

The Information Commissioner's response to the Home Office consultation "The Regulation of Investigatory Powers Act 2000 ('RIPA'): monetary penalties and consents for interception"

1.0 Introduction

- 1.1 The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA), the Privacy and Electronic Communications Regulations 2003 (PECR) and the Freedom of Information Act 2000 (FOIA). The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The Commissioner's comments in this document are primarily based on the practical experience he has gained in regulating compliance with the DPA and PECR.
- 1.2 The Information Commissioner welcomes the proposal to provide a more structured regulatory process for unlawful interceptions and to clarify the consent requirement under section 3(1) of RIPA. However there are still some concerns over whether the proposed changes go far enough and provide sufficient clarification of the circumstances in which civil sanctions can be considered. It is important that any changes do not have the effect of creating further areas of uncertainty.
- 1.3 The law surrounding interception of communications can be difficult to understand and its interface with UK data protection laws is not always clear. Any new regime should help to address this problem and not add further confusion.
- 1.4 The Information Commissioner has previously stated his concerns¹ over the gap in the regulatory regime and the potential problems associated with the lack of recourse available to individuals who

¹ The Information Commissioner's response to the Home Office consultation "Protecting the public in a changing communications environment".
Document accessible at www.ico.gov.uk

believe an unlawful unintentional interception has taken place. The Commissioner has also previously indicated his belief that the introduction of civil sanctions would go some way to bridging the gaps in the regulatory regime. The proposed change, giving the Interception of Communications Commissioner (IoCC) additional powers to investigate complaints against Communication Service Providers (CSPs), is a positive development.

- 1.5 The Information Commissioner has no regulatory competence to deal with interception of communications. Even where personal data are obtained as a result, the Information Commissioner cannot rule on the lawfulness or otherwise of an interception. That being said, the first data protection principle requires that the processing of personal data is fair and lawful. If personal data is intercepted unlawfully under section 1(1) of RIPA this may also constitute a breach of the first data protection principle. It will be important therefore to draft the legislation in a way which allows the ICO to work with the IoCC once it has been established if an interception is unintentionally unlawful.
- 1.6 In light of this we believe it is necessary for further clarification to be provided on the role of the ICO, the IoCC, the Home Office and other bodies involved in regulating areas touched upon by this consultation. Certainly in terms of the Information Commissioner's role, if any, we would welcome clarity in the legislation on the scope of his remit in terms of the regulation of interceptions.
- 1.7 It is also important to ensure that the law, or guidance on the law, gives clarity to service providers who, in the course of carrying or transmitting communications, may perform certain actions on those communications which they believe to be necessary to provide a reliable and efficient service but which may also constitute an interception.
- 1.8 This consultation poses a number of specific questions. The next sections of this document will detail the ICOs response to these questions.

2.0 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 will this have on Communication Service Providers?

- 2.1 The changes seek to remove the ambiguity created under section 3(1); in particular the intention is to provide clarification on when an interception will be deemed lawful by bringing the definition of consent in line with Article 5(1) of the E-Privacy Directive and Article 2(h) of the Data Protection Directive. We believe removing this ambiguity and emphasising the need to obtain consent from both parties rather than acting in the 'reasonable belief' that consent has been obtained will provide greater clarity on when an interception is a lawful interception. As mentioned at 1.7 above the law should be clear about which processing operations constitute an interception of communications so that senders, recipients and carriers are aware of the circumstances in which consent is required.
- 2.2 That being said, consent will also need to be clearly defined and the Home Office may need to issue a clear statement on the definition of consent in this context. Without more specific detail on this it is difficult to comment in any depth but if we assume that consent, however it is defined, is likely to require an acknowledgement or signal that the parties involved have understood and agreed to something, this may be difficult for CSPs to achieve.
- 2.3 Many CSPs will provide details of how personal data will be used in privacy policies of websites, in terms and conditions or in contractual terms. Whilst this is generally sufficient to satisfy the 'fair processing' element of the first principle (in that individuals are broadly informed how their information will be used) there may be issues for CSPs around how to obtain agreement or a signal of understanding from both parties where one of the parties will be the website the individual is accessing.
- 2.4 Nevertheless the concept of 'consent' is an important one in data protection legislation. To be valid consent must be informed and freely given. Obtaining consent involves more than simply the provision of information and it is a subject on which the ICO has provided guidance. It is important that the same approach is adopted in relation to consent for interception of communications and that different standards of consent do not develop in the field of information rights.

3.0 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?

- 3.1 The introduction of civil sanctions should address some of the inequalities in the regulation of intentional unlawful and unintentional unlawful interceptions. However, there appears to still be a lack of detail over what would be considered an unintentional unlawful interception. Currently, intentional unlawful interceptions are subject to criminal sanctions and the proposal is for unintentional unlawful interceptions to be subject to civil sanctions. Taking into account these differences in regulation there may need to be a clearer definition of an unintentional unlawful interception.
- 3.2 The consultation document makes specific reference to genuine errors when implementing interception warrants under section 5 of RIPA and these errors not falling within the proposed new civil sanction. However we are of the view that the Home Office will need to more specific in outlining not just those interceptions which will not fall within the sanctions but also those that will.
- 3.3 Furthermore the consultation document states that CSPs will need to take immediate action to mitigate errors and revise procedures. It is not clear though whether this will be a specific statutory requirement or whether it will simply be a good practice matter overseen by the IoCC.
- 3.4 In the case of Phorm the Information Commissioner was not in a position to determine whether an intentional unlawful interception had occurred although some believed this to be the case. Had the IoCC or any other body competent to make that determination established that this was so then the new civil sanctions would not have applied as the interception was not unintentional. However no prosecution or criminal sanction could be brought against Phorm for what may have been an intentional unlawful interception. This suggests there is still a gap in the regulatory regime.
- 3.5 The process for issuing a civil penalty seems to be very much process-driven and appears to have no consideration for factors such as harm or detriment to those affected by the interception. We are of

the opinion that further work may be needed in this area in terms of identifying whether actual and potential harm or detriment should be considered when deciding if a civil penalty is an appropriate measure and, if so, what the level of penalty should be.

- 3.6 In the case of interceptions involving traffic data where the purpose is to provide a value added service there may be some merit in considering this differently from the interception of traffic data for the purposes of commercial gain. We do recognise, however, that much will depend on how much detail is provided on what constitutes an unlawful unintentional interception but regardless of this we consider that the penalties should be proportionate to the impact or potential impact of the interception on the individuals concerned.
- 3.7 There is an indication that the civil sanctions will only apply to unintentional interception of communications transmitted by public telecommunications services. If there is no equivalent sanction for the interception of communications transmitted by private telecommunications services the new sanctions may create further imbalances in the regulation of unlawful interceptions.
- 3.8 There is reference in the proposals to the IoCC serving enforcement notices on CSPs where it has been decided that a penalty should be imposed. Our understanding is that enforcement notices would be used as a means of preventing a CSP from continuing any interception the IoCC considered unintentional and unlawful, whereas a fine will be a penalty for an unlawful interception that has already taken place. This is not incongruous and is in line with the ICO's own powers to issue monetary penalties and enforcement notices. However it may be helpful if the Home Office clarifies whether the proposals have been intentionally written to allow the IoCC to issue notices after penalties have been imposed and that, in any case, fines and enforcement notices can be issued independently of each other.
- 3.9 The ICO has issued guidance² which explains that there are some circumstances and factors which may be relevant to our decision to

² Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998.
Document accessible from www.ico.gov.uk

issue a monetary penalty for breaches of the DPA; in particular where a data controller has already complied with the rulings of another regulatory body. It is not our intention that organisations should be subject to 'double jeopardy' where an act constituting a breach of the DPA triggers regulatory penalties elsewhere. If an unintentional interception is deemed by the IoCC to be suitable for a fine this may be linked directly to a breach of the first data protection principle. It may therefore be necessary for the IoCC and the ICO to consider a memorandum of understanding to ensure that organisations are not served with two penalty notices for what is essentially one failure. For this reason it will be important to draft the legislation in a way which allows the IoCC to work and share information with the ICO.

- 3.10 It would seem appropriate for the IoCC or the Home Office to produce equivalent guidance to the ICO's guidance on issuing monetary penalties. The consultation document does indicate the IoCC will be required to issue guidance explaining the circumstances in which monetary penalty notices will be imposed and the penalty amount. We would hope this guidance would provide some much needed clarity and ensure that there is a degree of consistency in the process for imposing penalties in related regulatory regimes.
- 3.11 Following on from this, consideration should also be given to clarifying the circumstances in which the £10,000 fine will be levied. It is currently unclear whether the £10,000 fine is per incident or per person affected. In addition the Ministry of Justice has issued guidance³ on determining the most appropriate regulatory sanctions. This explains that fixed monetary penalty notices used for civil sanctions and set out under the Regulatory Enforcement and Sanctions Act 2008 are usually capped at £5,000 which is the statutory maximum fine a magistrate's court can impose in England. If the proposed penalty of £10,000 is introduced it appears that this may mean the penalty for an unintentional unlawful interception would be higher than the £5,000 penalty that can be applied for a criminal offence of intentional unlawful interception. Further clarification of this is needed as, on the face of it, the penalty for a business that commits an intentional act may be less than for one that commits an unintentional act.

³ Ministry of Justice guidance on creating new regulatory penalties and offences. Document accessible from www.justice.gov.uk

3.12 Finally, it should be born in mind that RIPA does not currently define the term 'communication service provider'. It is important that any definition of this term is consistent with other legislation, in particular PECR where the terms 'communications provider' and 'public communications provider' are used.

4.0 Are there any other options that the Government should consider or are there any changes that should be made to the recommended options?

- 4.1 Under section 51 of the DPA the Information Commissioner has a general duty to promote good practice. The Information Commissioner does this by providing advice and producing guidance both for individuals and for data controllers.
- 4.2 The Information Commissioner is often approached to give advice on the lawfulness of interceptions which, as already mentioned in this document, is outside his remit. Currently RIPA does not place a duty on the IoCC or any other body to provide advice to private sector organisations, including CSPs, and there is no indication in the proposals that this deficiency has been addressed.
- 4.3 It is important that an equivalent duty to the section 51 duty placed on the Information Commissioner is included in RIPA requiring the IoCC or another appropriate body to provide advice and guidance to CSPs. Whilst the proposed new powers do provide a means for individuals to raise concerns and complaints with the IoCC there is also a need for CSPs to be able to seek advice to help prevent unintentional interceptions from occurring.
- 4.4 Although CSPs do not appear to have any specific body to approach for technical advice or support; the IoCC will be able to approach Ofcom for independent advice on whether to issue civil penalties. It is not clear what level of detail and technical support Ofcom will be required to provide and how this will work in practice. However, if Ofcom are in a position to provide unbiased impartial advice to the IoCC on interceptions consideration should be given to whether Ofcom (or another independent body) can also offer this same technical advice directly to CSPs.

5.0 Do you think the First-tier Tribunal (General Regulatory Chamber) is the appropriate appellate body to determine the appeal? If not, where do you think the appeals should be directed and why?

- 5.1 The GRC has experience of dealing with regulatory issues. In addition to this, the proposed process for issuing monetary penalties appears to be similar to the ICO's process for issuing monetary penalties under which appeals are heard by the General Regulatory Chamber. The Ministry of Justice guidance also favours appeals against new civil sanctions being heard by the First-tier Tribunal.
- 5.2 The section of the consultation regarding the right of appeal states that appeal rights would be limited in a small category of cases. Whilst this is then expanded upon to explain this may be where the IoCC determines that interception was not made lawful by an interception warrant, greater clarity on how this limitation will work in practice is required.

6.0 What if any additional costs would these proposed changes impose on Communication Service Providers or others?

- 6.1 It is not appropriate for the Information Commissioner to comment on the potential costs that may be incurred by CSPs by complying with these proposed changes to the Regulations.

7.0 Conclusion

- 7.1 The Information Commissioner recognises the need to make these changes to the legislation and welcomes the proposed amendments. It is hoped these will provide some much needed clarification of the nature of consent required for lawful interceptions.
- 7.2 As already mentioned the Commissioner has had long standing concerns over the lack of a process allowing individuals to raise complaints over perceived unlawful unintentional interceptions. The introduction of a civil sanction and an avenue for individuals to direct their concerns is certainly welcomed. The continued lack of a source of advice and assistance for CSPs is however still of some concern.
- 7.3 The Information Commissioner has no power to oversee interceptions and, as mentioned in 1.6, we would welcome clarity in the legal

framework if there is an expectation that the Commissioner should be more involved in this area.

- 7.4 The wording of RIPA can at times create some uncertainty. For example, there is no standard legal definition of 'intentional' and 'unintentional' whereas the term 'knowingly and recklessly' has a generally understood meaning in law. There is a risk of ambiguity over the use of terms such as intentional and unintentional but the consultation does not seek to address this or suggest a clear definition of what is an unintentional unlawful interception.
- 7.5 The introduction of a £10,000 fine for unintentional unlawful interceptions may impact on the Information Commissioner's power to issue monetary penalties where an unlawful unintentional interception involves the unlawful collection of personal data. The Information Commissioner would therefore welcome the opportunity to discuss the interaction of these powers in more detail once a decision has been made on these proposals.

17 December 2010