

REGULATION OF INVESTIGATORY POWERS ACT 2000: PROPOSED AMENDMENTS AFFECTING LAWFUL INTERCEPTION

A CONSULTATION

Summary

Data protection is recognised in this country and throughout Europe as an important part of the wider protection of people's fundamental rights.

The Data Protection Act 1998, which transposed the European Data Protection Directive (95/46) has played an important role in ensuring that appropriate safeguards are in place and that individuals' personal data is protected. The European Commission recognised that additional legislation was required to ensure that the same principles of data protection also applied to electronic communications. This was particularly important given the increasing use of the internet and the growth in the range of services and applications available.

The E-Privacy Directive (2002/58) was introduced as part of the Regulatory Framework for Electronic Communications to ensure proper protection for individuals and businesses in the arena of electronic communications. The main vehicle for transposing the E-Privacy Directive into UK law was the Privacy and Electronic Communications (EC Directive) Regulations 2003, although some of the measures contained within the Directive were already included in existing UK legislation. An example of this is the offence of unlawful interception contained in s1(1) of the Regulation of Investigatory Powers Act 2000 (RIPA).

Although the transposition of the E-Privacy Directive was completed in 2003, the European Commission has recently identified deficiencies in the way in which the Data Protection Directive and the E-Privacy Directive are transposed, namely:

- i) the existing offence of unlawful interception in RIPA only addresses intentional unlawful interception; and
- ii) where both parties consent to an interception, making the interception lawful within the meaning of s.3(1) of RIPA, the meaning of "consent" does not reflect that set out in the Data Protection directive.

This paper sets out proposals to remedy these deficiencies and seeks your views on the proposed changes.

Consultation questions

- 1. Are you content with the way in which we propose to change section 3(1) of RIPA to make clear that interception will be lawful only where both parties to the communication give specific**

consent to the interception? What impact would this have on Communication Service Providers?

- 2. Given that the Government accepts that it needs to make legislative changes to address the deficiencies identified by the Commission, do you agree with the recommended option?**
- 3. Are there any other options that the Government should consider or are there any changes that should be made to the recommended options?**
- 4. Do you think the First-tier Tribunal (General Regulatory Chamber) is the appropriate appellate body to determine the appeals? If not, where do you think the appeals should be directed and why?**
- 5. What, if any, additional costs would these proposed changes impose on Communication Service Providers or others?**

Background

The UK recognises the importance of data protection, in particular the need to ensure that there are safeguards in place to protect access to, and use of, individuals' personal data. The Data Protection Directive (95/46/EC) was transposed into UK law through the Data Protection Act 1998. The European Commission (the 'Commission') recognised the need for additional, more specialist, regulations to ensure that, as the use of electronic communications and the internet increased, the same data protection principles and safeguards applied irrespective of how the data is processed.

The Commission introduced the E-Privacy Directive (2002/58/EC) in the Regulatory Framework for Electronic Communications. Some of the measures required by the Directive were already in existence in the UK, for example the offence of unlawful interception in s1(1) of RIPA. The Privacy and Electronic Communications (EC Directive) Regulations 2003 were introduced to ensure that all of the other requirements of the E-Privacy Directive that were not covered by existing legislation were transposed into UK law.

The Commission has questioned the UK's transposition of the Data Protection and E-Privacy Directives. The Commission has received complaints alleging that some Communication Service Providers (CSPs) were deploying new value added or advertising services, which relied on interception, without seeking the appropriate consent from users.

Having considered the issues raised by the Commission, the UK has agreed to make some changes to address the concerns raised. The proposals are set out in more detail below and we are seeking views on them.

The E-Privacy Directive also sets out separate requirements about the circumstances in which there is a need to record a communication for the purposes of business practice. These are dealt with in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. These regulations are not at issue in this consultation and there are no current requirements to make changes to them.

THE PROPOSED CHANGES TO RIPA

Specific consent when both parties consent to their communications being intercepted

RIPA makes provision for lawful interception without a warrant under certain limited circumstances. These include the provision in section 3(1) where both the sender and intended recipient of the communication give their consent to the interception, or where the person carrying out the interception “*has reasonable grounds for believing*” that consent has been given. The interception of communications will involve the processing of personal data, and it is important to ensure that there is clarity about the circumstances in which lawful interception can take place.

The current provisions do not provide the required clarity. This is because “reasonable grounds for believing” is open to different interpretations. We intend to remove the ambiguity in section 3(1), and thereby ensure that the provision is consistent with the definition of “consent” supplied by Article 5(1) of the E-Privacy Directive and Article 2(h) of the Data Protection Directive. The Directives make clear that consent to interceptions of electronic communications by persons other than users must be “freely given specific and informed”. The changes to section 3(1) will help to ensure that those who use the provisions in section 3(1) of RIPA to intercept communications, including internet service providers offering value added services, are clear that consent has been given by both parties so as to make the interception lawful.

- 1. Are you content with the way in which we propose to change section 3(1) of RIPA to make clear that interception will be lawful only where both parties to the communication give specific consent to the interception? What impact would this have on Communication Service Providers?**

A sanction for all types of unlawful interception

The Government considers the protection of both society at large and personal information to be of paramount importance. Consequently, any unlawful intrusion into a person’s privacy, such as unlawful interception, is considered a serious matter. This is reflected in the existing offence of unlawful interception (section 1(1)) of RIPA). The penalties for intentional

unlawful interception include imprisonment of up to two years and a substantial fine up to the statutory maximum. In the last five years, for which we have data, there have only been eight prosecutions for this offence.

The existing offence is confined to cases involving intentional interception. However, the E-Privacy Directive requires a sanction to deter all unlawful interception of electronic communications by communications service providers, whether intentional or otherwise. We therefore need to introduce an additional sanction to address unintentional unlawful interception to satisfy the requirements of Article 5(1) of the E-Privacy Directive. We do not consider that the Directive imposes any requirement to extend the sanction beyond CSPs.

The activities of the Intercepting Agencies that conduct lawful interception under the authority of a warrant issued by the Secretary of State, as set out in Part 1 Chapter 1 of RIPA, are already overseen by the Interception of Communications Commissioner (IoCC). The IoCC's responsibilities and powers are set out in s57 and s58 of RIPA. The safeguards contained in RIPA and the oversight of the IoCC ensure that the appropriate checks and balances are in place, together with an effective inspection regime. If an individual believes that his communications have been intercepted unlawfully by the State, he can make a complaint to the Investigatory Powers Tribunal which can consider the complaint and, if upheld, order appropriate redress.

We believe that the activities of communications service providers in giving effect to an interception warrant already fall within the existing remit of the Interception Commissioner and should be excluded from the scope of the proposed new sanction. Consequently, genuine errors which could amount to unlawful unintentional interception by service providers when implementing an interception warrant issued under section 5 of RIPA, in accordance with their obligations under section 11, would not fall within the new sanction. The exclusion would also apply to any other actions of CSPs which could be explained with reference to any obligation imposed through an interception warrant. Errors would continue to be reported to the IoCC and published in his annual report. Immediate action would need to be taken to mitigate any errors when they occur and to revise procedures appropriately.

The options

A criminal sanction

We considered introducing a criminal sanction: a new summary strict liability offence, punishable by a fine on conviction, consisting in the interception by a person providing a public telecommunications service, without lawful authority, of a communication in the course of its transmission across a public telecommunications system. As with the existing offence in s1(1) of RIPA, it would be investigated by individual police forces and prosecuted by the Crown Prosecution Service (CPS) and no proceedings would be instituted except with the consent of the Director of Public Prosecutions. A person found

guilty of the new offence would be liable to a fine limited to the statutory maximum of £10,000 on summary conviction.

Having considered the practicalities of this, and the potential resource burden that this would place on the police, we decided not to pursue this option. It would be difficult to achieve consistency of approach across 52 police forces in the United Kingdom, all of whom could potentially be investigating separate complaints about the activities of the same service provider(s). It may also be difficult for individual police forces to access sufficiently detailed technical advice to enable them to determine whether interception had taken place in specific circumstances.

A civil sanction

The alternative is a civil sanction with a civil penalty. There are a number of different ways in which such a scheme could be administered. Having considered and discussed them with the relevant Government Departments, we believe that the IoCC would be best placed to administer the new sanction. The IoCC already works closely with CSPs in relation to his existing RIPA oversight functions and administering the new sanction would be a logical extension of his existing powers.

The key features of the sanction would be:

- A civil penalty capable of being imposed by the IoCC where he is satisfied that a person providing a telecommunications service has, without lawful authority, unintentionally intercepted a communication in the course of its transmission by a public telecommunications system.
- A civil penalty would not be imposed if the Commissioner was satisfied that the CSP was subject to an obligation to act in accordance with an interception warrant which could explain the interception in question.
- The IoCC would investigate the case, determine whether a breach had taken place, and decide whether a penalty should be imposed.
- The penalty would be a fine of up to £10,000.
- If the IoCC was proposing to impose a penalty, he would first give a warning notice to the CSP specifying that he was proposing to impose the penalty, the proposed amount and the reasons for imposing the penalty of the amount in question.
- The CSP would have a specified period (28 days) in which to make representations to the IoCC. Where the CSP wished to object to the penalty on the grounds that its actions could be explained with reference to an obligation to act in accordance with an interception warrant, there would be an additional right to make oral representations to the Commissioner.

- The IoCC would be required to take account of any representations made by the CSP before deciding whether to impose a penalty. Before imposing any penalty, the IoCC would also have to ensure that the penalty imposed and its amount was determined in accordance with all issued guidance.
- If the IoCC decided not to impose a penalty he would have to inform the provider of his decision.
- If the IoCC decided to impose the penalty, he would give the provider notice of that decision, of the amount of the penalty (up to £10,000) and of the grounds on which the penalty is imposed. The penalty notice would specify how the money is to be paid and would set out the provider's rights of appeal to the relevant judicial authority (see below: "Rights of Appeal").
- If the IoCC decided to impose a penalty, the IoCC could, in addition, serve an enforcement notice on the CSP requiring it to halt the interception that is the subject of the notice.
- Having served the monetary penalty notice, the IoCC would be able to vary or cancel a monetary penalty, but he could not vary the notice in a way that would be detrimental to the provider, for example by increasing the penalty.
- It would be open to a CSP to ask the IoCC to vary or cancel any civil monetary penalty notice that is served.
- Should the fine be unpaid then the IoCC would be able to pursue the unpaid penalty as a civil debt, which will ordinarily be recoverable in the County or High Court.
- Monetary penalties would be paid into HM Treasury's Consolidated Fund.
- The sanction would have UK wide application.
- A person on whom a civil monetary penalty notice could be served would be under a general duty to disclose to or provide the IoCC with information to assist the IoCC in performing his duties in connection with the monetary penalty regime.
- The IoCC would be able to serve the provider with an information notice requesting that information be disclosed to the IoCC to enable him to determine whether a monetary penalty notice should be imposed. The information notice would set out the CSP's rights of appeal to the relevant judicial authority against the requirement to comply with an information notice (see "Rights of Appeal" below).

- Where a CSP refused to provide the information requested or gave false information in response to an information notice, the IoCC would be able to impose a penalty on the CSP of no more than the maximum penalty available for unintentional unlawful interception.
- The provider would not be obliged to comply with a monetary penalty notice or an information notice whilst an appeal is pending.

Additional Powers for the IoCC

The IoCC already has statutory powers in relation to oversight of the warranted interception regime. The new role would be a discrete addition to his existing functions. He would therefore need some additional powers to ensure that he can:

- obtain all of the relevant information that he requires to investigate a complaint against a CSP in relation to the new civil sanction of unlawful unintentional interception.
- issue notices (including a notice requiring an unintentional unlawful interception to cease).
- impose a civil monetary penalty.

The IoCC, who is required to have held high judicial office, may require additional technical advice to help inform his consideration of whether, as a matter of fact, interception has taken place. This is because there are many new forms of electronic communication, and use of the internet is expanding within a technically complex and constantly developing environment as new techniques and applications are introduced both for the benefit of internet users and for commercial reasons. We propose introducing a measure to enable the IoCC to seek technical assistance from Ofcom when deciding whether to impose a civil penalty; this would help provide unbiased technical advice that would not compromise the commercial confidence of communications service providers.

The IoCC will issue guidance on how he proposes to exercise his functions. The guidance will include the circumstances in which the Commissioner would consider it appropriate to impose a monetary penalty notice, how he would determine the penalty amount, and the circumstances in which he would consider it appropriate to issue an enforcement obligation.

Rights of Appeal

There will be a comprehensive appeals process.

The Tribunals, Courts and Enforcement Act 2007 (TCE Act) established a unified structure for the majority of tribunals, combining a number of previously separate bodies. There are two tiers - the First-tier Tribunal and

the Upper Tribunal. It is intended that appeals under the draft regulations will be made to the General Regulatory Chamber of the First-tier Tribunal (GRC).

The GRC was established on 1 September 2009 and brings together a range of previously separate tribunals that hear appeals on regulatory issues, ranging from Charity to Environment to Information Rights. Onward appeals from the First-tier Tribunal, GRC are made to the Upper Tribunal, Administrative Appeals Chamber.

Practice Statements issued by the Senior President of Tribunals govern the composition of a tribunal. For certain jurisdictions in the GRC and the Administrative Appeals Chamber of the Upper Tribunal (AAC) they enable non-legal members with suitable expertise or experience to sit in addition to tribunal judiciary. It is envisaged that similar provision would be made for the new appeal right.

Procedure rules for the GRC and for the AAC are made by the Tribunal Procedure Committee. The GRC Rules currently in force are the Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (SI 2009/1976 as amended by SI 2010/43). Those for the AAC are the Tribunal Procedure (Upper Tribunal) Rules 2008 (SI 2698/2008 as amended by S.I. 2009/274, S.I. 2009/1975, S.I. 2010/43, S.I. 2010/44 and S.I. 2010/747). Consolidated versions of both sets of rules are on the Tribunal Procedure Committee website at <http://www.tribunals.gov.uk/Tribunals/Rules/rules.htm>.

A provider who is served with a penalty notice would be able to appeal to the relevant Tribunal (First-tier Tribunal) against the issue of the penalty notice, the amount of the penalty, the imposition of an enforcement obligation, the requirement to comply with an information notice or any decision by the IoCC not to cancel or vary the penalty notice. Besides allowing or quashing the appeal the Tribunal would be able to substitute another monetary penalty notice or information notice. The Tribunal would be able to review any determination of fact on which the original notice was based.

The appeal rights would be limited in a small category of cases. Where the IoCC determines that the interception concerned was not made lawful by or could not otherwise be explained by an obligation to act in accordance with an interception warrant, the CSP would not be able to appeal this part of his decision to the General Regulatory Chamber. However the CSP would, in those limited cases, be able to make oral representations to the IoCC before the IoCC decided whether to impose the monetary penalty.

The recommended option

A civil penalty regime will avoid any impact on the criminal justice system and will give the body responsible for administering the penalty a significant degree of control over the circumstances in which penalties will be imposed, and the amount of those penalties. This has significant advantages: it means

that the process for dealing with the more minor cases of unintentional unlawful interception by providers can be allocated to a specialist body with statutory responsibility for oversight of this area. This should make the enforcement process more streamlined and reduce the administrative burden on the police, the CPS and courts. It should also secure consistency of interpretation and action, and access to technical expertise.

The IoCC already has expertise in dealing with issues of interception. The new functions conferred on the Commissioner would constitute a natural extension to his role. The ability to call on external technical expertise would help to reduce the potential additional burden, and consequent resource impact, of the proposals. The IoCC understands the relevant workings of providers, the interception agencies, and, critically, the relationship between the organisations.

- 2. Given that the Government accepts that it needs to make legislative changes to address the deficiencies identified by the Commission, do you agree with the recommended option?**
- 3. Are there any other options that the Government should consider or are there any changes that should be made to the recommended options?**
- 4. Do you think the First-tier Tribunal (General Regulatory Chamber) is the appropriate appellate body to determine the appeals? If not, where do you think the appeals should be directed and why.**

Costs

The IoCC will have a new limb to his jurisdiction in administering the new sanction and consequently may incur additional costs. Similarly, there may be some additional costs that Ofcom accrue on the occasions that they assist the IoCC. However, we do not believe that these additional costs will be significant. CSPs will already have in place mechanisms to seek consent for interception in certain circumstances and they will want to consider, in the light of the changes outlined here, whether they are likely to incur additional costs.

- 5. What if any additional costs would these proposed changes impose on Communication Service Providers or others?**

How to respond to the consultation

Please send responses to this consultation by 17 December 2010:

by email to:

ripa-consentandsanctionconsultation@homeoffice.x.gsi.gov.uk;

or

by post to Lucy Watts, Home Office, 5th Floor Peel Building, 2
Marsham Street, London SW1P 4DE.