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

RESPONSE OF THE E CENTRE[UK] LEGAL ADVISORY GROUP

Introduction

This Response to the Home Office Consultation Paper is submitted by the **e** centre[UK] Legal Advisory Group.

e centre[UK] was formed by the merger of the Article Number Association (ANA) with the Electronic Commerce Association (ECA) on 1st October 1998. **e** centre[UK] seeks to add value to its members by being the pre-eminent, most trusted source of the best standards for business data and the best practices for electronic commerce. It has over 16,000 members in most trade and industry sectors, covering the entire spectrum of small, medium and large companies drawn from the public and private sectors and representative of both users and suppliers (over 90% are users and over 90% are small and medium enterprises (SMEs)). Public sector members come from central government, local government and agencies. **e** centre[UK] is a non-profit making body incorporated as a company limited by guarantee, and is a member of EAN International, which is represented in 90 countries worldwide. The association offers a "one stop shop" for providing help and advice on electronic commerce to UK organisations at large and provides a comprehensive suite of services to its members to help them to adopt best practice in doing business electronically across the extended enterprise.

Its Legal Advisory Group, one of a number of expert groups, consists of **e** centre[UK] members who are legal practitioners, company legal staff and academics with experience of Internet and e-commerce legal issues. Recently the Legal Advisory Group has widened its membership to include representatives from the other associations involved in the Alliance for Electronic Business (that is the CBI, CSSA, DMA and FEI).

The **e** centre[UK] Legal Advisory Group welcomes the initiative of the Home Office in opening a consultation process on the modernisation of the interception of communications regime. This is necessary to ensure that the legislation is in step with today s communications developments and, equally importantly, that the requirements of the European Convention on Human Rights and the Human Rights Act 1998 (when implemented) are met.

The Group does, however, have serious concerns about some aspects of the proposals. Generally, in connection with issues such as authorisation procedures, the Group supports the position taken by *Justice*[1] and others regarding matters such as the desirability of judicial, rather than

[1] ***Under Surveillance - Covert policing and human rights standards - a Justice report***, 1998

administrative, warrants. These arguments have been well rehearsed in the past and we do not in this paper propose to repeat them.

Summary

This paper focuses on certain implications of the proposed extension of the interception regime to private networks. The Group takes the view that the Consultation Paper does not sufficiently distinguish between interception by the State and interception by private individuals; that that failure is, at least in part, founded on the incorrect assumption that the *Halford* case requires remedies to be provided in the private sphere as between private persons; and has led to the undesirable inclusion in this review of matters such as employer monitoring of employee communications on the employer s network. We suggest that this is inappropriate for a review whose primary purpose is to modernise the statutory regime governing State interception of private communications. Matters such as employer access to employee e-mails are best debated in the context of, for instance, data protection. We further comment on the proposals requiring Communication Service Providers to provide facilities for interception.

Discussion

There are three main aspects to the Consultation Paper:

1. Extension of the variety of networks to which the IOCA criminal offence of intercepting communications will apply.

2. Extension of the variety of networks in respect of which the Secretary of State will be able to issue interception warrants.

3. Introduction of a new regime (which would fall within the remit of the Data Protection Act) governing access by [agencies] to communications data (e.g. itemised billing records, details of telephone numbers called, e-mail addresses to which messages have been sent). This is contrasted with interception material, which refers to the actual content of communications.

The Consultation Paper rolls up together the separate issues of:

> (1) extending the authorisation regime for interception of communications by the State;
> (2) criminalising interception of communications by both the State and private persons; and
> (3) balancing the freedom of network owners and operators to access information on their own networks against legitimate privacy expectations of network users (including employees).

The Paper tends to refer to all these aspects together as the interception regime . Indeed the Paper s use of the term interception regime is often ambiguous. Regrettably, this obscures distinctions which are important in determining the appropriate way forward.

Two categories of persons who have not previously been affected by IOCA would, to differing extents, fall within the ambit of the proposed amendments.

Operators of private networks for private purposes.

Extension of IOCA criminality to the private sphere

The Paper proposes that the interception regime (see above as to the ambiguity of this phrase) will extend to all telecommunications networks, regardless of whether they are licensed as public or not [2]. It states that It will also cover interception of business telecommunications services, ranging from basic networks of a few lines found within a small office to large networks linking offices, in both the public and private sectors [3]. It appears clear from the references to e-mail in paragraph 4.5 and elsewhere, and from the general thrust of the Paper, that the Paper does not intend to make any distinction between voice and data communications, so that it intends by telecommunications networks to include computer networks such as corporate intranets, local area networks and so on.

The regime would also apparently, by implication, cover the increasingly common computer networks created by private individuals within their homes.

The existing IOCA criminal offence is contained in Section 1(1) of the Act. It provides that (subject to various exceptions):

> a person who intentionally intercepts a communication in the course of its transmission by post or by means of a public telecommunications system shall be guilty of an offence

No distinction is made in Section 1(1) between interception by the State and interception by a private person[4]. The section covers and potentially applies to both.

We understand that (subject to an exception for monitoring for business purposes - see below), the government proposes that the IOCA criminal offence should be extended to private networks used for private purposes. The new IOCA would (subject to its proposed exceptions) criminalise *authorised* access (e.g. by network owners and operators) to messages in transit across their own private computer systems and networks[5].

---

[2] Paragraph 4.2

[3] *Ibid.*

[4] The exceptions under Section 1 do of course make a distinction by permitting interception puruant to a warrant issued by the Secretary of State.

[5] The Computer Misuse Act 1990 already creates a regime criminalising unauthorised access to computer systems and the data and programs on them.

The IOCA interception offence is thus intended to subject to potential criminal liability the activities of (among others) owners and operators of private networks who read messages in transit on their own networks. The proposed extensions of IOCA criminality will affect not only public telecommunications networks and publicly available private networks, but also wholly private networks (including, potentially, private networks in the home).

Is the proposed extension of IOCA criminality required by Halford?
The Paper suggests that this extension of the interception regime is required by the *Halford* decision of the European Court of Human Rights. However, whilst *Halford* certainly requires State interception of communications on private networks to be put on a proper legal footing, and corresponding remedies to be provided, we doubt if *Halford* of itself requires the IOCA criminal offence to be extended to activities in the private sphere (i.e. horizontally between private persons).

The Consultation Paper proceeds on the assumption that the *Halford* decision requires the government to provide a remedy for interception of communications by any person, whether State or private. It is not at all clear that *Halford* requires this.

Halford concerned a public sector employee. The alleged interception was carried out by her employer, the police authority. The case therefore concerned direct interference with her private life by the State or an emanation of the State.

Does the ECHR create a positive obligation in these circumstances?

Halford itself sheds no light on the difficult question whether under the ECHR the government has, in the circumstances under discussion, not only a negative obligation to refrain from arbitrary interference with private life, but also a positive obligation to secure for its citizens protection from such interference by other private persons.

When discussing the circumstances in which a positive obligation may arise, the ECHR has emphasised that the purpose of Article 8 is essentially that of protecting the individual against arbitrary action by public authorities. Notwithstanding this, it is clear from the jurisprudence of the ECHR that such a positive obligation can exist. However, the circumstances in which it will be found to exist are by no means clear.

The Consultation Paper contains no discussion of whether, in any of the circumstances under discussion, a positive obligation arises, and if so to what extent it exists and how such obligation should be discharged. It simply assumes that *Halford* requires the existing IOCA criminal offence to be extended to non-publicly available networks without regard to the ownership of the network (private or public sector) or to the nature of the person doing the intercepting (State or private person) or the identity of the person doing the intercepting (owner of the network or third party).

Thus, whilst it is certainly justifiable (indeed necessary, given the particular threat posed to individuals by unconstrained activities of the State) to criminalise interception by the State

outwith the regime for lawful interception, the supposed requirement to extend IOCA criminality to cover all activities in the private sphere, especially private persons operating their own private networks, is by no means obvious.

If it does, is IOCA criminality the appropriate remedy?
Nor does it follow that, if the ECHR does apply horizontally so as to create a positive obligation requiring a remedy, the appropriate remedy for the actions of private persons in the private sphere is IOCA criminality. Other remedies are, or will become, available.

1. Data Protection Act 1998 (due to come into force 1 March 2000)

The Data Protection Registrar announced on 14 July 1999 that she would be developing a Code of Practice governing the use of personal data by employers, including interception of e-mail. She stated that when these were promulgated, failure to comply with them could lead to enforcement action by the Registrar or a claim for compensation by any individual who suffered as a result.

It is noteworthy that the Article 5 of the Telecoms Data Protection Directive[6] concerning confidentiality of communications on public networks, due to be implemented by 24 October 2000, is in relatively limited terms, requiring Member States to:

> 1. ... ensure via national regulations the confidentiality of communications by means of a *public telecommunications network 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). [emphasis added]
>
> 2. 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 private sphere is covered by the Data Protection Directive. Recital (11) of the Telecoms Data Protection Directive states:

> for all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by this Directive, including the obligations on the controller and the rights of individuals, Directive 95/46/EC [the Data Protection Directive] applies; whereas Directive 95/46/EC applies to non-publicly available telecommunications services;

[6] Directive 97/66/EC 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector OJ 30.1.1998.

2. Human Rights Act 1998 (not yet in force)

Section 6 of the Human Rights Act 1998 provides that it is unlawful for a public authority (including a court or tribunal) to act in a way which is incompatible with a Convention right. This provides a clear opportunity for the courts to determine whether the ECHR does have horizontal effect in any particular case before it and, if appropriate, to develop the common law to provide a remedy.

The question to what extent the ECHR may have horizontal effect between private persons in this field is among the most delicate and difficult issues that will fall to be decided as the caselaw under the Human Rights Act 1998 builds up in the future. It is not appropriate for the bludgeon of IOCA criminality to be applied to actions of persons in the private sphere. Contrary to the assumption underlying the Consultation Paper, nothing in the *Halford* case requires this. The flexible and fine-tuneable mechanisms of the Data Protection Act and the Human Rights Act will shortly be available and should be allowed to be tested in practice.

To extend the criminalisation of interception of messages on networks under IOCA to wholly private activities would cut across the axis whereby confidentiality of personal data is addressed as part of the data protection regime.

The Group also views with concern the action of the Home Office[7] in requesting OFTEL to circulate guidance to employers on recording of telephone conversations. We have two reasons for this concern: first, the action again assumes that the ECHR and the Human Rights Act have horizontal effect in the private sphere; second, the extension of the role of OFTEL, essentially a competition and technical regulator, into matters of privacy through the medium of conditions in the TSL and SPL telecommunications class licences has already set a precedent; it is inappropriate for this role extension to be encouraged further and can only create uncertainty and confusion as different regulatory bodies compete for primacy in this area.

The anomalous consequences of extending IOCA criminality to the private sphere

This is illustrated by the fact that IOCA itself (both proposed and old) is concerned only with interception of communications - i.e. real-time interception of live communications traffic. The Act does not give powers to access stored communications data, nor does it criminalise such access. The proposed extensions of IOCA (which it appears from the Consultation Paper would preserve that distinction) would create the strange result that an employer s monitoring of an employee s e-mail in transit across the employer s network would be covered by the Act and its exceptions - but searching for and retrieving the e-mail from the server would not. An e-mail attachment could be read on the system, but not intercepted in transit across the system.

This anomaly is a consequence of attempting to deal with the private sphere in a piece of

[7] See OFTEL Press Release 19 August 1999 OFTEL publishes new guidance on recording of telephone conversations .

legislation whose real purpose is to regulate State activity. The anomaly could be addessed by extending IOCA to cover access in the private sphere to stored data. But in the private sphere that would be to go further down the undesirable path of creating an alternative, parallel, data protection regime.

The danger of unforeseen change

Further, while it may be thought that the business purposes exception to the extended criminal offence (para 3.9) appears on the face of it likely to be reasonably broad[8], this structure of an exception carved out of a criminal offence is fundamentally flawed. Owners and operators of private networks may in the future have wholly legitimate, but currently unanticipated reasons for wanting to read messages on their networks. If they fell outside the exception they would risk criminal prosecution. All employers (not just employers in specialised areas such as financial services) have a legitimate interest in maintaining firewalls and intrusion detection and in screening incoming and outgoing messages for any number of reasons, e.g. filtering junk mail or network-clogging file types (such as video). These reasons may develop and change over time. Any worthwhile exception to a criminal offence would have to be very broadly worded.

The private sphere should be addressed within the context of employment or data protection law

For all these reasons the private sphere should not be within the realm of this IOCA consultation[9]. If intervention in the private sphere is thought appropriate, for instance in the context of employer monitoring and access to e-mail, that should be debated in its own right and dealt with in the context of employment and/or data protection legislation, not tacked on to legislation whose primary purpose (regulating State interception of communications) is wholly different.

It is inappropriate to seek to regulate employer-employee relationships and the use of wholly private networks by their owners and operators in an Act whose primary purpose is regulating the interception of communications by government agencies.

Operators of publicly available private networks.

The Paper defines Communications Service Providers as:

> any person providing publicly available communication services or authorised to provide telecommunications systems or networks for the conveyance of publicly available telecommunications services . (Para 5.1)

---

[8] Although we note that the possible ambit of such an exception is mentioned in four places in the Paper, all differently drafted: Background, p.3; Summary, p.5; paragraph 3.9; paragraph 4.6

[9] For clarity, we emphasis that by the private sphere we mean relations between private persons. We do not mean that State interception of communications on private networks outwith the authorisation regime should not be criminalised**.**

The Paper intends this to include, for instance, Internet Service Providers and International Simple Resale providers, who do not fall within the ambit of the current IOCA. (Para 3.5).
The significance of the definition of CSPs is that CSPs will be subject to the requirement to take reasonable steps to ensure that their system is capable of being intercepted . It appears that only CSPs will be subject to this requirement.

We are concerned that the scope of the definition of CSPs may be unclear. In view of the potentially heavy burden on a CSP to maintain interception capabilities it is important that the definition of CSPs is no wider than strictly necessary to satisfy the legitimate and proportionate requirements of the objects of the Act.

Clearly, ISPs who provide advertise retail Internet access services are intended to fall within the definition. But does a company which provides Internet access to a few business customers fall within the definition? Would an outsourcing company which manages private networks on behalf of business customers fall within it? Hosting a Web site could, on a liberal definition, be regarded as a communication service. On the other hand it would not make sense to include storage services, as the whole basis of IOCA is real-time interception of communications traffic, not access to stored data. The proposed definition of CSPs requires careful consideration.

Ambit of proposed interception powers

The Paper makes a number of statements to the effect that the interception regime will apply to all networks, private and public. In the absence of any explicit statement to the contrary in the Paper, we assume that the government proposes that the Secretary of State should be able to issue interception warrants directed at the operators of private networks used for private purposes (even though, unlike CSPs, they are not required to maintain interception capabilities). If the government does mean this, employers could be be required to permit Agencies to intercept their own employees communications on the employers networks.

To apply such interception powers to wholly private networks would be highly intrusive. It would involve serious concerns about the important privacy and human rights aspects that the government has highlighted.

e centre[UK] Legal Advisory Group.
23 August 1999