EJLT European Journal of Law and Technology

Response to the consultation by the Home Office regarding its proposals amend the *Regulation of Investigatory Powers Act 2000* to address deficiencies identified by the European Commission

Judith Rauhofer [1] [2]

Cite as: Rauhofer, J., 'Response to the consultation by the Home Office regarding its proposals amend the *Regulation of Investigatory Powers Act 2000* to address deficiencies identified by the European Commission', European Journal for Law and Technology, Vol. 3, No. 1, 2012

Background

This is a collaborative submission from a group of academics based in the UK with expertise in information technology law and related areas. The preparation of this response has been funded by the Information Technology Think Tank, which is supported by the Arts and Humanities Research Council and led by the SCRIPT/AHRC Centre for Research in Intellectual Property and Technology, University of Edinburgh.

Questions and Responses

Question 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?

Although the proposals provide that the Government intends 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*', they do not specify the way in which the Government plans to achieve this. This makes it difficult to comment on the proposals. Given the clear requirement in Article 5(1) of the *E-Privacy Directive* that member states must prohibit 'listening, tapping, storage or other kinds of interception or surveillance of communications [...] without the consent of the users concerned', the Government should remove the words 'has reasonable grounds for believing' from section 3(1) of RIPA.

Use of consent in an online environment

It would also have been useful, if the proposals had included a description of the means with which parties wishing to intercept communications should be permitted to obtain the consent of both the sender and the recipient. Will communications service providers be permitted to rely on their customers' consent where this has been implied by means of the providers' terms of business or privacy policy or will the new provisions provide that such consent must be more specifically given? Will third parties planning to intercept communications with the assistance of communications service providers be able to rely on the consent so obtained by the providers or will they be required to obtain the users' voluntary, specific, and informed consent themselves?

Although Article 5(1) of the *E-Privacy Directive* clearly provides for the use of consent in relation to the interception of communications, it is widely accepted that the interpretation of that term raises a number of issues in a consumer context, particularly in the online arena. Article 2(h) of the *Data Protection Directive* defines consent as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement'. Recital 17 of the *E-Privacy Directive* further provides that '[c]onsent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website'. Both definitions point towards some form of active behaviour on the part of the user through which he signifies that he is in fact aware of the condition to which he has been asked to consent and that he specifically approves, or agrees to, that condition. It has therefore been widely questioned whether, for example, the inclusion of provisions implying consent to specific actions by the service provider in the provider's privacy policy or terms of business can be sufficient to fulfill this requirement. In practice, these terms and policies are rarely read and even more rarely understood by users who often bypass them in the knowledge that they are usually non-negotiable anyway.

The Article 29 Working Party has in the past advocated a restrictive interpretation of the requirement to obtain consent - rejecting, for example, the practice of using pre-ticked boxes to imply consent and arguing in favour of a restriction on consent in situations where there is an unequal relationship between the data subject and the data controller (for example, in an employment relationship). [3] Although the telecommunications market is generally considered to be competitive, thereby giving users the option of switching providers easily, in practice, telecommunications service provision to consumers is dominated by a handful of big service providers whose terms of service are very similar. Those providers do not, as a rule, compete with each other on the basis of their 'privacy offering' nor is there any incentive for them to do so. Consequently, users often find themselves in a relatively weak bargaining position if they want to reject, or refuse to consent to, specific provisions included in providers' terms of service. It is therefore at least questionable how 'freely given' users' consent can be seen to be, if - as is likely - an industry standard develops under which the terms of service of all big providers habitually include a term which implies users' consent to the interception of their communications by the provider.

The European Commission acknowledges the difficulties that the use of consent in an online environment presents. In its Communication 'A comprehensive approach on personal data protection in the European Union' published in November 2010, it has identified the need to ensure informed and free consent as one of the key objectives of its new comprehensive approach to data protection. [4] A few months earlier, in May 2010, 75% of respondents to a public consultation by the European Commission on 'Priorities for a new strategy for European information society (2010-2015)' believed that consent to the processing of personal data 'should meet higher requirements (in terms of transparency, and simpler/more understandable privacy notices), with options other than simply 'take it or leave it'.[5]

The Government should take these developments into account when determining the conditions with which parties planning to intercept users' communications on the basis of consent must comply when obtaining that consent. In particular, the Government should clarify that consent to such interceptions may not solely be implied through online providers' privacy policies or terms of business unless those providers ensure that users are aware of the right to intercept and have explicitly agreed to such a right (for example by ticking a box).

The right to refuse consent to intentional interceptions

The Government should also ensure that access to any communications services must not be made conditional on users granting communications service providers a right to intercept their communications for their own commercial (except technical and operational) purposes. It is particularly likely that such situations will develop where, as in the case of the Phorm Webwise system, the interception of communications is necessary to support new revenue generation and monetisation strategies employed by the providers and their business partners. If service providers were given such a right, it is - again - to be expected that, over time, all of them would make the provision of their services conditional on users' acceptance of a right of the provider to intercept users' communications. It would thus become an industry standard.

This could ultimately lead to a situation where users may not be able to find a service provider willing to provide the service without the users granting it a right to intercept. This would leave individuals that wished to enter into an agreement with a communications service provider in a situation where they would have to

agree to the interception of their communications in order to obtain the service. At a time when access to the internet has become an essential aspect of most people's lives - it facilitates not only economic and social activities but also education and political participation - the Government should not allow a situation to develop where users would effectively have to choose between internet access and the secrecy of their communications. This would not only severely impact on users trust in the communications infrastructure, it would most likely also amount to a violation of users' fundamental human rights, which might, in turn, become the trigger that would require Government to protect and promote individuals' rights by more formally restricting such general monitoring practices.

Recommendation:

The Government should:

- remove the words 'has reasonable grounds for believing' from section 3(1) of RIPA.
- require the relevant regulator to provide clear and comprehensive guidance to providers, for example in the form of a code of practice, on the way in which and the purposes for which consent to interceptions must be obtained.
- ensure that the revised RIPA provisions are drafted in a way which make it clear that users must be free to withhold consent to the interception of their communications even in a contractual relationship without suffering a loss of service as a consequence.

Question 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?

The Government's 'recommended option' for a new civil sanction for unintentional interceptions raises a number of substantive concerns which need to be addressed.

Unintentional interceptions

Article 5(1) of the *E-Privacy Directive* states that '[m]ember [s]tates shall ensure the confidentiality of communications [...] by means of a public communications network and publicly available electronic communications services, through national legislation'. The authors agree with the Government that the confidentiality of communications will be affected by both intentional and unintentional interceptions and that, consequently, this requirement has not been properly implemented through section 1(1) of RIPA which only relates to intentional interceptions.

However, the authors fail to see why the Government has come to the conclusion that the Directive only imposes a requirement to extend legal sanctions for unintentional interceptions to interceptions carried out by communications service providers. As the recent events relating to the interception of individuals' communications by Google in the course of its mapping of WiFi routers has shown beyond doubt, it is feasible for such unintentional interceptions to be committed by non-CSPs. Despite the fact that communications were clearly intercepted, it has proved impossible to prosecute Google for their actions under the existing RIPA regime. Were the Government to proceed with its current proposals without amendments, it would still not be possible to prosecute such actions under the revised regime. This cannot be the desired policy effect, neither with a view to the need for the proper implementation of the *E-Privacy Directive* nor from the perspective of thousands of users who were understandably upset and angered that a company was able to show such disrespect for the secrecy of their communications and was able to 'get away with it'.

Criminal versus civil sanctions

While criminal sanctions for unintentional interceptions are likely to have more of a deterrent effect, the authors agree with the Government that criminal sanctions consisting merely of a potential fine would impose a considerable resource burden on the police and would be unlikely to be appropriate from a public policy point of view.

Level of proposed fine

However, the authors are not convinced that a civil fine of up to £10,000 will be sufficient to persuade businesses to take the necessary measures to ensure that no such unintentional interceptions will take place. Depending on the size of the business in question, the cost of putting in place appropriate organisational and security measures, staff training, equipment etc. may very well exceed the potential fine by some margin, meaning that providers will have little incentive to invest in these measures and will most like rely on not getting caught. In addition, the proposed fine compares unfavourably with similar sanctions that are available, for example, in the area of data protection breaches (up to £500,000) and competition (up to 10% of worldwide turnover). Breaches of the confidentiality of communications, even unintentionally through negligence or recklessness, have severe implications for the rights of individuals as well as for the public interest because it may damage the public's trust in the communications infrastructure. This would have consequences for both citizens' economical and political participation. In the event that a civil sanction is introduced, the Government should therefore consider raising the fine to a level that is more commensurate with the potential harm caused by unintentional interceptions and with fines currently levied in comparable regulatory contexts. The fine to be imposed should be variable and measured against the severity of breach and the ability of the offender to pay.

Other regulatory sanctions

The government should also explore the use of other regulatory sanctions. For example, the 2009 *Citizens' Rights Directive* amended the *E-Privacy Directive* by introducing a requirement for communications service providers to notify the national regulator of any personal data breach. In cases where the personal data breach is likely to adversely affect the personal data or privacy of an individual user, the provider must also notify the user of the breach without undue delay. [6] These requirements were introduced because it was widely accepted that the damage to the reputation which would occur if a providers has to publicly admit that it did not take appropriate steps to protect users' personal data was a far more effective deterrent than the threat of a fine. The European Commission, in the context of its review of the general EU data protection regime , is currently considering whether to extend the security breach notification regime to all data controllers.[7] In light of the similarity between the impact of a data security breach and an interception of communications it is suggested that a more general notification requirement including notification of unintentional interceptions of communications should be introduced under the oversight of the relevant regulator (see below).

Recommendations:

The Government should:

- increase the level of the proposed fine to an amount that is more likely to represent a real deterrent. For example, it would be prudent to impose fines comparable to those which may be levied for serious personal data security breaches. Fines should be variable and measured against the severity of breach and the ability of the offender to pay.
- explore the use of other regulatory sanctions like, for example, the introduction of an 'unintentional interception breach notification requirement'.

Oversight

To begin with, the authors would like to express their surprise that the Government has decided not to specifically consult on the question which authority should oversee the new regime. This is despite the fact that the reference of the UK to the ECJ by the European Commission includes a clear concern that there is currently no independent national authority to supervise the interception of some communications. Although the Government proposes to task the Interception of Communications Commissioner (IoCC) with overseeing and implementing the new sanction for unintentional interceptions of communications, it has not made this fundamental policy decision an official part of the consultation process. However, this decision can be criticised in two important respects.

First, the current function of the IoCC is strictly limited to oversight of the conduct of a limited number of public bodies and those communications service providers that act at the request of those public bodies. The Commissioner's function is to review the exercise and performance by those bodies of the powers conferred on them under RIPA. The Commissioner discharges his duties through the detailed investigation of a selection of authorised interceptions and through the publication of an annual report. His function is not to increase the transparency to the public of the way in which these interceptions are carried out but to assure the public that the legal requirements are being complied with while at the same time keeping the details of the interceptions secret. While this form of 'commissionary' legal protection may be necessary in relation to interceptions authorised by the police and security services in the interests of national security and investigating serious crime (and there is some doubt about that), it is entirely unsuitable in relation to interceptions carried out by private entities without legal authorisation. As already pointed out above, these kinds of interceptions need to be made public to ensure that those carrying out unlawful interception will be prosecuted and to give users the opportunity to draw their own conclusions from the private entity's behaviour. The transparency required in relation to the oversight of interceptions by private entities is therefore entirely alien to the culture of secrecy that currently dominates the work of the IoCC. The authors believe that it would be more appropriate, if oversight of private entity interceptions was assigned to the Information Commissioner's Office (ICO) which is experienced in reviewing the conduct of private entities and which has the necessary procedural and organisational structures in place to take on this additional function without having substantially to adapt its own 'corporate culture'. Unless the IoCC managed to keep the oversight regimes for public and private bodies entirely separate, it is unlikely that one regime that requires the IoCC to maintain complete secrecy will be able productively to coexist with another regime that by definition must strive for the utmost transparency.

Secondly, the Government should take into account that every instance of unlawful interception by a private entity (whether intentional or unintentional) will in almost all cases also constitute a breach by that entity of data protections laws. This means that in such a case, for example the interceptions of communications carried out by Google Streetview, the Information Commissioner will already be required to investigate the incident with a view to imposing the necessary sanctions under the *Data Protection Act 1998*where appropriate. It seems to be counter-productive to introduce a parallel oversight regime which would effectively require the same incident to be investigated and sanctioned by two different Commissioners thereby providing for a costly, time-consuming and confusing duplication of effort. This argument is further supported by the fact that the ICO is very aware of the existing gaps in oversight in relation to private entity conduct and, despite his lack of an official oversight role already provides guidance in relation to interception of communications where this overlaps with issues of data protection. For example, Part 3 of the ICO's Employment Practices Code includes detailed supplemental guidance about the way in which the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000* are to be applied. [8]

Recommendation:

Government should consider whether the oversight function in relation to interceptions of communications by private entities might not more effectively sit with the ICO rather than the IoCC.

Oversight procedure

The procedure for imposing sanctions in cases of unintentional interceptions included in the proposals is generally acceptable in relation to incidents which have come to the regulator's attention. However, the Government's proposals do not address the way in which the regulator might learn about those interceptions.

Except for the review of the conduct of public bodies, and private entities acting under their authority, the current regime relies almost exclusively on receiving complaints from users who suspect that their communications might have been intercepted. Part IV of RIPA established the Investigatory Powers Tribunal as a means of receiving such complaints under section 7(1)(a) of the *Human Rights Act 1998*and to provide redress to individuals. This retrospective form of review has already been criticised even in relation to interceptions carried out by or on behalf of public authorities under warrant. For example, Ferguson and Wadham argue that '[r]etrospective review is likely to be less rigorous than prior scrutiny and it may well be

easier to satisfy the requirements of necessity and proportionality when armed with the incriminating results of the surveillance' .[9]

However, while there may again be national security justifications for retrospective review in relation to interceptions by public bodies, this form of oversight is wholly unsuited to interceptions by private entities. The very nature and logic of interceptions means that individuals will rarely be aware of the fact they are being observed. This is borne out by the fact that in the years from 2006-2009 the Investigatory Powers Tribunal received only between 66 and 176 complaints per year. Of those complaints only four were upheld. While the Government might argue that these figures imply that most interceptions are carried out lawfully, experiences like the Phorm Webwise system and the Google Streetview incident suggest that there is a massive grey area where interceptions may take place without ever coming to the attention of the user. In order to ensure that the UK complies with the call by the European Commission for the establishment of an independent national authority to supervise the interception of communications by private entities, it must equip the relevant authority with the necessary tools proactively to monitor and detect infractions. This means that the regulator should be given full auditing powers - including dawn raid powers, if necessary and sufficient resources to carry out this vastly more demanding role. The mere introduction of a right to serve suspected offenders with information, enforcement and penalty notices is unlikely to be sufficient. As before, parallels may be drawn with the regulatory regime operating in the area of data protection. The ICO has recently been granted additional powers to serve assessment notices on certain data controllers and to carry out compulsory data protection audits where it suspects that severe breaches of data protection law have taken place. Equivalent powers should be considered as part of the newly established oversight regime for interceptions of communications by private entities.

Recommendation:

The Government should provide the relevant regulator with additional powers to inspect and audit private entities suspected of carrying out unlawful interceptions of communications.

Question 3
Are there any other options that the Government should consider or are there any changes that should be made to the recommended options?

Government's assessment that the safeguards contained in RIPA together with the oversight of the IoCC and an effective inspection regime ensures that the appropriate checks and balances are in place is incorrect.

Intentional interceptions by private entities

A supervisory gap currently exists not only in relation to unintentional interceptions but also in relation to the intentional interception of communications by private entities for their own commercial purposes. While the IoCC is currently charged with reviewing the exercise and performance by public bodies of the powers conferred on them under RIPA, no comparable supervisory regime exists in relation to intentional interceptions by private entities. As pointed out above, the only means of enforcement available to users in this context is the right to bring a claim before the Investigatory Powers Tribunal. This form of retrospective review is in stark contrast to the robust regulatory regime that exists in relation to the protection of personal data. As a result, companies like Phorm were able intentionally to intercept the communications of large numbers of internet users without being subject to any form of regulatory oversight.

This is unlikely to comply with the requirements of the *E-Privacy Directive* and, indeed, the European Commission's decision to refer the UK to the EU's Court of Justice is a direct reaction to complaints brought forward by civil society organisations and individual citizens in response to trials carried out by Phorm and various UK telecommunications providers which involved the intentional interception of communications. The European Commission clearly believes that the current UK regime does not comply with the EU requirement for independent regulatory supervision.

Recommendation:

The Government should ensure that the body which will eventually be charged with overseeing private entity interceptions should be required to carry out that role in relation to both intentional and unintentional private entity interceptions to avoid continuing gaps in regulatory supervision.

Prior notification requirement

To facilitate the supervisory role of the relevant regulator in relation to intentional interceptions, the Government should consider introducing a prior-notification requirement for such interceptions by private entities, along the lines of the register of data controllers. Although notification in the area of data protection has been widely criticised for encouraging mere 'tick-box' compliance, the situation in the case of intentional interceptions is somewhat different.

To begin with, it is almost certain that fewer private bodies will be engaged in the intentional interception of communications than in the processing of personal data. The regulatory burden for industry as a whole and the administrative burden for the regulator would therefore be very small. Secondly, notification would considerably improve the regulator's ability to monitor, detect and intervene in cases of unlawful interceptions. For this reason, the notification requirement should include notification of interceptions for technical and operational purposes which are permitted under RIPA and the *E-Privacy Directive*. Thirdly, the regulator would be able to enforce violations of the notification requirement as a separate offence. This would act as a deterrent designed to keep private bodies from carrying out intentional interceptions in secret.

Recommendation:

The Government should introduce a prior notification requirement for intentional interceptions by private entities for their own commercial (including technical and operational) purposes.

Question 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?

Subject to the recommendations made in relation to

- the authority that should be responsible for overseeing the interception of communications by private entities; and
- the powers that should be granted to that authority to ensure effective oversight

appeals from any decision made by the relevant regulator in respect of any finding of unlawful interception by private entities should be made to the First-tier Tribunal. Appeals should be permitted both by the person alleged to have unlawfully intercepted communications and by the individual whose communications were so intercepted.

Question 5
What, if any, additional costs would these proposed changes impose on Communication Service Providers or others?

No response is submitted to this question.

Annex 1

List of Recommendations

1. The Government should:
   - remove the words 'has reasonable grounds for believing' from section 3(1) of RIPA.

- require the relevant regulator to provide clear and comprehensive guidance to providers, for example in the form of a code of practice, on the way in which and the purposes for which consent to interceptions must be obtained.
- censure that the revised RIPA provisions are drafted in a way which make it clear that users must be free to withhold consent to the interception of their communications even in a contractual relationship without suffering a loss of service as a consequence.

2. The Government should:
   - increase the level of the proposed fine to an amount that is more likely to represent a real deterrent. For example, it would be prudent to impose fines comparable to those which may be levied for serious personal data security breaches. Fines should be variable and measured against the severity of breach and the ability of the offender to pay.
   - explore the use of other regulatory sanctions like, for example, the introduction of an 'unintentional interception breach notification requirement'.
3. The Government should consider whether the oversight function in relation to interceptions of communications by private entities might not more intuitively sit with the ICO rather than the IoCC.
4. The Government should provide the relevant regulator with additional powers to inspect and audit private entities suspected of carrying out unlawful interceptions of communications.
5. The Government should ensure that the body which will eventually be charged with overseeing private entity interceptions should be required to carry out that role in relation to both intentional and unintentional private entity interceptions to avoid continuing gaps in regulatory supervision.
6. The Government should introduce a prior notification requirement for intentional interceptions by private entities for their own commercial (including technical and operational) purposes.

---

[1] See http://www.homeoffice.gov.uk/publications/consultations/ripa-effect-lawful-intercep/ripa-amend-effect-lawful-incep?view=Binary) This response has been approved by the Executive of BILETA (the British and Irish Law, Education and Technology Association (http://www.bileta.ac.uk/default.aspx) and is therefore submitted on behalf of BILETA.

[2] Ms Judith Rauhofer specializes in cyberlaw, online privacy and data protection. She is dually qualified in Germany and the UK as a Rechtsanwältin and Solicitor respectively and has spent five years working in legal practice. She is currently employed as data protection editor by an online legal information service in London while completing a doctoral thesis on the human rights implications of data retention at the University of Vienna. She has held a number of academic positions; most recently she worked as a Research Fellow for the Centre of Law, Information and Converging Technologies at the University of Central Lancashire. She is a member of the Executive of the British & Irish Law, Education & Technology Association (BILETA). Important contributions to preparing the response were also made by Dr. Ian Walden, Queen Mary, University of London, Dr Ian Brown, Oxford Internet Institute, University of Oxford, Professor Burkhard Schafer, SCRIPT, University of Edinburgh, Dr Abbe Brown, SCRIPT, University of Edinburgh, Prof. Joe Cannataci, CLICT, University of Central Lancashire, Prof. Lilian Edwards, University of Strathclyde, Glasgow

[3] Article 29 Working Party, Working Document on a common interpretation of Article 26(1), adopted on 25 November 2005, WP114.

[4] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "A comprehensive approach on personal data protection in the European Union", 4 November 2010, COM(2010) 609 final; available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, last visited 10 December 2010.

[5] Summary of responses to the public consultation 'Priorities for a new strategy for European information society (2010-2015)', 19 May 2010, 13, at http://ec.europa.eu/information_society/digital-agenda/documents/consultationresponses.pdf (last visited 10 December 2010)

[6] 2009/136/EC

[7] See, the Commission's Communication *'A comprehensive approach on personal data protection in the European Union'*, at note 4 above.

[8] Information Commissioner's Office, Employment Practices Code, Part 3, See Supplementary Guidance for more information about the Lawful Business Practice Regulations; available athttp://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/supplementary_guidance/monitoring_at_work_3.html, last visited 11 December 2010.

[9] G Ferguson and J Wadham, 'Privacy and Surveillance: A Review of the *Regulation of Investigatory Powers Act 2000*' [2003] EHRLR Suppl (Special issue: privacy) 101, 105.