



**Consumer
Focus**
Campaigning for a fair deal

Response to Ministry of Justice call for evidence on the current data protection legislative framework

October 2010

About us

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

We operate across the whole of the economy, persuading businesses and public services to put consumers at the heart of what they do. Consumer Focus gives a strong voice to consumers on the issues that matter to them and works to secure a fair deal on their behalf.

We work with consumers and a range of organisations to tackle the problems customers face and to achieve creative solutions that make a difference to people's lives.

Preliminary comments

We welcome the Ministry of Justice (MoJ) call for evidence on the current data protection legislative framework prior to the detailed review of the EU Data Protection Directive which is scheduled for next year. We are the consumer champion; therefore our answers to the MoJ questions are given from a consumer rights perspective, from the perspective of the people (or 'data subjects') whose personal information (or data) is being processed.

As a preliminary, and important, remark, we emphasise that the Data Protection Directive and the related UK Data Protection Act (DPA) is one of the instruments that deals with management of personal information. On its own it is unlikely to be sufficient, as it needs to be considered in harmony, conforming to and supporting other important pieces of legislation safeguarding the fundamental right to privacy, as expressed in Article 8 of the European Convention of Human Rights (enshrined in the UK Human Rights Act) and Article 8 of the EU Charter of Fundamental Rights which became legally binding with the signing of the Lisbon Treaty in 2009. This means that the basic data protection rules and principles now have constitutional status. In addition, the DPA is complemented by the Privacy and Electronic Communications Regulation (2003), which will be revised during 2011 to conform to the revised and strengthened e-privacy legislation in the Telecoms Package¹. Therefore, while legalistic and material harm evidence, as required in many of the questions in this questionnaire are undoubtedly important, the MoJ must also bear in mind in analysing the evidence provided, that issues of fundamental rights to privacy, and consumer confidence on how those rights are safeguarded are just as important.

Consumer attitudes to, and awareness of, privacy and data protection should form an important part of the evidence for any future review, though the detailed questions below do not really allow for such evidence to be provided. This includes, for example, the Information Commissioner's Office's (ICO) own annual tracking report on individual attitudes and awareness of data protection. The latest of these (2009) shows an overwhelming majority of respondents were concerned about how information is handled (93 per cent of respondents are concerned about protecting people's information (up 23 per cent since 2004). The public is also showing high levels of concern about the potential mismanagement of their information, with the two highest concerns being passing or selling personal details to other organisations (97 per cent) and security (96 per cent)². Clearly public perception is a vital factor in assessing the effectiveness and importance of a piece of legislation, and is part of the impact assessment and business case for effective privacy protection. Furthermore consumers' concern over safety of personal data may undermine their confidence to engage in the use of new technologies, such as e-commerce or online public services³.

¹ The Department of Business Innovation and Skills is currently consulting on the implementation of the new Revised Framework Directive, including amendments to the e-privacy legislation such as the new rule of mandatory notifications for personal data breaches and prior consent of the user to the installation of cookies on users' computers. See <http://bit.ly/dtYVa3>.

² ICO, Annual Track 2009, 4.1 and 4.2.

³ See for eg Office of Fair Trading recent study of e-commerce that confirms some of these concerns <http://bit.ly/aaeRZz>.

Specific questions

Question 1. What are your views on the current Data Protection Act and the European Directive upon which it is based? Do you think they provide sufficient protection in the processing of personal data? Do you have evidence to support your views?

Overall we strongly support the principles based approach, and the principles themselves, of the EU Data Protection Directive and the UK DPA on which it is based. However we think that the application of this legal framework no longer adequately meets the challenges outlined in the call for evidence document (developments in technology and globalisation, merging of EU pillars). Both are no longer fit for purpose both in terms of powers and in terms of enforcement. Our main concerns are:

- The rights of consumers (data subjects) are increasingly abused and it is very difficult for ordinary people to identify and correct errors, which may only become apparent when something goes seriously wrong. There is also very little that consumers can do if their data is disclosed deliberately, hacked into or lost through negligence. There is no easy way for consumers to know what data is held about them; there is also no easy way for consumers to get their data deleted with no need to prove damage or abuse⁴
- When these rights are breached, consumers do not receive redress. The remedies provided on complaint to the ICO are very limited, while litigation is not practical and very expensive for the majority of people, so in reality civil actions are rare or non-existent. Furthermore, if the harm is done when information is stored or transferred overseas, there are questions of applicable law as well as other practical barriers. There is no possibility for group action which would help in one go many consumers whose personal information has been disclosed illegally for example⁵

An 'abysmally low' level of compliance with data protection law by 'data controllers' and 'data processors'. For example the transparency rules – ie the legal obligations to inform consumers and citizens (data subjects) 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.

⁴ See inter alia: New Challenges to Data Protection, Final Report, European Commission – DG JFS, January 2010, page 45, also Annex 6, United Kingdom Country Study, <http://bit.ly/bkJsSx>. Also Data Sharing and data protection – National Consumer Council's response to the Data Sharing Directive, February 2008, <http://bit.ly/as9VK4> and more generally evidence provided in the Consumer Focus response to ICO consultation on a Code of Practice for personal information online, March 2009, <http://bit.ly/auMbTY>.

⁵ Ibid. Regarding applicable law, see also BEUC answer to the consultation on the EU General Data Protection Framework, Dec 2009, page 7, <http://bit.ly/aQoL0Q>.

The vast majority of consumers do not read privacy notices, because they are long, over-complicated, incomprehensible and obscure on vital issues, such as with what third parties data is shared and who these third parties are or what they intend to do with the data⁶

- There are no legal responsibilities for third parties, with the result that many companies collecting personal data pass it on to third parties that often process this data for different purposes from those initially notified by the data controller. Distinctions between data controllers, data processors and third parties are increasingly blurred. The regulatory framework neglects altogether the area of liability for third party data loss and negligence⁷
- Lack of meaningful user control. In practice consumers often sign away control of their data, as picking out the default option is a typical human characteristic (behavioural economics) and especially in the UK data protection law, implied consent is permitted. Research shows that even when consumers don't mind giving away personal information for certain purposes, such as behavioural advertising, they still like to know what is going on and have control over what goes on⁸
- Very poor enforcement of the legislation. The ICO is under-resourced both in powers and resources; it appears to have fewer powers to investigate and enforce the law than its counterparts in other EU countries, although it does now have the power to audit government departments and its fine levels have been increased for serious cases⁹
- The UK's DPA does not implement European law properly. There has been criticism from the EU as far back as 2007 that the UK has failed to fully implement the current EU Data Protection Directive, in roughly a third of its articles including the powers of the ICO. These relate to, inter alia, the articles about definitions of personal data, conditions when sensitive data can be processed, fair processing notices given to individuals, rights granted to data subjects, and ability of individuals to seek a remedy, which have not been properly implemented¹⁰. The UK government has not shed light on these claims except to say that they are being investigated. However the European Commission recently acknowledged this fact with a public call to the UK to strengthen its data protection laws, followed by the recent announcement of referral to the European Court of Justice¹¹. Recent in-depth academic comparative analysis for the Commission confirms these claims (see list of references below)

⁶ See inter alia Research report: Fair Processing Notification, current effectiveness and opportunities for improvement, IC, 2007 <http://bit.ly/9A0siR>. See also for eg study by the Consumer Council of Norway which shows consumers generally do not understand terms offered on social networks, <http://bit.ly/a2rNMg>; also Fair Game? Assessing commercial activity on children's favourite websites and online environments, National Consumer Council and Childnet, 2007, <http://bit.ly/dffkJI>. The study shows that a quarter of third-party advertiser sites do not have privacy policies, while children and their parents do not read or understand them.

⁷ Eg about 350,000 third party applications are offered through Facebook, which by default have access to user information.

⁸ Private lives, a people's inquiry into personal information, by Peter Bradwell, Demos, with support from Consumer Focus and the Information Commissioner's Office, March 2010.

⁹ See in particular the European Commission DG JFS report (note 4 above), Annex 6, United Kingdom Country Study.

¹⁰ The claims were first reported in 2007, following a FoI request to the European Commission, see www.out-law.com/page-8472.

¹¹ See <http://bit.ly/de3c2W> and <http://bit.ly/cmlUIJ>.

- The difference in definition of personal data in DPA and the Data Protection Directive has caused particular tension in relation to the question whether IP addresses are personal data in the context of copyright enforcement. According to the UK definition of personal data, an IP address would only be considered personal data if combined with other information, though this definition is not supported by European data protection officials. The difference in definition has led to considerable problems when the Digital Economy Bill passed through parliament and as a result Section 3 to 16 of the Digital Economy Act 2010 is potentially in breach of the Directive and/or cannot be implemented in compliance with the Directive
- Export of UK consumer personal information to third countries (outside EU) with weaker data protection legislation, and legal uncertainty regarding applicable law and the competent jurisdiction. This issue is increasingly acute with the advent of 'cloud computing', as well as extensive use of call centres outside the EU. It is also compounded by the EU's slow process of confirming which countries have adequate data protection legislation (the adequacy test) and by the very poor implementation of the US-EU Safe Harbour agreements, whereby US companies who want to do business with the EU self-certify that they adhere to the EU data protection principles. In fact, currently many companies based outside the EU but who do extensive business in the UK, such as search engines or major networking sites, claim that they're subject to their national laws, most often the US¹²

Question 2. What are your views of the definition of 'personal data', as set out in the Directive and the DPA?

The definition of personal data is narrower in the DPA than set out in the Directive, though even the latter no longer addresses fully the capabilities of new technologies, as well as globalisation. It is now virtually impossible to anonymise fully any personal information. A good example of this is the case of AOL Research in 2006 which released twenty million 'anonymised' search key words for over 650,000 million users over a three-month period; within days the New York Times was able to identify an individual from the released anonymous search records by cross-referencing them with phonebook listings¹³. This was a relatively simple case of cross-referencing; modern technologies and techniques able to match 'data shadows' left by individuals to build a comprehensive picture of their profile and life, make the task even easier. There is a need therefore to expand the definition of what is personal data and the ways an individual may be identified online in order to keep pace with technological development. So called anonymised data can be used to identify individuals¹⁴.

Moreover, the difference in definition of personal data in DPA and the Data Protection Directive has caused particular tension in relation to the question whether IP addresses are personal data in the context of copyright enforcement. According to the UK definition of personal data, an IP address would only be considered personal data if combined with other information, though this definition is not supported by European data protection officials.

¹² On the lack of effectiveness of the EU-US Safe Harbor agreement, see for eg The US Safe Harbor – Fact or Fiction?, Chris Connolly, Galexia, 2008, <http://bit.ly/bpTKmS>.

¹³ <http://bit.ly/dxdscY>.

¹⁴ New Challenges to Data Protection, Final Report, European Commission – DG JFS, January 2010 (see note 4 above), page 28 'The serious problems stemming from the near-impossibility of full anonymisation of personal data in the new socio-technical global environment pose some of the most crucial challenges to data protection, and should be at the heart of any debate on a review of the European data protection regime'.

The difference in definition has led to considerable problems when the Digital Economy Bill passed through parliament and as a result Section 3 to 16 of the Digital Economy Act 2010 are potentially in breach of the Directive and/or can not be implemented in compliance with the Directive. We give full details on the tensions between data protection legislation and the Digital Economy Act in Annex 1 attached to this call for evidence¹⁵.

Question 3. What evidence can you provide to suggest that this definition should be made broader or narrower?

As well as the guidance provided on these issues by the WP29 in its Opinion on the concept of personal data¹⁶, the US Federal Trade Commission (FTC) for example has acknowledged that restricting protection to personally identifiable information does not recognise developments in profiling technology. The FTC state that both Personally Identifiable Information (PII) and non-PII raise privacy issues and so the distinction is no longer meaningful¹⁷.

Question 5. What evidence can you provide about whether biometric personal data should be included within the definition of ‘sensitive personal data’?

In the ICO 2006 tracking survey¹⁸, a majority of respondents considered biometric data as extremely sensitive, but felt religious beliefs, sexual orientation, etc were less so. The sensitive personal data list should become a non-exhaustive list, so as to add the biometric and other data that appear to be sensitive with technology development. Given the special characteristics of biometric data, in that it may be health and genetic related and also that it is a sort of universal ‘key’ in getting all kinds of personal information, it should be considered as sensitive personal data generally¹⁹.

Question 7. Are there any other types of personal data that should be included? If so, please provide your reasons why they should be classed as ‘sensitive personal data’?

Arguable there are types of personal information that should be classified as sensitive, for example personal financial and debt-related information (as is the case in some of the other EU member countries) and, a relatively recent development, the detailed hourly or half-hourly individual household energy consumption that can be revealed by smart meters being rolled out across the UK. The need for classification as ‘sensitive’ for the former is clear, particularly given the alarming rates of online fraud. With regard to the latter, as research has shown, detailed records of household energy consumption can reveal intimate details of its living habits and potentially result in fraud, crime and function creep.²⁰

¹⁵ See also **Consumer Focus response to Ofcom consultation – ‘Online Infringement of Copyright and the Digital Economy Act 2010 Draft initial obligations code’**, July 2010.

¹⁶ Opinion 4/2007 on the concept of personal data, 20 June 2007, WP136.

¹⁷ FTC staff report: Self-Regulatory Principles For Online Behavioural Advertising, February 2009.

¹⁸ <http://bit.ly/dCQNQn>.

¹⁹ See also the arguments and evidence in Identifying Legal Concerns in the Biometric Context, by Yue Liu, Norwegian Research Centre for Computers and Law, University of Oslo, published in Journal of International Commercial Law and Technology Vol. 3, Issue 1 (2008).

²⁰ See for eg Privacy and the New Energy Infrastructure, Elias L. Quinn, 2009, <http://bit.ly/VgQIj>.

Question 8: Do you have any evidence to suggest that the definitions of ‘data controller’ and ‘data processor’ as set out in the DPA and the Directive have led to confusion or misunderstanding over responsibilities?

In practice it is difficult for consumers to distinguish between a ‘controller’ and a ‘processor’, or a third party or a non-third party. These relationships are increasingly complex, for example with the advent of cloud computing or in multinational companies.²¹ Third parties can be added to a service or platform and governed just by the host’s website terms and conditions or by nothing at all. For consumers it is very difficult to follow the chain of responsibilities. Facebook for example has some 350,000 third party applications, which overall fail to be transparent about the fact that they collect users information and their friends’ personal data. Our research in the past has shown that third parties may not even display privacy policies or notices²²

Question 10: Is there evidence that an alternative approach to these roles and responsibilities would be beneficial?

There is wide opinion among experts that similar to other types of consumer contract terms, obligations and liability should be extended to data processors, whoever they are, including third parties. So for example social networking sites can be required to have contracts providing minimum standards of data protection when engaging third party service providers²³.

Question 23. Is there any evidence to support a requirement to notify all or some data breaches to data subjects?

The latest in the series of UK now famous data breaches is the recent security breach of legal firm ACS:Law, whereby the personal details of thousands of people alleged to have shared music or films illegally appeared online.²⁴ Those opposing data breach notification to data subjects argue that consumers cease to take notice of notification after a time, and quote legislation in many of the US states as evidence²⁵. These critics regard data breach notification as a means of reducing the number of incidents of fraud, for eg by enabling consumers to take safety precautions. However, data breach notification should not be regarded as a remedy in itself, but more as a deterrent and incentive to companies to strengthen their security processes. Companies are more likely to take note of the law if there is a risk to their reputation through data breach notification requirements. It is an additional and valuable security principle. Furthermore, this principle has already been established for the communications companies under the revised Telecoms Package legislation, so should be extended to other online businesses too²⁶.

Question 24. What would the additional costs involved be?

Most companies mass-market to their customers, the same can be done for security breach notification; we do not see a valid argument for large extra costs. Moreover,

²¹ This is also relevant in relation to developments in eHealth. In the NHS there are data controllers (in Scotland) at health board level and within GP practices for example, but as national products like the Emergency Care Summary are developed there can be a lack of a clearly identifiable data controller. In situations where the technology can get ahead of the governance arrangements this can be a problem.

²² See note 6.

²³ See note 4.

²⁴ <http://bbc.in/9bqv4o>.

²⁵ <http://bit.ly/lmi0c>.

²⁶ See note 1.

increased security is likely to save companies money in the long run, for example in fraud or reputation costs.

Question 29: What, if any, further powers do you think the Information Commissioner should have to improve compliance?

The recently increased powers of the ICO to impose larger fines for manifestly abusive cases of data breach and to audit government department practices are to be welcomed. However we think that as a start and as a minimum, the DPA should address the criticism of the European Commission regarding the powers of the Information Commissioner and comply with the existing Directive, before any review is discussed. This means the ICO should have the power to monitor and assess the adequacy of third countries' data protection; and that it should perform random checks on personal data processors, or enforce penalties following these checks²⁷.

Question 31. Do you have evidence to suggest the current principles-based approach is the right one?

The eight principles have stood the test of time, have been endorsed by the Organisation for Economic Co-operation and Development (OECD) via its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data²⁸, now in their 30th year, and have been increasingly adopted as a basis for legislation throughout the world, including throughout Asia and Africa, essential in an increasingly global environment. The notable exception is the US, where the principles' absence has emphasised the weakness of that country's data protection system²⁹. Furthermore, the the principles have the great advantage of being technology neutral and allowing for flexibility in the interpretation of the legislation according to the circumstances and the medium. However, with ever increasing sophistication of the technology, such as profiling and targeting, cloud computing, user generated content, etc, both their application and their interpretation will become increasingly challenging.

Question 32. Do you have evidence to suggest that the consent condition is not adequate?

The DPA does not give a definition of consent, which in the Directive is defined as freely given, specific and informed indication of a person's wishes. Definitions apart, in practice the requirement to obtain consumer consent before personal information is collected and processed is frequently and blatantly disregarded, particularly online. Surveys repeatedly show that a majority of consumers believe they have lost control of their data, while online privacy notices are seldom read or understood, so do not allow consumers to give meaningful consent³⁰. At the same time there are internet sites that give very detailed information to users on how to control the amount of data collected, which include complex tables with tick boxes on different functionalities (for example on social networking sites), or so-called dashboards or control panels increasingly used by advertising networks to allow users to opt-out of being profiled and targeted by marketing messages. All this is in the name of 'user empowerment'. However, behavioural economics research shows that few people have the time or inclination to do complex risk analysis of potential harms of privacy breaches, and in addition people tend to accept default settings – and default settings are often not privacy friendly. The EU Article 29

²⁷ See note 11.

²⁸ <http://bit.ly/9SW2IV>.

²⁹ See in particular New Challenges to Data Protection, European Commission – DG JFS (as in note 4), which includes a US country report.

³⁰ See notes 2 and 6.

Working Party has suggested in an opinion that privacy settings on social networking sites should therefore be set at maximum privacy by default.³¹

The issue of consent also arises in the health sphere where some data processing is done on the basis of implied consent. For example in cases where a GP refers a patient to hospital, it can be assumed that the GP will send information about the patient to the hospital. However if the NHS is setting up some new way of sharing information – for example the Care Summary Record – then if implicit consent is the basis of this, there needs to be really good evidence that people know about it.

Question 35: Do you have evidence to suggest that data subjects do or do not read fair processing notices?

The vast majority of consumers do not read privacy notices, because they are long, over-complicated, incomprehensible and obscure on vital issues, such as with 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. Numerous past efforts both by privacy commissioners and consumer organisations to encourage brief, plain English and visible statements, have resulted in only patchy improvements. A recent study carried out by the Consumer Council of Norway reveals that 73 per cent of users aged 15-30 rarely or never read privacy notices. Other studies, including one by the National Consumer Council in 2007 show similar results.³²

³¹ <http://bit.ly/9yh7Ju>.

³² See also Research report: Fair Processing Notification, current effectiveness and opportunities for improvement, IC, 2007 <http://bit.ly/9A0siR>. The study by the Consumer Council of Norway shows consumers generally do not understand terms offered on social networks, <http://bit.ly/a2rNMg>; also Fair Game? Assessing commercial activity on children's favourite websites and online environments, National Consumer Council and Childnet, 2007, <http://bit.ly/dffkJI>. The study shows that a quarter of third-party advertiser sites do not have privacy policies, while children and their parents do not read or understand them.

Annex 1

Definition of personal data: IP addresses and copyright enforcement

The Data Protection Act 1998 (DPA) implements the Directive 95/46/EC (the Data protection Directive) into UK law. However, it is clear that DPA does not ‘transpose’ the Directive, as stated in the consultation document.³³ In relation to IP addresses in the context of copyright enforcement, the problem is not so much that the Directive “has remained static” in the face of technological advances, as stated in the consultation document,³⁴ but the problem is that DPA does not fully transpose the Directive in relation to the definition of personal data. In relation to IP addresses we do not believe that the definition of personal data contained in the Directive is out of date, indeed we believe that this aspect of the Directive is working well and should be retained. We do believe that the definition of personal data contained in DPA should be amended so that it transposes the definition contained in the Directive. It is also our view that in relation to IP addresses the UK should take ‘into consideration the work already done by, among others, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data,’ as stated in the Telecoms Package.³⁵

Article 2(a) of the Data Protection Directive states that:

“personal data” shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity³⁶

Section 1 of the DPA states that:

‘personal data’ means data which relate to a living individual who can be identified—
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller³⁷

The DPA therefore does not implement the definition of personal data as contained in the Data Protection Directive. The Directive defines personal data in terms of ‘any information relating to an identified or identifiable natural person’, whereas the DPA defines personal data in terms of ‘data which relate to a living individual who can be identified from those data’. This means that the definition of personal data is much narrower in the DPA than in the Data Protection Directive. According to the definition contained in the DPA an IP address would only be personal data if it allows for an individual to be identified.

³³ **Call for Evidence on the data protection legislative framework**, Ministry of Justice, July 2010, pg.5.

³⁴ **Call for Evidence on the data protection legislative framework**, Ministry of Justice, July 2010, pg.5.

³⁵ **Telecoms Package**, Universal Service Directive, recitals 52.

³⁶ **Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data**, 24 October 1995, Article 2(a)

³⁷ **Data Protection Act 1998**, Section 1.

Indeed the prevailing legal advice in the UK has been that that under the DPA the IP address is only personal data if combined with other personal data, ie can be used to identify a living individual.³⁸

While the consultation document acknowledges that the Directive states that data become personal data if it “relates” to an individual³⁹ the consultation document subsequently states that data only becomes personal data if it is combined with other information that allows an individual to be identified:

‘...anonymised data... such information will not normally fall within the scope of the DPA. However in certain limited circumstances this information does qualify as personal data. The key point is whether the data controller holds other information which would enable it to be identify an individual from the anonymised data’.⁴⁰

This interpretation of personal data, while consistent with the definition of personal data as contained in the DPA, is not consistent with the definition of personal data contained in the Directive, and neither is it consistent with the guidance issued by the Article 29 Working Group. In 2006 the Article 29 Working Group underlined that in order to establish that data ‘relate’ to an individual, as defined in the Directive, either a ‘content’ element, a ‘purpose’ element or a ‘result’ element should be present. This means that data is personal data when it contains information about a specific person (content), when it is used or likely to be used to determine the treatment of a specific person (purpose), or when it is likely to have an impact on a specific person (result).⁴¹ Thus, under the Data Protection Directive, IP addresses might not always be classified as personal data and the context within which the data is processed must be examined to determine whether one of the three criteria have been met.⁴²

In our experience the inconsistency between the definition of personal data contained in the directive and DPA has caused considerable problems, particularly in the context of the Digital Economy Act 2010 and copyright enforcement in relation to online copyright infringement more generally. The Digital Economy Act implements what has been termed a ‘graduated response’ or ‘three strikes’ in relation to internet subscribers suspected of copyright infringement through peer to peer filesharing. This process relies on the collection and processing of IP addresses. According to the European Data Protection Supervisor:

³⁸ For example, Pinsent Masons LLP advises on Data protection Act and IP addresses in **IP addresses and the Data Protection Act**, Out-Law Pinsent Masons, March 2008.

³⁹ **Call for Evidence on the data protection legislative framework**, Ministry of Justice, July 2010, pg.11.

⁴⁰ **Call for Evidence on the data protection legislative framework**, Ministry of Justice, July 2010, pg.12.

⁴¹ **Opinion N° 4/2007 on the concept of personal data**, Article 29 data Protection Working Party, June 2007, pg.10.

⁴² Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri, **Review of the European Data Protection Directive**, Rand & ICO, 2009, pg.27.

'...copyright holders using automated technical means, possibly provided by third parties, would identify alleged copyright infringement by engaging in monitoring of Internet users' activities, for example, via the surveillance of forums, blogs or by posing as file sharers in peer-to-peer networks to identify file sharers who allegedly exchange copyright material. After identifying Internet users alleged to be engaged in copyright violation by collecting their Internet Protocol addresses (IP addresses), copyright holders would send the IP addresses of those users to the relevant Internet service provider(s) who would warn the subscriber to whom the IP address belongs about his potential engagement in copyright infringement. Being warned by the ISP a certain number of times would automatically result in the ISP's termination or suspension of the subscriber's Internet connection.'⁴³

The Digital Economy Act, and indeed any graduated response, has to comply with the right to privacy, as laid down in Article 8 ECHR and Article 7 of the Charter of Fundamental Rights, and stemming from the right to data protection as laid down in Article 8 of the Charter of Fundamental Rights and Article 16 of the Treaty on the Functioning of the European Union, and as elaborated in Directive 95/46/EC and Directive 2002/58/EC.⁴⁴ Therefore the question of whether the IP address is personal data in the hands of the copyright owner and/or the hands of the Internet Service Provider (ISP) has been pertinent when the Digital Economy Bill passed through parliament, and remains contentious as Ofcom is trying to implement the now passed Act through an initial obligations code.

It has been generally accepted that the IP address is personal data in the hands of the ISP under the DPA, because the ISP holds other data that would allow the identification of an individual on the basis of the IP address. However, in the UK there is widespread disagreement on whether IP addresses are personal data in the hands of the copyright owner. According to the definition of personal data in the DPA it is not, while it is personal data as defined in the Directive in the context of the three strikes policies in the Digital Economy Act. The Article 29 Working Group confirmed this in the 2005 'Working document on data protection issues related to intellectual property rights':

'The legitimate purpose followed by right holders to prevent misuse of protected information often results in the tracing of users and the monitoring of their preferences. In particular, the use of unique identifiers linked with the personal information collected leads to the processing of detailed personal data. Directive 95/46 on the protection of personal data provides for several principles that shall be complied with by any right holder in such case where personal data are being processed. Article 2(3) (a) of Directive 2004/48/EC, on the enforcement of intellectual property rights confirmed the principle that the Directive 2004/48/EC does not affect Directive 95/46 and therefore the application of the data protection principles.'⁴⁵

In 2007 the Article 29 Working Group furthermore elaborated that:

⁴³ **Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)**, 2010/C 147/01, 22 February 2010, paragraph 21 & 22.

⁴⁴ **Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)**, 2010/C 147/01, 22 February 2010, paragraph 23.

⁴⁵ **Working document on data protection issues related to intellectual property rights**, Article 29 Data Protection Working Party, January 2005, pg.4.

'Especially in those cases where the processing of IP addresses is carried out with the purpose of identifying the users of the computer (for instance, by Copyright holders in order to prosecute computer users for violation of intellectual property rights), the controller anticipates that the "means likely reasonably to be used" to identify the persons will be available eg through the courts appealed to (otherwise the collection of the information makes no sense), and therefore the information should be considered as personal data.'⁴⁶

In 2010 the Data Protection Supervisor confirmed the Article 29 Working Group's position in stating that:

'Directive 95/46/EC is applicable since the three strikes Internet disconnection policies involve the processing of IP addresses which — in any case under the relevant circumstances — should be considered as personal data... If one considers the definition of personal data provided in Article 2 of Directive 95/46/EC, 'any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number', it is only possible to conclude that IP addresses and the information about the activities linked to such addresses constitutes personal data in all cases relevant here. Indeed, an IP address serves as an identification number which allows finding out the name of the subscriber to whom such IP address has been assigned. Furthermore, the information collected about the subscriber who holds such IP address ('he/she uploaded certain material onto the Web site ZS at 3 p.m. on 1 January 2010') relates to, ie is clearly about the activities of an identifiable individual (the holder of the IP address), and thus must also be considered personal data.'⁴⁷

More recently the ICO has confirmed to Ofcom in its response to the consultation on the initial obligations code which implements the Digital Economy Act, that the IP address is personal data in the hands of the copyright owner. The ICO stated that that 'The consultation document makes it clear that in order to take legal action against those infringing their rights, copyright holders will often seek to relate the IP address allocated to the uploader to an actual person and physical UK address.' The ICO went on to state that the Information Commissioner considered the IP address personal data in the hands of the copyright owner for the purpose of the Digital Economy Act process.⁴⁸ In doing so, the ICO has followed the definition of personal data as contained in the Directive, not the DPA.

The question of whether the IP address is personal data in the hands of the copyright owners turned into a political issue as the Digital Economy Bill went through parliament. Those organisations who engage in the collection of IP addresses of subscribers suspected of copyright infringement and those who have lobbied the previous Government to pass Section 3 to 16 of the Digital Economy Act into law maintain that IP addresses are not personal data.

⁴⁶ **Opinion N° 4/2007 on the concept of personal data**, Article 29 data Protection Working Party, June 2007, pg.16-17.

⁴⁷ **Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)**, 2010/C 147/01, 22 February 2010, paragraph 25 to 27.

⁴⁸ **ICO response to OFCOM consultation on Draft Initial Obligations Code**, Information Commissioner's Office, July 2010.

For example, the British Phonographic Industry (BPI), which engages in the collection of IP addresses of subscribers suspected of copyright infringement through peer-to-peer filesharing on behalf of record companies, stated that ‘...the methods that BPI has employed to detect and notify infringers – and which we would expect to continue to deplore in the context of the preferred approach – have no implications for data protection provisions...’⁴⁹ Rightholders do not have the ability to link an IP address to an individual ISP customer.... ISPs have the ability to make the connection between an IP address and customer details...⁵⁰. When giving evidence to the Joint Committee on Human Rights, the Alliance Against IP Theft stated that: ‘The Alliance is clear that the creation and maintenance of such a list does not infringe human rights and is in compliance with all European directives. IP addresses alone are not personal data. It is information publicly available when engaging in file-sharing activity.’⁵¹ Responding to the same Committee the Periodicals Publishers Association (PAA), which like the Alliance Against IP Theft, had lobbied for the Digital Economy Act, states that ‘IP addresses alone do not constitute personal data for the purposes of the Data Protection Act 1998’.⁵²

It appears to us that the previous Government, when drafting the Digital Economy Bill and passing into law, took the view that IP addresses are not personal data in the hands of the copyright owner. Hence following the definition of personal data in DPA, not the Directive. This means that Section 3 to 16 of the Digital Economy Act are potentially in breach of the Directive and/or can not be implemented in compliance with the Directive. More generally, the difference in definition makes it very difficult to determine whether IP addresses are personal data under UK and EU law. This difference in definition also means that the UK defines the IP address as not being personal data, while other EU countries define it as personal data.⁵³

Recommendation

- The definition of personal data in DPA should be broadened, transposing the definition of personal data contained in the Data Protection Directive
- In relation to IP addresses the UK should take into consideration the work done by the Article 29 Working Party and the opinions of the European Data Protection Supervisor

⁴⁹ **BPI Limited response to BERR Consultation: ‘Legislative Options to Address Illicit Peer-to-Peer (P2P) Filesharing’**, The British Recorded Music Industry, October 2008, pg.10.

⁵⁰ **BPI Limited response to BERR Consultation: ‘Legislative Options to Address Illicit Peer-to-Peer (P2P) Filesharing’**, The British Recorded Music Industry, October 2008, pg.11

⁵¹ **Legislative Scrutiny: Digital Economy Bill – Fifth report of session 2009-10**, House of Lords & House of Commons, Joint Committee on Human Rights, January 2010, pg.41

⁵² **Legislative Scrutiny: Digital Economy Bill – Fifth report of session 2009-10**, House of Lords & House of Commons, Joint Committee on Human Rights, January 2010, pg.92

⁵³ According to a study of six EU countries which are all subject to the Data protection Directive, ie Austria, Belgium, France, Germany, Spain and Sweden, the data protection authorities and courts in five out of the six countries generally consider the IP address personal data (France has made conflicting rulings).

Study on Online Copyright Enforcement and Data protection in Selected Member States, European Commission DG Internal Market and services, November 2009



Consumer Focus response to Ministry of Justice Call for Evidence on the Current Data Protection Legislative Framework

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

www.consumerfocus.org.uk

Copyright: Consumer Focus

Published: October 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