



**Consumer
Focus**
Campaigning for a fair deal

Consumer Focus response to the Home Office consultation of Investigatory Powers Act 2000: proposed amendments affecting lawful interception

December 2010

About Consumer Focus

Consumer Focus is the statutory consumer champion for England, Wales, Scotland and (for postal consumers) Northern Ireland.

We operate across the whole of the economy, persuading businesses, public services and policy makers to put consumers at the heart of what they do.

Consumer Focus tackles the issues that matter to consumers, and aims to give people a stronger voice. We don't just draw attention to problems – we work with consumers and with a range of organisations to champion creative solutions that make a difference to consumers' lives.

Introduction

We welcome the Home Office consultation that addresses the issue of deficiencies in the implementation of the Data Protection Directive and the ePrivacy Directive into the UK legislation under the Regulation of Investigatory Powers Act 2000 with regard to interception of communication.

The ability to lawfully intercept communication and obtain communications data is critical to combating terrorism, and serious and organised crime, such as child sex abuse, kidnap and murder.¹ Such activities are subject to relevant laws that include the:

- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Anti-Terrorism, Crime & Security Act 2001
- Human Rights Act 1998
- Electronic Communications (Universal Service) Order 2003
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- ePrivacy Directive (EC Directive) Regulations 2003 and the European Union's Data Retention Directive

Consumer Focus recommends:

- that in relation to serious crime only law enforcement agencies should be given the appropriate powers under EU and UK law to undertake lawful interception of communication and to obtain communications data retained by communication service providers (CSPs) that include providers of value added communication services capable of applying interception techniques
- that under no circumstances should CSPs and other applicable service providers be allowed or forced to retain data and release such data to private agents or companies
- that the right of citizens and consumers not to have their communication intercepted by private agents or companies without their consent should be safeguarded

According to the European Data Retention Directive (Directive 2006/24/EC):

'Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive.'

¹ Telecommunications: Databases, Written question James Brokenshire, Answer Mr. Coaker, 8 October 2008; <http://www.parliament.the-stationery-office.com/pa/cm200708/cmhansrd/cm081008/text/81008w0012.htm>

*The adoption of an instrument on data retention that complies with the requirements of Article 8 of the European Convention on Human Right is therefore a necessary measure.*²

Article 8 of the European Convention secures citizens 'and consumers' right to privacy. The objective of the Directive is to 'harmonise the obligations on providers to retain certain data and to ensure that those data are made available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law'.³

According to the Privacy and Electronic Communications Directive (e Privacy Directive 2002/58/EC) and the Data Retention Directive CSPs are not allowed to retain data, such as IP address logs, other than for the purpose of transmitting the communications, billing purposes, and where required to do so in relation to 'serious crimes' as defined by UK law and in compliance with the European Convention on Human Rights.⁴ However Consumer Focus is concerned that obligations are placed on CSPs to retain data for matters not relating to serious crime. For example, section 3 to 16 of the Digital Economy Act 2010 place a duty on CSPs such as internet service providers to retain and release IP address logs to copyright owners and their agents for the purpose of the pursuit of civil copyright infringement by consumers without a court order.

The interception of communications should be limited to law enforcement agencies and undertaken in compliance with all relevant laws as a matter of principle. UK citizens and consumer are within their rights under EU law to not have their communication intercepted by private agents and companies without their consent. And it is the responsibility of the UK Government to safeguard this right. In this respect the European Commission has recently referred the UK to the European Court of Justice in relation to the improper implementation of EU data protection, retention and privacy laws. In doing so the UK has effectively allowed BT and Phorm to run two secret trials in 2006 and 2007 on its broadband customers using deep-packet inspection technology for the purpose of behavioural advertisement. Such interception of communication is not lawful under EU law, unless undertaken for legitimate law enforcement purposes, or with the consent of the consumers concerned. As the European Commission stated, when making the referral to the European Court of Justice, it is the responsibility of the UK Government to ensure the confidentiality of the communications and related traffic data by prohibiting unlawful interception and surveillance.⁵

² Data Retention Directive, Recital 9; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>

³ Data Retention Directive, Recital 21; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:P>

⁴ Privacy and Electronic Communications Directive, Article 5, 6 and 9 and Data Retention Directive, Article 1(1) and recital 20; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>

⁵ Digital Agenda: Commission refers UK to Court over privacy and personal data protection, European Commission press release, 20 September 2010; <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215&format=HTML&aged=0&language=EN&guiLanguage=en>

Issues of concern

Means of executing 'freely given specific and informed' consent

We welcome the Home Office proposal to remove the legal ambiguity with regard to 'consent' for interception of communication. It aims to ensure that its definition is consistent with the definition of 'consent' provided by Article 5(1) of the ePrivacy Directive and Article 2(h) of the Data Protection Directive. However we are disappointed that the Home Office proposal failed to shed light on its intentions on how this law will be implemented in practise.

We fear that the proposed change will do little to improve the existing situation on seeking user's consent on lawful interception of communication unless transparency rules on seeking consumers consent improve dramatically. We would like to point out that the existing transparency rules, ie the legal obligations to inform consumers and citizens (data subject) about the collection and processing of personal data do not work. Many privacy policies, particularly those of online service providers, do not abide by the compulsory transparency rules, many do not have privacy policies at all.

The vast majority of consumers do not read privacy notices, because they are long, over-complicated, incomprehensible and obscure on vital issues, such as what third parties data is shared and who these third parties are or what they intend to do with the data. Often they are difficult to find, or concealed as a clause within general terms and conditions. Therefore in our view allowing consent on such privacy sensitive issue as interception of data will not work unless the existing model of privacy notices to consumers will become more transparent and provide for meaningful consent. Our recommendations are inline with the Recital 25 of the revised ePrivacy Directive that requires notices to be provided in a 'clear and comprehensive' manner and 'as user friendly as possible'.

The issue of informed consent has been recently raised in the context of the implementation of the cookie provision under the revised ePrivacy Directive that requires providers of electronic communications services to seek users' consent before installation of cookies on the users' terminal. The Article 29 Working Party in its opinion on seeking consumers' consent on the installation of cookies considered that:⁶

'...providing a minimum of information directly on the screen, interactively, easily visible and understandable, would be the most effective way to comply with this principle. It is important for information to be easily accessible and highly visible. This essential information may not be hidden in general terms and conditions and/or privacy statements'.

In its opinion the Article 29 Working Party concluded further that the informed consent on the installation of cookies requires active participation of the user to grant consent and simply assumed or implied will of data subject would not comply with legal requirement of consent.⁷ Hence the Article 29 Working Party recommended that CSPs are required to seek active consent of users' that can be exercised via pop in boxes on computer's screen with 'opt in' option.⁸

⁶ <http://bit.ly/eMnOmm>, p.18.

⁷ <http://bit.ly/eMnOmm>

⁸ <http://bit.ly/eMnOmm>

We strongly recommend this model is adopted by communication service providers and other relevant stakeholders that process or store personal data in relation to seeking consent with regard to data interception.

In addition we recommend the Home Office ensures that additional conditions are taken into account when obtaining consent for data interception that include:

- consent is obtained freely and not conditional to granting user's right to use a service
- consent is given for a limited period of time
- the user has the right to revoke given consent
- special safeguards are in place to protect children against data interception

The need to extend the application of RIPA beyond CSPs

We do not share the Home Office view that the application of RIPA under the scope of the ePrivacy Directive should be limited to CSPs. We would like to refer the Home Office to the Opinion of the Article 29 Working Party of 2008 that ruled out that Article 5(3) of the ePrivacy Directive is a general provision, which is applicable not only to electronic communication services but also to any other services when the respective techniques are used such as for example search engines.⁹ Furthermore the revised ePrivacy Directive Article 5(3) is technologically neutral, therefore according to the 29 Working Party, it is applicable to any technology used to store or gain access to information stored in their individuals' technical equipment such as cookies, behavioural advertising, spyware, malware and others.¹⁰

Therefore Consumer Focus recommends the Home Office to extend the applicability of RIPA provisions to all relevant providers of information society services in order to comply with the requirements of the revised ePrivacy Directive.

Civil sanctions

We agree with the Home Office rationale to apply civil sanctions for electronic communication providers that carry out unlawful data interception.

However we strongly recommend that any civil sanction proposed by the Home Office should be **effective, proportionate** and **dissuasive**.

In our view the proposed fine of up to £10,000 would fail to meet such requirements. Hence we strongly recommend the Home Office to reconsider its proposal to meet the three essential criteria mentioned above.

Enforcement

We recommend the Home Office re-examines its proposal of placing the responsibility for oversight and administrating the new sanction for unintentional interceptions of communications with the Interception of Communications Commissioner (IoCC).

We are concerned as to whether the powers and technical capabilities of IoCC will allow oversight of the provisions on data breach notification under the revised ePrivacy Directive that requires CSPs to notify data subjects in case of serious data breaches that can compromise privacy of data subjects that would apply also to cases of unintentional interception.

⁹ Opinion 1/2008 on data protection issues related to search engines, adopted on 4 April 2008.

<http://bit.ly/hbGH3Y>

¹⁰ <http://bit.ly/eMnOmm>

In our view such powers and technical capabilities lie within the Information Commissioner's Office (ICO) that is required in any case to investigate unlawful interception by private entities. Hence to avoid duplication and for costs effective purposes we recommend the oversight function to be aligned with ICO.



Consumer Focus response to the Home Office consultation of Investigatory Powers Act 2000: proposed amendments affecting lawful interception

If you have any questions or would like further information about our research, please contact Marzena Kisielowska-Lipman, by telephone on 020 7799 7981 or via email marzena.kisielowska-lipman@consumerfocus.org.uk

www.consumerfocus.org.uk

Copyright: Consumer Focus

Published: December 2010

If you require this publication in Braille, large print or on audio CD please contact us.

For the deaf, hard of hearing or speech impaired, contact Consumer Focus via Text Relay:

From a textphone, call 18001 020 7799 7900

From a telephone, call 18002 020 7799 7900

Consumer Focus

4th Floor
Artillery House
Artillery Row
London SW1P 1RT

Tel: 020 7799 7900

Fax: 020 7799 7901

Media Team: 020 7799 8004 / 8005 / 8006