumers should be made aware of the intention of businesses to intercept calls for whatever purpose. National standards should be set to govern interceptions by business.

Corporation of London

The scope of the regulations is too narrow. It would be very costly and difficult to gain consent before making interceptions for staff training etc. It is too early to say what the compliance costs will be. However, any imposition on industry would compromise UK competitiveness.

Department of Social Security

The regulations should make clear that interceptions for the purpose of disciplinary investigations are permitted. It is unclear how the regulations will fit with the Home Office Circular (HOC 15/1999) about interception on non-public networks. Guidance should be developed for Government Departments.

Cliff Dilloway (Private Individual)

The Computer Misuse Act 1990 makes unauthorised use of a (telecommunications) computer a crime. Preventing or detecting crime and investigating or detecting unauthorised use are permitted purposes of interceptions. Those permitted purposes allow the keeping of a record of business communications which term is defined in a practical way.

It would appear that as criminal (paedophile) material may be found on a computer and authorisation requirements under the Computer Misuse Act (para 17 (5)) are so strict the Draft Regulations do not effectively constrain any interception of business communications.

Direct Marketing Association

The regulations are too narrowly drafted and as such impose unnecessary constraints on business, particularly when read in conjunction with the notes in the consultation document, severely limiting the ability of companies to carry out their legitimate day-to-day business.

Call centres have legitimate business reasons for monitoring or recording telephone calls in order to maintain the high standards of performance expected in the telemarketing industry and to conduct disciplinary investigations.

The regulations as drafted would seem to deny business day-to-day access to their correspondence sent to and from the mail boxes of employees - the employer or another employee must be able to listen to an absent member of staff's telephone messages or look at their e-mails without having to obtain the consent of both parties.

The current system of implied consent for the monitoring or recording of live telephone calls should continue. This includes the activities listed in Q2 as well as other legitimate practices. The obtaining of consent for non-live communications is impractical and unnecessary.

Any necessary clarification should be included in the Regulations themselves rather than in additional guidelines. The Regulations focus too much on the right to privacy and do not achieve a balance with the need to facilitate essential, legitimate business practices. The impact of the Regulations is likely to be significant, both in terms of costs and inconvenience.

DLA (Solicitors)

Regulating the use of e-mail and Internet usage by employees , to ensure that excessive or inappropriate use is not commonplace. Employers have a duty to ensure that email systems and other telecoms systems are not misused to send racist, sexist or material. There are particular concerns about the misuse of Internet access to view pornographic websites in work time or the use of email to circulate pornographic material in the work place.

Businesses believe that the interception by employers of conversations between their staff and customers is for the protection of and for the benefit of all parties concerned as it helps to resolve disputes, it allows quality control and it assists in training.

Guidelines are necessary to explain what "reasonable grounds" means and what "reasonable efforts" are required.

E Centre UK

The regulations fail to take account of the differences between voice telephony on the one hand and internet, voicemail and email on the other. The privacy expectations of someone who communicates with a business via email or voice mail are less than those of someone who uses voice telephony. They are the same as those of someone who sends a letter in conventional post.

The regulations would not allow interceptions necessary for the day to day functioning of a business such as accessing staff mailboxes for email records. The regulations would not allow businesses to check communications, some of which might be personal, in order to find out whether they were related to the business.

The proposals take an unnecessarily wide interpretation of the Telecoms Data Protection Directive. In particular, the proposals assume that Article 5 of the Directive extends to the

interception on private networks of communications that have travelled on the public network.

The scope of the regulations should be widened. They should be generally permissive, identifying and excluding only those practices which are thought to be undesirable. The requirement to make all reasonable efforts to inform callers of interceptions is impossible to comply with and in some cases inappropriate.

The regulations should contain a general provision allowing interceptions to comply with legal obligations to produce information or documents.

Peter Edwards (Housing Association)

In order to maintain a high level of probity in the use of business communications by our staff, and also to protect our staff from unacceptable materials sent by others... monitoring of emails and Internet usage is a reasonable step for an employer to take both to protect itself and its staff. It is also reasonable for an employer to be able to monitor the standard of work of staff to inform training plans and decisions on work allocation.

We require staff to share communications, with activity-based open filing structures in which important emails are made accessible across workgroups.

E. Emezc (Private Individual)

The draft Regulations are geared towards telephone calls. They do not adequately distinguish between voice, email and internet communications. The regulations deal with monitoring and recording but do not refer to interceptions which block or delete communications.

The Regulations might have the effect of encouraging companies to ban staff use of the systems in order to avoid the danger of illegally intercepting private communications. The requirement to inform third parties of interceptions is unworkable for internet and email communications.

EURIM (Parliament-Industry Group)

The regulations need significant further work including consultation with the operators of call centres, help desks and e-commerce operations as well as those responsible for corporate voice and data networks. Businesses contacted to date are confused as to what

changes to current industry practice are intended and fear unintended dislocation and additional costs.

Their main concerns are:

- a) The definition of "business communications". When monitoring traffic over corporate networks it is impractical to discriminate before the event between private and business communications. The issue is how private communications are subsequently handled.
- b) There is a need to ensure that the Regulation does not conflict with other Regulations (especially in the financial services industry), codes of practice (such as the proposed email code of practice from the Office of the Data Protection Commissioner) and practices mandated as part of externally verified security and quality control procedures.
- c) The approach to consent appears impractical (e.g. for unsolicited calls or emails). Greater clarity is needed on when implied consent can be used - alternatives will be expensive, take time to implement and are unlikely to cover all types of communication.
- d) Businesses should be allowed to intercept communications not just for the additional reasons mentioned in the Consultation Paper (such as quality control, staff training and market research), but also for other business reasons such as internal discipline. Such uses for data are often included within the DPA registered purposes and appear to be included by the definitions in both the Telecoms Data Protection Directive and the Regulation of Investigatory Powers Act.
- e) The implementation of any changes in business operation will take time and effort to implement. A transition period is needed over which this can happen, and other work, such as the development of any supporting Industry Codes of Practice and of alternative forms of obtaining consent, can be undertaken.

Employment Lawyers Association

The regulations might allow for broader interpretation than the Government intends. Various terms require more precise definition. The requirement to inform callers of interceptions will place a high burden on business and will be difficult to comply with in certain cases. The Government needs to clarify the circumstances in which an interceptor would have reasonable grounds to believe they had consent for an interception. The Government needs to clarify the circumstances in which an interception would be deemed to be effected in the UK.

Faculty of Advocates

In paragraph 2 of the draft regulations, "business" is defined so as to include the activities of a "Government Department, or any public authority, or of any personal office holder on whom functions are conferred by or under any enactment..." It is not clear that the structure of the Regulations properly has regard to the provisions of the Directive in that the ability of a Government Department, public authority etc., to intercept communications in terms of paragraph 3(1)(a)(iv) would appear to extend beyond what would normally be considered to be the kind of commercial context envisaged in article 9(2) of the Directive. Although there is a convincing case given in the Consultation Paper as to why such interception of communications may be desirable, it is not clear that it would be authorised by article 5(2) of the Directive, the problem being that it would at least be open to interpretation by the Courts as to whether advice sought by an individual and without payment would properly fall within the definition of "business."

The Faculty agrees that a "broad-brush" approach does have the necessary flexibility and welcomes the use of Regulations to lay down general principles rather than to attempt minute and rigid regulation. It will, of course, be appreciated that such an approach may lead to a greater involvement by the courts in the interpretation and development of the principles in their application to individual cases.

Federation of Small Business

The FSB fundamentally supports the aims of the legislation and recognises that there is a careful balance to be struck between respecting personal privacy on the one hand and the needs of business to provide evidence of a communication which records a commercial transaction on the other. However, it has reservations that the broad-brush approach envisaged but the draft legislation may lead to problems in the future due to their imprecise nature and feels that additional clarification, especially with regard to online privacy while using the internet, would prevent speculative and malicious court action being taken against businesses.

Finance and Leasing Association

Agree that the correct balance has been struck to allow for businesses to protect themselves against possible security risks and facilitate business transactions. It seems

reasonable in situations where the purpose of the interception is not directly related to the business transaction or necessary for evidentiary purposes that reasonable steps have been taken to ensure that the customer consents.

Suggest that consideration is given to specialist money advice lines which can act on behalf of the customer. Generally, individuals in the UK take a practical stance towards privacy which would seem to be well reflected in the Regulations. At this stage it would be difficult to quantify the costs of implementation without further clarifications. A process of notification could be potentially straightforward for business, whereas the obtaining, recording and processing of express consent would be costly

Financial Law Panel

The practice of taping telephone calls is recognised as sound business practice throughout the financial industry and would probably continue even if it were not required or recommended by the regulatory regime. The regulations should be designed to cater not only for the regulatory structure as it currently applies but also for any variations that occur as it evolves.

Financial Services Authority

FSA does not at present require regulated firms to tape calls as a means of meeting record keeping or other regulatory requirements, although this is subject to review as the Handbook develops. However, FSA's proposed Inter-Professionals Code does identify taping as a practice which can usefully assist in deal capture and dispute resolution. Views of the industry have been sought on whether further rules in this area would be helpful. As indicated above, many firms which operate telesales units, or similar, record calls for quality control and staff training purposes. As currently drafted, therefore, the Regulations will impose a new obligation on these firms to obtain the consent of those involved in order to be able to continue with this practice.

Although quality control is listed as an activity which does not fall within the scope of the draft Regulations, we believe that it is a grey area, which overlaps with interception for the authorised purpose of ensuring compliance with practices and procedures.

The ambiguity around whether quality control in certain circumstances could be regarded as authorised is undesirable. From a practical, supervisory point of view, it is not clear how

FSA will distinguish between firms' interception of calls for authorised regulatory compliance purposes and interception for other quality control purposes.

Interception for quality control and staff training purposes is ultimately undertaken to benefit and protect consumers in ensuring competent staff are communicating relevant and appropriate information at the right time. In this respect, they differ from interception for marketing or market research purposes, where the benefit more obviously accrues to the firm.

Forestry Commission

The Commission welcomes the regulations. It agrees with the scope of the regulations and does not anticipate significant implementation costs. It would support the development of additional guidance.

IBM

Businesses should be authorised to intercept communications for staff training or quality control purposes without consent providing such activities are conducted within certain safeguards.

It might be very difficult to ensure the consent of staff before making interceptions for these purposes, particularly in the case of contracted staff.

Independent Healthcare Association

Whilst supporting the Regulations in general terms, IHA has concerns over the medical confidentiality of patients and residents of care homes; and also over the need to obtain consent from the sender of an email to permit the content checking of emails to protect both employees and organisations from offensive emails.

Information Security Forum

Consolidated guidelines are needed to make sure that organisations do not break the law accidentally or spend unnecessarily large sums of money to ensure compliance.

All organisations take security copies of email data for contingency purposes. They need to be able to continue doing this in future.

It would not be logical to seek consent or inform callers when recording calls in order to gain evidence of bomb threats or abusive behaviour.

The Telecoms Data Protection Directive is inadequately drafted because it does not differentiate between telephone communications and email.

The Regulations and guidelines need to be very clear in order to ensure that the possibility of misinterpretation in the courts is reduced to a minimum.

Institute of Chartered Accountants of Scotland

The Regulations should give businesses the right to intercept communications to a business number. This would avoid the need to include a pre-recorded warning and thus save callers' time. Contracts of employment should state that the business has the right to monitor communications and businesses should be required to state that calls may be monitored in their advertising. Employees should be given clear information on what is and is not permitted.

Institute of Directors

It is possible that the Government has chosen to interpret the Telecoms Data Protection Directive too liberally. It is not clear whether the Directive applies to email systems maintained and paid for by the private sector.

The regulations need to make clear that employers can check emails of absent employees. The regulations should allow businesses to intercept communications for purposes such as staff training and market research provided that they have made receivers and callers aware that interceptions may take place.

Further clarification of the Regulations may be necessary. However, allowing particular sectors to generate their own rules might result in a series of conflicting guidelines. It would be preferable to develop an overarching set of guidelines after a wide ranging consultation process.

There is a real danger of the Regulations adding to the climate of uncertainty and driving some business activities off-shore.

Clarification is needed on whether basic steps to protect a company's legal position, such as employee contract of employment clauses authorising the use of routine monitoring

within corporate networks would be deemed lawful in the context of the European Convention on Human Rights.

Institute of the Management of Information Systems

The Telecoms Data Protection Directive was drafted many years ago. It was not until the first round of DTI consultation over implementation (a year ago) that officials in London and Brussels began to appreciate that it might apply to e-mail and the Internet.

More-over the regulations can be readily bypassed by basing monitoring facilities outside the EU. In consequence, unless the regulations are drafted and implemented in such a way as to give businesses confidence that they need make little, if any, change to current practice, the effect will be to increase the pace of relocation of current e-commerce operations (from ISP and Internet hubs to Call Centres) to outside the UK/EU.

Organisations are liable for traffic over their voice and data networks under a wide variety of legislation. Those who do not routinely monitor traffic run an equally wide variety of legal and business risks. The IMIS guidelines in this area (based on the policies of many large and well-run UK and US organisations) are attached as an Appendix.

The integrated nature of monitoring products and services and the rate of change mean that attempts to define and distinguish between the range of business reasons are, in practice, unrealistic. The "store and forward" nature of modern communications networks makes the distinction between on-line monitoring and the subsequent analysis of recorded traffic similarly unrealistic. The use of records of traffic is a more significant issue. But declarations of the reasons for which this is held have long been covered under UK Data Protection legislation and it is unclear what change, if any, is intended or needed.

Any DTI Regulations should permit organisations to state simply and clearly in their contracts of employment that all communications (voice and data) over their voice and data networks are routinely monitored and recorded for legal, quality control and other business purposes and that those wishing unmonitored personal communications should use non-corporate facilities such as personally-owned mobiles or external facilities in rest areas.

Similarly, any DTI regulations should enable organisations to state simply and clearly in contracts, terms of trade, advertisements and on websites that all communications over corporate networks and switchboards are routinely monitored and that those wishing

personal and unmonitored communications should ask the relevant member of staff to contact them over non-corporate facilities.

There should be no further requirement to change existing ways of doing business. In particular there should be no requirement for explicit statements in response to all incoming traffic or prefacing all-outgoing traffic if the organisation's policy is clearly and publicly stated in advertisements and contracts.

Justice (Human Rights Organisation)

The scope of the regulations is too broad. The provisions to allow businesses to intercept "to establish the existence of facts" and to "detect unauthorised use" might be used by employers to justify a range of intrusive interceptions and there is no requirement for employers to examine issues of necessity and proportionality. Businesses should not be allowed to intercept to detect crime as this is the responsibility of the law enforcement agencies. The absence of any specific restriction on interception of legally privileged material also raises questions of compliance with ECHR standards.

Justice believes that interceptors should have a duty to inform correspondents of interceptions before they take place. Employers should be required to consult with employees before interception procedures are implemented. Industry guidelines should be developed to ensure consistency and should include the recommendations made by the EU Data Protection Commissioners on telecoms and privacy in labour relations.

KPNQuest

The regulations should allow interceptions for a broader range of purposes. It agrees that highly detailed regulations would be impracticable and favours industry-led action to clarify the regulations. It agrees that the regulations should not impose a significant burden on business.

Law Society of Scotland

The Society agrees with the scope of the regulations and that a fair balance has been achieved between the protection of privacy and legitimate business practices. It agrees with the broad drafting of the regulations but suggests that the definition of "business"

should be more precisely defined. It believes that commercial as well as charitable helplines should be able to monitor calls in order to protect staff.

Level 3 Communications

Level 3 agrees with the scope and approach of the regulations but suggests that more information is needed to make a clear assessment of the costs to business. It would need to install new technology to implement the regulations.

Dr C. H. Lindsey (Private Individual)

The scope of the draft regulations is too narrow. The regulations have been drafted with voice calls in mind and are inappropriate for fax or email.

LINX (ISP Partnership)

The regulations may unintentionally prohibit routine interceptions which would not commonly be regarded as an invasion of privacy such as SPAM or virus filters or email forwarding systems.

London Investment Banking Association

It is important that the Regulations are broadly enough drafted to permit financial services firms to continue with current practices which are required or necessary to exercise effective control over their businesses, and to enable them to comply with regulatory obligations or regulators' published 'expectations' by recording and monitoring communications with or on behalf of the firm or using its facilities. We welcome in particular draft Regulation 3(1)(a)(iii), and also the intention behind draft Regulation 3(1)(b), although in the latter case we believe that redrafting is required to avoid ambiguity. LIBA would like resolution of the following points:

The wording of Regulations 2(f) and 3(1)(a)(iv) permits interception to ascertain compliance with regulatory practices and procedures which are imposed on the firm. This wording should be extended to cover compliance by firms with regulatory practices and procedures which are expected or recommended by regulators or auditors.

The DTI has stated in the consultation document that the Regulations currently exclude interception for the facilitation of training. In financial services, however, maintenance of

competence is a regulatory obligation. It should be made clear that the Regulations allow interception in connection with training where the purpose of the interception is to help satisfy a regulatory obligation. If this is covered by Regulation 3(1), it may be that no specific drafting change is required to the Regulations themselves beyond that identified in the first point above.

Employees, agents, customers and counterparties of financial services firms expect and understand that communications are routinely recorded. Where this is clear, it should be the case that Regulation 3(2)(c)(i)(bb) is satisfied. In any event, a statement in employment contracts and customer terms of business that communications may be intercepted should satisfy Regulation 3(2)(c)(i)(aa). If anything more than this is envisaged, the cost implications could be significant, and the DTI should consult further.

London Underground

It is possible that a business might inadvertently intercept private communications over its network. The Regulations should make allowance for this.

It is not clear what will constitute "all reasonable efforts to inform correspondents that the communication will be intercepted". It is easy to ensure that employees are aware but not customers, job applicants, contractors etc.

Manufacturing, Science and Finance Union

MSF supports the need for regulation covering the interception and monitoring of communications at work as part of our desire to safeguard the confidentiality of communications and the right of personal privacy including privacy at work.

The draft Regulations as proposed have insufficient regard to the need for proportionality between the nature of a lawful business practice presently defined in the draft Regulations and the permitted invasion of privacy.

We do not consider that the Regulations as currently proposed take sufficient account of the over-riding aim and need to protect the confidentiality of communications and the right to privacy.

The wording of the Regulations in providing legal rights to intercept communication without user consent is in our view too unspecific and imprecise to meet the requirements of the Directive. In particular the scope for employer self-determination provided by Regulation

3(1)(a)(iii) and the lack of specificity in defining the scope of the first part of Regulation 3(1)(a)(iv) would provide the potential for indiscriminate or arbitrary interception and monitoring of employee communication. Regulations 3(1)(a)(iii) and 3(1)(a)(iv) should be more tightly worded to reflect the aims of the Directive.

We believe that as currently drafted the Regulations in providing legal rights to intercept communication without user consent may be open to legal challenge in not meeting the obligations of confidentiality of communications and protection of personal privacy in accordance with EC Directive 97/66 and its forthcoming successor and the European Convention for the Protection of Human Rights and Fundamental Freedoms as enacted in the Human Rights Act.

With the aim of enabling the operation of the Regulations to reflect sectoral circumstances whilst according with the objectives of the Directive, we propose that the Regulations should provide for the use of workplace agreements along the lines of the MSF Model e-Facilities Agreement and draft Code of Practice on Protection of Privacy at Work.

Magnetic North Software Ltd

Call centres need to be able to monitor calls without consent for training and quality control purposes. If call centres were required to gain consent before monitoring for these purposes, that would result in a lowering of service standards and a deterioration in staff training.

The Mortgage Group Ltd

The Mortgage Group Limited engages in telephone marketing and monitors calls for quality control and training purposes. The Company will not be able to take advantage of the Lawful Business Practice Regulations in their current form and will therefore be forced to obtain full consent as required by the Regulation of Investigatory Powers Act 2000. It is believed that the process of obtaining consent in the early stages of outbound telephone calls will reduce the efficiency of the telemarketing process. It is further believed that the Act does nothing whatsoever to enhance the confidentiality of the information provided by potential customers as this is already carefully regulated. Without an appropriate derogation in the Regulations the new law will simply impose a burden on the operation of

the business with attendant costs and provide no benefit at all to those individuals the Company's marketing operation contacts.

The Mortgage Group Limited therefore urges the government to extend the scope of the Regulations to exclude the monitoring of calls for staff training and quality control from the Act.

National Crime Squad

The National Crime Squad agrees with the scope of the regulations insofar as they impact on its capability to maintain professional standards. Given the clarity of the regulations, the NCS is not convinced that further guidance will be necessary. However, it would be willing to participate in the development of such codes.

The regulations should allow the emergency services to continue to record calls for a broad range of evidentiary purposes beyond the pursuit of criminal prosecutions.

National Electricity Consumers Council

The regulations appear to allow business, but not consumers, to intercept communications in order to collect evidence of conversations. If this is the case, the effect would be to give business an unfair advantage in civil law, ADR and arbitration cases, businesses will be treated more favourably than consumers.

National Federation of Consumer Groups

The regulations are too broadly drafted and allow business excessively wide scope to intercept communications without consent. The regulations do not take sufficient account of the need to protect confidentiality and the right to privacy.

National Union of Journalists

Many employers impose contractual terms on employees which give them the right to monitor communications. However, in many cases, there is no real need to monitor and this is simply a further method of control.

The Government should consider making provision in the regulations for employers and employees to agree on levels of surveillance through collective bargaining.

Natural Environmental Research Council

The Regulations should explicitly permit businesses to presume that persons who communicate with them are aware that their communications may be intercepted without consent for the purposes of preventing or detecting crime and investigating or detecting unauthorised use. The alternatives either make legitimate interception impractical or impose an unnecessary burden on businesses.

Employment Lawyers Association

The regulations might allow for broader interpretation than the Government intends. Various terms require more precise definition. The requirement to inform callers of interceptions will place a high burden on business and will be difficult to comply with in certain cases. The Government needs to clarify the circumstances in which an interceptor would have reasonable grounds to believe they had consent for an interception. The Government needs to clarify the circumstances in which an interception would be deemed to be effected in the UK.

Faculty of Advocates

In paragraph 2 of the draft regulations, "business" is defined so as to include the activities of a "Government Department, or any public authority, or of any personal office holder on whom functions are conferred by or under any enactment..." It is not clear that the structure of the Regulations properly has regard to the provisions of the Directive in that the ability of a Government Department, public authority etc., to intercept communications in terms of paragraph 3(1)(a)(iv) would appear to extend beyond what would normally be considered to be the kind of commercial context envisaged in article 9(2) of the Directive. Although there is a convincing case given in the Consultation Paper as to why such interception of communications may be desirable, it is not clear that it would be authorised by article 5(2) of the Directive, the problem being that it would at least be open to interpretation by the Courts as to whether advice sought by an individual and without payment would properly fall within the definition of "business."

The Faculty agrees that a "broad-brush" approach does have the necessary flexibility and welcomes the use of Regulations to lay down general principles rather than to attempt

minute and rigid regulation. It will, of course, be appreciated that such an approach may lead to a greater involvement by the courts in the interpretation and development of the principles in their application to individual cases.

Federation of Small Business

The FSB fundamentally supports the aims of the legislation and recognises that there is a careful balance to be struck between respecting personal privacy on the one hand and the needs of business to provide evidence of a communication which records a commercial transaction on the other. However, it has reservations that the broad-brush approach envisaged but the draft legislation may lead to problems in the future due to their imprecise nature and feels that additional clarification, especially with regard to online privacy while using the internet, would prevent speculative and malicious court action being taken against businesses.

Finance and Leasing Association

Agree that the correct balance has been struck to allow for businesses to protect themselves against possible security risks and facilitate business transactions. It seems reasonable in situations where the purpose of the interception is not directly related to the business transaction or necessary for evidentiary purposes that reasonable steps have been taken to ensure that the customer consents.

Suggest that consideration is given to specialist money advice lines which can act on behalf of the customer. Generally, individuals in the UK take a practical stance towards privacy which would seem to be well reflected in the Regulations. At this stage it would be difficult to quantify the costs of implementation without further clarifications. A process of notification could be potentially straightforward for business, whereas the obtaining, recording and processing of express consent would be costly

Financial Law Panel

The practice of taping telephone calls is recognised as sound business practice throughout the financial industry and would probably continue even if it were not required or recommended by the regulatory regime. The regulations should be designed to cater not

only for the regulatory structure as it currently applies but also for any variations that occur as it evolves.

Financial Services Authority

FSA does not at present require regulated firms to tape calls as a means of meeting record keeping or other regulatory requirements, although this is subject to review as the Handbook develops. However, FSA's proposed Inter-Professionals Code does identify taping as a practice which can usefully assist in deal capture and dispute resolution. Views of the industry have been sought on whether further rules in this area would be helpful. As indicated above, many firms which operate telesales units, or similar, record calls for quality control and staff training purposes. As currently drafted, therefore, the Regulations will impose a new obligation on these firms to obtain the consent of those involved in order to be able to continue with this practice.

Although quality control is listed as an activity which does not fall within the scope of the draft Regulations, we believe that it is a grey area, which overlaps with interception for the authorised purpose of ensuring compliance with practices and procedures.

The ambiguity around whether quality control in certain circumstances could be regarded as authorised is undesirable. From a practical, supervisory point of view, it is not clear how FSA will distinguish between firms' interception of calls for authorised regulatory compliance purposes and interception for other quality control purposes.

Interception for quality control and staff training purposes is ultimately undertaken to benefit and protect consumers in ensuring competent staff are communicating relevant and appropriate information at the right time. In this respect, they differ from interception for marketing or market research purposes, where the benefit more obviously accrues to the firm.

Forestry Commission

The Commission welcomes the regulations. It agrees with the scope of the regulations and does not anticipate significant implementation costs. It would support the development of additional guidance.

IBM

Businesses should be authorised to intercept communications for staff training or quality control purposes without consent providing such activities are conducted within certain safeguards.

It might be very difficult to ensure the consent of staff before making interceptions for these purposes, particularly in the case of contracted staff.

Independent Healthcare Association

Whilst supporting the Regulations in general terms, IHA has concerns over the medical confidentiality of patients and residents of care homes; and also over the need to obtain consent from the sender of an email to permit the content checking of emails to protect both employees and organisations from offensive emails.

Information Security Forum

Consolidated guidelines are needed to make sure that organisations do not break the law accidentally or spend unnecessarily large sums of money to ensure compliance.

All organisations take security copies of email data for contingency purposes. They need to be able to continue doing this in future.

It would not be logical to seek consent or inform callers when recording calls in order to gain evidence of bomb threats or abusive behaviour.

The Telecoms Data Protection Directive is inadequately drafted because it does not differentiate between telephone communications and email.

The Regulations and guidelines need to be very clear in order to ensure that the possibility of misinterpretation in the courts is reduced to a minimum.

Institute of Chartered Accountants of Scotland

The Regulations should give businesses the right to intercept communications to a business number. This would avoid the need to include a pre-recorded warning and thus save callers' time. Contracts of employment should state that the business has the right to monitor communications and businesses should be required to state that calls may be

monitored in their advertising. Employees should be given clear information on what is and is not permitted.

Institute of Directors

It is possible that the Government has chosen to interpret the Telecoms Data Protection Directive too liberally. It is not clear whether the Directive applies to email systems maintained and paid for by the private sector.

The regulations need to make clear that employers can check emails of absent employees. The regulations should allow businesses to intercept communications for purposes such as staff training and market research provided that they have made receivers and callers aware that interceptions may take place.

Further clarification of the Regulations may be necessary. However, allowing particular sectors to generate their own rules might result in a series of conflicting guidelines. It would be preferable to develop an overarching set of guidelines after a wide ranging consultation process.

There is a real danger of the Regulations adding to the climate of uncertainty and driving some business activities off-shore.

Clarification is needed on whether basic steps to protect a company's legal position, such as employee contract of employment clauses authorising the use of routine monitoring within corporate networks would be deemed lawful in the context of the European Convention on Human Rights.

Institute of the Management of Information Systems

The Telecoms Data Protection Directive was drafted many years ago. It was not until the first round of DTI consultation over implementation (a year ago) that officials in London and Brussels began to appreciate that it might apply to e-mail and the Internet.

More-over the regulations can be readily bypassed by basing monitoring facilities outside the EU. In consequence, unless the regulations are drafted and implemented in such a way as to give businesses confidence that they need make little, if any, change to current practice, the effect will be to increase the pace of relocation of current e-commerce operations (from ISP and Internet hubs to Call Centres) to outside the UK/EU.

Organisations are liable for traffic over their voice and data networks under a wide variety of legislation. Those who do not routinely monitor traffic run an equally wide variety of legal and business risks. The IMIS guidelines in this area (based on the policies of many large and well-run UK and US organisations) are attached as an Appendix.

The integrated nature of monitoring products and services and the rate of change mean that attempts to define and distinguish between the range of business reasons are, in practice, unrealistic. The "store and forward" nature of modern communications networks makes the distinction between on-line monitoring and the subsequent analysis of recorded traffic similarly unrealistic. The use of records of traffic is a more significant issue. But declarations of the reasons for which this is held have long been covered under UK Data Protection legislation and it is unclear what change, if any, is intended or needed.

Any DTI Regulations should permit organisations to state simply and clearly in their contracts of employment that all communications (voice and data) over their voice and data networks are routinely monitored and recorded for legal, quality control and other business purposes and that those wishing unmonitored personal communications should use non-corporate facilities such as personally-owned mobiles or external facilities in rest areas.

Similarly, any DTI regulations should enable organisations to state simply and clearly in contracts, terms of trade, advertisements and on websites that all communications over corporate networks and switchboards are routinely monitored and that those wishing personal and unmonitored communications should ask the relevant member of staff to contact them over non-corporate facilities.

There should be no further requirement to change existing ways of doing business. In particular there should be no requirement for explicit statements in response to all incoming traffic or prefacing all-outgoing traffic if the organisation's policy is clearly and publicly stated in advertisements and contracts.

Justice (Human Rights Organisation)

The scope of the regulations is too broad. The provisions to allow businesses to intercept "to establish the existence of facts" and to "detect unauthorised use" might be used by employers to justify a range of intrusive interceptions and there is no requirement for employers to examine issues of necessity and proportionality. Businesses should not be allowed to intercept to detect crime as this is the responsibility of the law enforcement

agencies. The absence of any specific restriction on interception of legally privileged material also raises questions of compliance with ECHR standards.

Justice believes that interceptors should have a duty to inform correspondents of interceptions before they take place. Employers should be required to consult with employees before interception procedures are implemented. Industry guidelines should be developed to ensure consistency and should include the recommendations made by the EU Data Protection Commissioners on telecoms and privacy in labour relations.

KPNQuest

The regulations should allow interceptions for a broader range of purposes. It agrees that highly detailed regulations would be impracticable and favours industry-led action to clarify the regulations. It agrees that the regulations should not impose a significant burden on business.

Law Society of Scotland

The Society agrees with the scope of the regulations and that a fair balance has been achieved between the protection of privacy and legitimate business practices. It agrees with the broad drafting of the regulations but suggests that the definition of "business" should be more precisely defined. It believes that commercial as well as charitable helplines should be able to monitor calls in order to protect staff.

Level 3 Communications

Level 3 agrees with the scope and approach of the regulations but suggests that more information is needed to make a clear assessment of the costs to business. It would need to install new technology to implement the regulations.

Dr C. H. Lindsey (Private Individual)

The scope of the draft regulations is too narrow. The regulations have been drafted with voice calls in mind and are inappropriate for fax or email.

LINX (ISP Partnership)

The regulations may unintentionally prohibit routine interceptions which would not commonly be regarded as an invasion of privacy such as SPAM or virus filters or email forwarding systems.

London Investment Banking Association

It is important that the Regulations are broadly enough drafted to permit financial services firms to continue with current practices which are required or necessary to exercise effective control over their businesses, and to enable them to comply with regulatory obligations or regulators' published 'expectations' by recording and monitoring communications with or on behalf of the firm or using its facilities. We welcome in particular draft Regulation 3(1)(a)(iii), and also the intention behind draft Regulation 3(1)(b), although in the latter case we believe that redrafting is required to avoid ambiguity. LIBA would like resolution of the following points:

The wording of Regulations 2(f) and 3(1)(a)(iv) permits interception to ascertain compliance with regulatory practices and procedures which are imposed on the firm. This wording should be extended to cover compliance by firms with regulatory practices and procedures which are expected or recommended by regulators or auditors.

The DTI has stated in the consultation document that the Regulations currently exclude interception for the facilitation of training. In financial services, however, maintenance of competence is a regulatory obligation. It should be made clear that the Regulations allow interception in connection with training where the purpose of the interception is to help satisfy a regulatory obligation. If this is covered by Regulation 3(1), it may be that no specific drafting change is required to the Regulations themselves beyond that identified in the first point above.

Employees, agents, customers and counterparties of financial services firms expect and understand that communications are routinely recorded. Where this is clear, it should be the case that Regulation 3(2)(c)(i)(bb) is satisfied. In any event, a statement in employment contracts and customer terms of business that communications may be intercepted should satisfy Regulation 3(2)(c)(i)(aa). If anything more than this is envisaged, the cost implications could be significant, and the DTI should consult further.

London Underground

It is possible that a business might inadvertently intercept private communications over its network. The Regulations should make allowance for this.

It is not clear what will constitute "all reasonable efforts to inform correspondents that the communication will be intercepted". It is easy to ensure that employees are aware but not customers, job applicants, contractors etc.

Manufacturing, Science and Finance Union

MSF supports the need for regulation covering the interception and monitoring of communications at work as part of our desire to safeguard the confidentiality of communications and the right of personal privacy including privacy at work.

The draft Regulations as proposed have insufficient regard to the need for proportionality between the nature of a lawful business practice presently defined in the draft Regulations and the permitted invasion of privacy.

We do not consider that the Regulations as currently proposed take sufficient account of the over-riding aim and need to protect the confidentiality of communications and the right to privacy.

The wording of the Regulations in providing legal rights to intercept communication without user consent is in our view too unspecific and imprecise to meet the requirements of the Directive. In particular the scope for employer self-determination provided by Regulation 3(1)(a)(iii) and the lack of specificity in defining the scope of the first part of Regulation 3(1)(a)(iv) would provide the potential for indiscriminate or arbitrary interception and monitoring of employee communication. Regulations 3(1)(a)(iii) and 3(1)(a)(iv) should be more tightly worded to reflect the aims of the Directive.

We believe that as currently drafted the Regulations in providing legal rights to intercept communication without user consent may be open to legal challenge in not meeting the obligations of confidentiality of communications and protection of personal privacy in accordance with EC Directive 97/66 and its forthcoming successor and the European Convention for the Protection of Human Rights and Fundamental Freedoms as enacted in the Human Rights Act.

With the aim of enabling the operation of the Regulations to reflect sectoral circumstances whilst according with the objectives of the Directive, we propose that the Regulations should provide for the use of workplace agreements along the lines of the MSF Model e-Facilities Agreement and draft Code of Practice on Protection of Privacy at Work.

Magnetic North Software Ltd

Call centres need to be able to monitor calls without consent for training and quality control purposes. If call centres were required to gain consent before monitoring for these purposes, that would result in a lowering of service standards and a deterioration in staff training.

The Mortgage Group Ltd

The Mortgage Group Limited engages in telephone marketing and monitors calls for quality control and training purposes. The Company will not be able to take advantage of the Lawful Business Practice Regulations in their current form and will therefore be forced to obtain full consent as required by the Regulation of Investigatory Powers Act 2000. It is believed that the process of obtaining consent in the early stages of outbound telephone calls will reduce the efficiency of the telemarketing process. It is further believed that the Act does nothing whatsoever to enhance the confidentiality of the information provided by potential customers as this is already carefully regulated. Without an appropriate derogation in the Regulations the new law will simply impose a burden on the operation of the business with attendant costs and provide no benefit at all to those individuals the Company's marketing operation contacts.

The Mortgage Group Limited therefore urges the government to extend the scope of the Regulations to exclude the monitoring of calls for staff training and quality control from the Act.

National Crime Squad

The National Crime Squad agrees with the scope of the regulations insofar as they impact on its capability to maintain professional standards. Given the clarity of the regulations, the NCS is not convinced that further guidance will be necessary. However, it would be willing to participate in the development of such codes.

The regulations should allow the emergency services to continue to record calls for a broad range of evidentiary purposes beyond the pursuit of criminal prosecutions.

National Electricity Consumers Council

The regulations appear to allow business, but not consumers, to intercept communications in order to collect evidence of conversations. If this is the case, the effect would be to give business an unfair advantage in civil law, ADR and arbitration cases, businesses will be treated more favourably than consumers.

National Federation of Consumer Groups

The regulations are too broadly drafted and allow business excessively wide scope to intercept communications without consent. The regulations do not take sufficient account of the need to protect confidentiality and the right to privacy.

National Union of Journalists

Many employers impose contractual terms on employees which give them the right to monitor communications. However, in many cases, there is no real need to monitor and this is simply a further method of control.

The Government should consider making provision in the regulations for employers and employees to agree on levels of surveillance through collective bargaining.

Natural Environmental Research Council

The Regulations should explicitly permit businesses to presume that persons who communicate with them are aware that their communications may be intercepted without consent for the purposes of preventing or detecting crime and investigating or detecting unauthorised use. The alternatives either make legitimate interception impractical or impose an unnecessary burden on businesses.

5. SUMMARY

The Telecommunications Data Protection Directive requires Member States to protect the confidentiality of communications made by means of a public telecommunications network. The interception of communications on a public telecoms network is prohibited in the UK under the Interception of Communications Act 1985. The Regulation of Investigatory Powers Act, (which received Royal Assent on 28 July 2000 and is expected to come into force in October 2000), will repeal the 1985 Act and provide a new regime to govern interception and protect confidentiality. However, the Directive permits Member States to authorise the interception of communications for the purposes of providing evidence of a commercial transaction or other business communication, and for purposes of national security, the detection of criminal offences and the detection of unauthorised use of a telecoms system.

The Government proposes to make "Lawful Business Practice" Regulations under Section 4(2) of the RIP Act to specify the circumstances in which both private businesses and public authorities may lawfully intercept communications.

This Consultation Document provides a detailed description of the legislative background and the draft Regulations. It provides a list of "Questions for Consultees" and invites comments on these or any other aspects of the proposals *by 15 September 2000*.

6. STATUTORY INSTRUMENTS

2000 No.

Telecommunications

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Made 2000

Laid before Parliament 2000

Coming into force [2nd October]2000

The Secretary of State, in exercise of the powers conferred on him by sections 4(2) and 78(2) and (5)(a) of the Regulation of Investigatory Powers Act 2000 (4) ("the Act") , hereby makes the following Regulations:-

Citation and commencement

These Regulations may be cited as the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and shall come into force on [2nd October] 2000.

Interpretation

In these Regulations, references to a business include references to any activities of a government department, of any public authority or of any person or office holder on whom functions are conferred by or under any enactment; and-

"business communications" means-

(a) communications by means of which transactions are entered into in the course of a business, or

(b) other communications relating to a business or taking place in the course of its being carried on;

"charitable helpline" means a confidential telephonic counselling and support service provided by a charitable body free of charge to members of the public who may choose to remain anonymous; and

"evidence" has the same meaning as in Directive 97/66/EC of the European Parliament and of the Council. (5)

Lawful interception of a communication

(1) For the purpose of section 1(5)(a) of the Act, conduct is authorised, subject to paragraph (2) of this regulation, if it consists of interception of a communication, in the course of its transmission by means of a telecommunication system, which is effected for the purpose of-

(a) monitoring or keeping a record of business communications-

(i) by a person specified in section 6(2)(a) to (i) of the Act in the interests of national security, or

(ii) for the purpose of preventing or detecting crime,

(iii) for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system, or

(iv) in order to provide evidence of the communications for the purpose of either establishing the existence of facts or ascertaining compliance with practices or procedures relevant to the business carried on by the person by or at whose request the interception is effected; or

(b) monitoring communications made to a charitable helpline.

(2) Conduct is authorised by paragraph (1) of this regulation only if

(a) the interception in question is effected in connection with a business carried on by the person by or at whose request it is effected,

(b) the telecommunication system in question is provided for use wholly or partly in connection with that business, and

(c) the person effecting the interception-(i) has made all reasonable efforts to inform every person to whom or by whom the communication in question is made that it will or may be intercepted, or

(ii) otherwise has reasonable grounds to believe that every such person is aware that it will or may be intercepted.

Patricia Hewitt

Minister for Small Business and E-Commerce

Department of Trade and Industry

2000

Explanatory Note

(This note is not part of the Regulations)

These regulations authorise certain interceptions of telecommunication communications which would otherwise be prohibited by section 1 of the Regulation of Investigatory Powers Act 2000. To the extent that the interceptions are also prohibited by Article 5.1 of Directive 97/66/EC, the authorisation does not exceed that permitted by Articles 5.2 and 14.1 of the Directive.

The interception has to be by or at the request of a person carrying on a business (which includes the activities of government departments, public authorities and others exercising statutory functions) in connection with that person's business and using that business's own telecommunication system. Interceptions are authorised for monitoring or recording communications in the interests of national security, to prevent or detect crime, to investigate or detect unauthorised use of telecommunication systems or to obtain evidence of the communications themselves, and also for monitoring communications made to charitable helplines.

Interceptions are authorised only if the interceptor has made reasonable efforts to inform the persons making or receiving the communications of the possibility of interception or has reasonable grounds to believe that they are aware of that possibility.

The Regulations do not authorise interceptions to which the persons making and receiving the communications have consented: they are not prohibited by the Act.

7. Legislative Background

The Telecoms Data Protection Directive

The Telecoms Data Protection Directive was adopted in December 1997. The Directive aims to ensure the protection of fundamental rights and freedoms throughout the European Community with regard to the processing of personal data and the protection of personal privacy in the telecommunications sector. Article 5(1) of the Directive requires Member States to safeguard the confidentiality of communications by means of a public telecommunications network:

Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network [3] and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users without the consent of the users concerned, except when legally authorised, in accordance with Article 14(1).

This requirement extends to all types of electronic communication made "by means of a public telecoms network" including, for example, transmissions such as fax and email. The requirement also extends to communications on private networks (e.g. office telephone networks or email systems) which will also travel or have also travelled on a public network. However, the Directive leaves scope for Member States to authorise the interception of communications by businesses when this is necessary for the purpose of providing evidence of business communications. Article 5(2) states:

Paragraph 1 shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

The Directive also leaves scope for Member States to restrict the requirement to protect confidentiality laid down in Article 5.1 for purposes of national security, defence, public security and the detection of criminal offences. Article 14.1 states:

Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Article 5, 6 and Article 8(1), (2), (3) and (4), when such restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system, as referred to in Article 13(1) of Directive 95/46/EC.

Member States were required to implement the majority of provisions in the Directive by October 1998. However, an exemption was made for Article 5 which must be implemented by all Member States by 24 October 2000.

The Regulation of Investigatory Powers (RIP) Act

The existing arrangements for the interception of communications are established in the Interception of Communications Act 1985. The RIP Act, (which received Royal Assent on 28 July 2000 and which is expected to come into force in October 2000), will repeal the 1985 Act and provide for a new regime to govern the use of intrusive investigative techniques, including interception. The new legislation reflects changes which have taken place in the communications industry over the last 15 years, and will ensure that the statutory basis for the use of such techniques is fully compliant with the requirements of the European Convention on Human Rights.

The Act creates offences of unlawful interception on public telecommunication systems, and a tort of unlawful interception on a private telecommunication system by the operator of that system. The Act authorises the interception of communications in cases where the interceptor has reasonable grounds to believe that both the sender and intended recipient have consented to the interception. The Act provides for the Secretary of State to authorise interception in certain limited circumstances, by means of warrants issued to organisations such as the security and intelligence agencies and the police

8. QUESTIONS FOR CONSULTEES AND ISSUES

The Government invites comments on all aspects of its proposals and will give careful consideration to consultation responses before making the Regulations. It would particularly appreciate comments on the issues set out below.

Scope of the Regulations

The primary aim of Article 5 of the Telecoms Data Protection Directive is to safeguard the confidentiality of communications and, thereby, to protect the fundamental right to personal privacy. The intention of Articles 5(2) is to allow interceptions only when there are strong arguments that the provision of evidence should be considered more important than the protection of confidentiality or privacy. The draft regulations authorise businesses and public authorities to intercept communications without consent for the following purposes:

(a) providing evidence of a communication in cases where it may be necessary to provide records of the specific facts of individual communications, e.g. - Providing evidence of a commercial transaction

Providing evidence of other business communications to establish facts or ascertain compliance with regulatory practices or procedures.

Audit

Debt recovery

Dispute resolution

(b) detecting and preventing crime, and detecting the unauthorised use of a telecoms system, e.g. - Preventing or detecting crime

Detecting the unauthorised use of an electronic communications system

Protecting a network against viruses or hackers

Combating or investigating fraud or corruption

The draft regulations also authorise public authorities, but not businesses, to intercept communications without consent in the interests of national security.

Question 1: Bearing in mind the constraints of the Directive, do you agree with the scope of the Regulations?

The Regulations do not, in their current form, authorise businesses to intercept communications for non-evidential purposes such as staff training, market research, quality control and the like. If businesses wish to intercept communications for these purposes, they will need to have reasonable grounds for believing that correspondents have consented to the interception as required by Section 3(1) of the RIP Act.

Question 2: Do you agree that businesses should gain the consent of callers before making interceptions for purposes such as quality control, staff training, marketing or market research?

Charitable Helplines

Certain charities currently monitor communications on their helplines in order to provide front-line staff adequate support and protection when taking long, stressful and, sometimes, abusive calls. However, it may not be practicable for charities to ensure the consent of callers before intercepting communications of this nature.

For these reasons, the Regulations will authorise charitable bodies to monitor communications to counselling and support helplines provided free of charge on an anonymous basis. They will not be required to gain the consent of callers but they will be required to make all reasonable efforts to inform callers, or to have reasonable grounds to believe that callers are aware that the interception may take place.

Charities will not be permitted to record conversations, and they will only be permitted to monitor conversations provided that the helpline is operated on an anonymous basis. These restrictions will ensure that the caller's confidentiality is not compromised as a result of the interception.

Question 3: Do you agree that appropriate charities should be authorised to intercept communications on their helplines without the consent of callers?

Drafting of the Regulations

There is a danger that overly prescriptive regulations might, unintentionally, either permit or prohibit interception activities in contradiction to the spirit of the legislation. There is also a danger that highly detailed regulations might need regular revision in order to keep pace with commercial and technological developments. For these reasons, the Government has taken a broad brush approach to the drafting of the Regulations. The proposed Regulations outline the broad circumstances in which businesses may intercept communications but they do not provide an exhaustive list of acceptable or unacceptable interception activities.

Question 4: Do you agree with the Government's approach to the drafting of the Regulations?

Industry Guidelines

The Government believes that further clarification of the Regulations should, if necessary, take the form of industry guidelines. It believes that any such guidelines should be developed by industry groups with sector-specific expertise in accordance with accepted principles for the development of self or co-regulatory codes of conduct.

A set of guidelines might provide clarification of the circumstances in which businesses can legitimately intercept communications under the Lawful Business Practice Regulations

and in what circumstances, in accordance with the Regulations, they would have reasonable grounds to believe that telecoms users were aware that interceptions might occur. The guidelines might also outline how, in other cases, businesses should ensure that correspondents consent to interception; and they might outline the measures that businesses should take to safeguard the privacy of staff.

Question 5: Do you consider that industry guidelines should be developed to provide further clarification of the Regulations? If so, which bodies should be chiefly involved?

Protection of Personal Privacy

The primary aim of both the Telecommunications Data Protection Directive and the RIP Act is to safeguard the confidentiality of communications and the right to personal privacy. The intention of both pieces of legislation is to authorise the interception of communications without consent only when there are powerful arguments that the collection of evidence should be considered more important than confidentiality or privacy.

Question 6: Do you consider that the Regulations take sufficient account of the need to protect the confidentiality of communications and the right to privacy?

Impact on Business

These regulations do not, in themselves, impose a regulatory burden. On the contrary, they make exceptions to the general requirement (imposed by Section 3(1) of the RIP Act) to gain the consent of correspondents before making an interception. When making interceptions authorised by the regulations, businesses will need to make all reasonable efforts to inform callers that interceptions may take place. When making interceptions which fall outside the scope of the regulations, they will need to gain consent. While

businesses may need to modify their procedures to meet these requirements, there has been no evidence so far that they will encounter significant costs.

Question 7: Do you agree with the broad conclusions of the regulatory impact assessment that businesses should not incur significant costs as a result of the regulations? What do you consider the compliance costs of implementing the regulations will be?

Question 8: Do you agree with the conclusion of the regulatory impact assessment that small businesses should not incur significant costs as a result of the regulations? What do you consider the compliance costs of implementing the regulations will be for small businesses

9. How to respond

The closing date for consultation responses is 15 September 2000.

Respondents should make clear whether or not they wish their comments to remain confidential. In every case, respondents should include a brief description of the nature of their organisation and, if relevant, the groups whom they represent. Respondents should provide a short non-confidential summary of their concerns for publication on the DTI website. Consultation responses should be sent by email in electronic form (Word format) to: tdpd.tdpd@dti.gov.uk

Hard copies of consultation responses should, if necessary, be sent to:

Communications and Information Industries Directorate

Department of Trade and Industry

151 Buckingham Palace Road

London SW1W 9SS

The Government intends to publish a summary of consultation responses and a response to consultation at the end of August. These documents will be available on the DTI website in the Telecoms industry. We have encountered a number of delays in developing the draft regulations. At the same time, the RIP Act has made faster recent progress through Parliament than anticipated. The DTI regrets that, in order to bring the regulations into force at the same time as the RIP Act (anticipated in October), it is necessary to limit the consultation period to four weeks (now extended by three weeks). We have taken a number of measures to make sure that, despite this restriction, the consultation exercise will be as effective as possible. We have held preliminary presentations and discussions with some seventy representatives of the financial services and information industries; and we have contacted over 1300 interested parties including telecoms operators, service providers, financial services organisations, trade associations, small businesses, small firms organisations, charities, and consumer bodies to draw their attention to the start of the consultation.

Timescale

- 28 July 2000 The Regulation of Investigatory Powers Act received Royal Assent.
- 15 September 2000 End of public consultation on these regulations
- From 15 September 2000 The Government publishes a summary of responses and a response to consultation on the DTI website.
- October 2000 The Secretary of State makes the new Regulations.
- October 2000 The RIP Act and Regulations expected to come into force.
- 24 October 2000 Formal deadline for transposition of Article 5 of the Telecoms Data Protection Directive

10. Key Issues raised in the consultation

The Government received more than 80 consultation responses from businesses, charities, individuals and representative organisations. The majority of responses represented business interests and focused on the need to facilitate legitimate business activities. Others represented the interests of employees and consumers. This section outlines the key issues raised in the consultation exercise and the steps we have taken to address consultees' concerns.

Interceptions for operational purposes

A number of businesses have suggested that the draft Regulations might not allow them to make essential interceptions to ensure the operation of their telecoms systems.

Businesses need to monitor communications to protect their systems against viruses and other threats. They also need to make routine interceptions for operational purposes such as backing up and forwarding emails to the correct destination.

We understand that businesses need to intercept communications for a variety of purposes relating to the operation of their systems. We have expanded the regulations to make clear that businesses are allowed to record or monitor communications without consent in order to secure, or as an inherent part of, the effective operation of their telecoms systems. This will make clear that businesses are able to intercept to protect against viruses, to route traffic and for other similar purposes.

Routine access to business communications

A number of consultees have suggested that the RIP Act and the Regulations may not provide business with sufficient authority to gain access to their own communications. Businesses need to check voicemail systems and email accounts in order to access communications during the absence of staff. It would be unreasonable and impracticable to require businesses to gain the consent of senders and recipients of communications before doing so.

We understand that businesses need to have access to their own communications. We have expanded the Regulations to authorise businesses to monitor communications without consent in order to determine whether they are relevant to the business. This will achieve a balance between giving businesses free access to their own communications and protecting the privacy of non-business communications where these are permitted.

Interceptions for quality control purposes

The consultation paper specifically asked respondents to comment on interceptions for quality control purposes. A large number of respondents suggested that businesses ought to be able to monitor calls for these purposes. A variety of businesses regularly monitor calls for a range of customer relations management purposes, for example, staff-training and quality control. The operators of call centres, in particular, monitor calls as an essential method of maintaining service standards.

Consultation responses made clear that call centres would need to overhaul their procedures if they were required to gain consent for this type of interception. The majority of call centres monitor calls on a random basis. Their current equipment and procedures would not allow them to stop monitoring if a customer refused consent. One major operator suggested that the costs of implementing procedures to gain consent would be over £800,000 per annum.

In the light of these arguments, the Government has come to the conclusion that it would not be in the interests of businesses or consumers to require consent before monitoring for quality control. We have expanded the scope of the Regulations to allow businesses to intercept without consent in order to ascertain or demonstrate the standards which ought to be achieved by persons using their systems. This will allow businesses to continue monitoring as at present for purposes such as staff training which are of benefit for consumers.

Interceptions for other purposes such as marketing and market research

A small number of consultation respondents suggested that businesses ought to be able to intercept communications without consent for purposes such as marketing or market

research. However, the Government would be reluctant to authorise businesses to intercept without consent for purposes which were neither strictly essential nor necessarily in the interests of consumers. It is our understanding that in most cases, such functions could be performed using stored data without the need for interception. (These activities would probably fall within the scope of the Data Protection Act 1998). We also believe that Regulations that authorised these interceptions might be inconsistent with the Telecoms Data Protection Directive. For these reasons, we have decided not to widen the scope of the Regulations to allow interceptions without consent for other purposes such as marketing or market research.

Monitoring calls to welfare helplines

Certain charities currently monitor communications on their helplines in order to provide counselling staff with adequate protection. Helpline calls can sometimes be distressing and monitoring offers a practical way to support staff. For these reasons, the consultation draft proposed to allow charities to monitor (but not record) communications to counselling and support helplines providing that these services were offered free of charge and on a confidential basis.

A number of businesses have explained that they also run confidential, welfare helplines and that they also need to monitor calls in order to protect helpline staff. These businesses include television and radio broadcasting companies and trades unions.

The Government accepts that businesses, like charities, have a legitimate need to monitor calls to their counselling helplines in order to protect staff. We have therefore modified the Regulations to allow any business to monitor, without consent, communications to counselling or support helplines. The Regulations specify that monitoring is only authorised if the helpline is provided free of charge and on a confidential basis. This will safeguard the confidentiality of conversations despite the fact that monitoring may take place.

Monitoring for unauthorised use

A number of businesses have indicated that they currently intercept communications in order to check for unauthorised use. Some businesses monitor internet use to check that

employees are not accessing offensive material using the company's system. Some scan emails for indications of harassment or abuse.

The final regulations, like the consultation draft, will authorise businesses to intercept communications without consent in order to investigate or detect unauthorised use of their telecoms systems. This will allow businesses to check that staff are not using their equipment for inappropriate purposes such as those described above.

The sure way to make it clear what is or is not authorised use would be to circulate a notice to staff and/or to put notices on telephones and PCs explaining what use of the business's telecoms system was authorised, what use was unauthorised. Some uses, however, would be unauthorised even without a notice, such as anything illegal (eg, downloading child pornography) or in breach of an employee's duty (eg, passing trade secrets to a competitor).

The requirement to inform correspondents of interceptions

The draft regulations required businesses to make "all reasonable efforts" to inform all parties to communications that interceptions might take place or, otherwise, to have "reasonable grounds to believe" that the parties to communications were already aware that interceptions might take place. The large majority of respondents commented on the costs and practical difficulties that this provision might impose.

Businesses have not expressed concern about having to inform their own staff that interceptions may take place. A large number of businesses do so already. Where this is not current procedure, businesses could use a variety of methods to inform staff that call recording or monitoring might take place. Our discussions with business groups indicate that this could be done without significant difficulty or cost.

However, businesses are worried about the additional costs of informing third parties that interceptions may take place. They could do this by means of recorded messages at the start of telephone calls or by means of notices in publicity literature. But in both cases, the financial burden of reorganising procedures might be considerable.

Businesses have also suggested that in some cases it would be inappropriate or impracticable to inform correspondents of interceptions. Certain organisations, for example record calls to their switchboards in order to provide evidence of bomb threats. In case like

this, they suggest that it would be inappropriate to inform callers that recording takes place.

The Government is anxious to make clear and workable regulations and to avoid placing unreasonable burdens on business. We accept that, in many cases, a requirement to inform outside correspondents of interceptions would place an excessive burden on business. For that reason, we have removed the requirement to inform all parties to communications of interceptions.

However, we have retained a requirement for businesses to "make all reasonable efforts" to inform the users of their own telecoms systems that interceptions might take place. This will ensure that, in accordance with current best practice, businesses inform employees of that communications may be monitored or recorded.

Workplace Practice

A small number of respondents have suggested that the Regulations should establish a legal framework for workers and management to discuss company practices relating interception.

The Government would certainly wish to encourage businesses to agree with employees on appropriate levels of recording or monitoring if they wish. The Regulations will certainly not inhibit or discourage such discussions.

However, the Government would not want to oblige businesses to engage in collective bargaining on interception. Businesses need to intercept for a variety of essential purposes such as ensuring the routine operation of their systems. We believe they should have a clear right to do this providing they inform their employees that interceptions may take place.

The Data Protection Commissioner is currently developing a Code of Practice on the Use of Personal Data in Employer/Employee Relationships. The Commissioner intends to publish a draft of the Code in October 2000 for consultation. The Code will address the impact of the data Protection Act 1998 on the monitoring by employers of telephone calls, emails and internet access involving their employees. The Commissioner has told us that she intends that the Code of Practice will take account of the Regulations and address their inter-relation with data protection requirements. The Government believes that the Data Protection Commissioner's Code will provide an excellent opportunity to develop best

practice regarding monitoring of employees at work. We would urge interested parties to participate in the consultation.

A Proportionality Test

A small number of consultation responses suggested that the Regulations should include a proportionality test to govern the extent of businesses' interception activities. They argue that such a test would ensure that a business's interception activities were in proportion to the level of need for interception.

The Government is not convinced that this approach would lead to transparent or workable regulations. It would leave businesses and others unsure as to what interception activities were permitted. This would place businesses in a vulnerable legal position and might encourage some to relocate operations outside the UK.

The Data Protection Act 1998 applies a proportionality test to the obtaining and recording and processing of personal data. We believe that this Act is sufficient to ensure that businesses act in a proportionate manner when collecting and using personal information.

The Rights of Consumers

A small number of respondents suggested that the Regulations might result in an imbalance between the rights of business and the rights of consumers. They were concerned that the combined effect of the Regulations and the RIP Act would be to allow businesses to record their calls with customers, but to deny consumers the right to record their calls with businesses.

This is not the case. The Regulation of Investigatory Powers Act does not prohibit individuals from recording their own communications for their own use, because that does not fall within the meaning of "interception" in the Act. Consumers will be able to record their calls with business providing that the recording is for their own use. Nothing in the Act would prevent the consumer from choosing subsequently to disclose or make use of that record in the courts or dispute resolution proceedings.

11. OUTLINE OF THE ORIGINAL PROPOSALS

The Consultation Paper provided a first draft of the Lawful Business Practice Regulations and invited interested parties to comment on its proposals.

The draft Regulations would have authorised businesses, including public authorities, to intercept communications without consent for the purposes of establishing the existence of facts, detecting crime and detecting the unauthorised use of their telecoms systems. They would have authorised charitable bodies to monitor calls to confidential counselling helplines. And they would have authorised public authorities to intercept communications on their or (where invited) others' private systems in the interests of national security.

In all of these cases, the draft regulations required the interceptor either to make all reasonable efforts to inform all parties to the communication that interceptions might take place or, otherwise, to have reasonable grounds to believe that the parties to the communication were already aware that interceptions might take place

12. OUTLINE OF THE FINAL REGULATIONS

The final regulations will authorise businesses (in the widest sense of the word, which covers charities and other non-commercial bodies and expressly includes public authorities) to monitor or record all communications transmitted over their systems without consent for the following purposes:

- Establishing the existence of facts

- Ascertaining compliance with regulatory or self-regulatory practices or procedures

- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system

- Preventing or detecting crime

- Investigating or detecting unauthorised use of the business's telecoms system

- Ensuring the effective operation of the system.

The Regulations will also authorise businesses to monitor (but not record) communications for the following purposes:

- Checking whether or not communications are relevant to the business

- Monitoring calls to confidential, counselling helplines run free of charge.

The Regulations will also authorise public authorities to monitor or record in the interests of national security. In all of these cases, the Regulations require businesses to "make all reasonable efforts" to inform those people who use the organisation's telecoms systems that interceptions may take place.

13. LEGISLATIVE OVERVIEW

The Regulation of Investigatory Powers (RIP) Act establishes a new legal framework to govern the interception of communications. The Act reflects the changes which have taken place in the communications industry over the last 15 years. The Act also ensures that the UK's interception regime is compliant with the Telecoms data Protection Directive. The Directive requires Member States to protect the confidentiality of communications made by means of public telecoms systems and specifically prohibits activities such as recording or tapping by others than users. It is worth noting that the European Commission has published proposals for a revised Telecoms Data Protection Directive which will be negotiated in 2001. (See Further Information and the original consultation document for additional background information.)

The Act establishes offences of unlawful interception on a public or a private telecoms system and a tort of unlawful interception on a private system by the operator of that system. However, the Act authorises interception in cases where the interceptor has reasonable grounds to believe that both the sender and the intended recipient have consented. And Section 4(2) of the Act allows the Secretary of State to make Lawful Business Practice Regulations authorising businesses to intercept on their own systems without consent for certain purposes.

In the past, businesses and others operating private telecoms systems were at liberty to intercept communications on their own systems. One of the effects of the RIP Act is that, in future, businesses which intercept on their own systems will need to be sure that their actions are legally authorised. If they intercept unlawfully, the sender or recipient of the communication may be able to obtain an injunction or sue for damages. All interceptions are authorised if there are reasonable grounds to believe in consent. The Lawful Business Practice Regulations will authorise businesses to intercept without consent for certain purposes.

URN 06/1481