Response to the consultation by the Department for Business Innovation and Skills regarding its proposals for implementing the revised EU Electronic Communications Framework

(See http://www.bis.gov.uk/Consultations/revised-eu-electronic-communications-framework?cat=open)

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.

This response has been prepared by Ms Judith Rauhofer and Dr Christopher Marsden.

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).

Dr Christopher T. Marsden is Senior Lecturer at the School of Law of the University of Essex, Colchester, UK and a Fellow of both Keio University[1] and GLOCOM, International University of Japan[2]. He has published on network neutrality and other issues surrounding bottleneck gatekeepers in European communications since 1997. He has also consulted for various Member State

[1] http://www.keio.ac.jp/english/research/atoz_it_its.html
[2] http://www.glocom.ac.jp/e/organization/

governments including the Department for Trade and Industry and Ofcom on Internet content regulation[3], the European Commission itself, the OSCE and Council of Europe, as well as non-EU governments and private corporations and thinktanks during that period. His most recent book is 'Net Neutrality: Towards a Co-regulatory Solution' (Bloomsbury Academic, London, 2010)[4]. His blog on network neutrality in Europe has received more than 30,000 viewings in 2010[5]. He has also responded by invitation to the FCC network neutrality consultation as noted by 'Washington Watch'[6], and to the European Commission consultation[7]. He was the only independent expert invited to address the joint European Commission-European Parliament Network Neutrality Summit on 11 November in Brussels[8].

Important contributions to preparing the response were also made by Dr Ian Brown, Oxford Internet Institute, University of Oxford and Professor Burkard Schafer, University of Edinburgh.

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.

In addition, this response is submitted by the following individuals:

Judith Rauhofer
Dr Christopher Marsden, University of Essex
Dr Ian Brown, Oxford Internet Institute, University of Oxford
Professor Burkard Schafer, University of Edinburgh
Dr Abbe Brown, SCRIPT, University of Edinburgh
Professor Abdul Paliwala, University of Warwick

[3] http://www.ofcom.org.uk/research/tv/reports/videoregulation/
[4] http://www.bloomsburyacademic.com/view/NetNeutrality_9781849662192/book-ba-9781849662192.xml?mode=book&page=1&pageSize=8&result=1&resultPage=/search&sortBy=ft:score($doc)&t1=1222|Information+and+Communications+Technology
[5] http://chrismarsden.blogspot.com/
[6] https://www.neca.org/cms400min/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=2979
[7] http://www.scribd.com/doc/34398109/OPEN-INTERNET-AND-NET-NEUTRALITY-IN-EUROPE-Marsden-respons%E2%80%A6
[8] http://www.scribd.com/doc/42298185/Three-Wise-Monkeys-of-Net-Neutrality

Q1 to Q9

No response is provided to questions Q1 to Q9.

Minimum quality of service (Network Neutrality)

Although the consultation document does not seek views in relation to the government's plans for the establishment of a minimum service requirement under Article 22(3) of the Universal Service Directive, the authors would like to raise the following issues.

In paragraph 188 of the consultation document, the government states that it proposes

"to implement the changes to Article 22(3) [Universal Service Directive] through a minor amendment to the Communications Act to give Ofcom the necessary power [to impose minimum quality of service obligations on electronic communications network and service providers]. On 24 June 2010, Ofcom published a consultation document on traffic management, where it states that its likely initial view would be to explore existing competition tools and consumer transparency options before considering using these powers. Ofcom's consultation closed on 9th September 2010[9]"

BIS has publicly stated that issues concerning the open Internet and network neutrality are too broad-ranging and politically important to be left to the regulator.

The Minister has recently affirmed, corrected and reaffirmed his commitment to an open Internet, and claimed to agree with Sir Tim Berners Lee on the centrality of network neutrality to freedom of expression and Internet innovation[10].

The Impact Assessment and overall Framework fails to consider the need for ex ante provisions beyond competition powers and consumer transparency, simply stating a binary 0 or 1 option. At p.99 of the Impact Assessment, it is stated that:

> *"[c]urrently consumers are not always provided with all the information about terms and conditions and the quality of service they can expect, or are provided with the information in a way that is not user friendly, when making decisions and they may therefore make sub-optimal decisions."*

However, the remedy to this is only considered in relation to disabled users, though logically one can extend the chosen path with that for general users:

> *"Ofcom is likely to consider using existing competition tools and consumer transparency options before considering using this power."*[11]

Option 2, to extend powers to provide a further set of potential tools for intervention, should have been considered, as the French regulator, Autorité de Régulation des

[9] http://www.bis.gov.uk/assets/biscore/business-sectors/docs/i/10-1132-implementing-revised-electronic-communications-framework-consultation at p.48.
[10] A refresher for the Minister would be: Cooper, Alissa (2010) *The Next Tim Berners-Lee: Response to Ofcom Discussion on Traffic Management and Net Neutrality*, 9 September 2010, at http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Cooper_A.pdf
[11] http://www.bis.gov.uk/assets/biscore/business-sectors/docs/i/10-1133-implementing-revised-electronic-communications-framework-impact at p.99

Communications Électroniques et des Postes (ARCEP) has done with its 'Ten Network Neutrality Principles'[12] under the proposed French intervention[13].

The fact that BIS and Ofcom do not yet agree with such a policy does not mean excluding an Option 2 from the Impact Assessment. Not to consider a further alternative is poor Impact Assessment practice.

Q10 and Q11

No response is provided to Q11 and Q12.

Breach of Personal Data and Penalties

Q12 We welcome suggestions as to how the provisions of the Directive could be better enforced.

The enforcement of data controllers' compliance with the EU data protection framework has long been blighted by the lack of an effective enforcement regime. This has been recognised by the European Commission on many occasions, most recently in the Commission's Communication "A comprehensive approach on personal data protection in the European Union"[14]. As a result, the need to provide "*a stronger institutional arrangement for the effective enforcement of data protection rules*" and to make "*remedies and sanctions more effective*" constitute two of the core challenges faced by the European Commission when reviewing the provisions of the 1995 Data Protection Directive.

Similar considerations informed the inclusion of a new Article 15a(1) in the revised ePrivacy Directive which requires member states to adopt rules on "*effective, proportionate and dissuasive*" penalties, including criminal sanctions where appropriate, for infringements of national data protection provisions, and to take all measures necessary to ensure that those penalties are implemented.

The recent expansion of the Information Commissioner's enforcement powers which were introduced through the Criminal Justice and Immigration Act 2008 and the Coroners and Justice Act 2009 are likely to go some way towards achieving that objective. In particular, the Information Commissioner's power under section 55A of the Data Protection Act 1998 to impose a fine of up to £500,000 for serious contraventions of the Act, is likely to deter many small to medium enterprises that act as data controllers and for whom such a fine would have a noticeable impact on profit. However, it is questionable whether even a fine of £500,000 may act as a sufficient deterrent for large multinational companies where the cost

[12] Autorité de régulation des communications électroniques et des postes (2010) Internet and network neutrality: proposals and recommendations, September, at http://www.arcep.fr/uploads/tx_gspublication/net-neutralite-orientations-sept2010-eng.pdf

[13] Hutty, M. (2010) *ARCEP launches principles for network neutrality*, LINX Public Affairs blog, with Google translation of ARCEP principles, at https://publicaffairs.linx.net/news/?p=1587

[14] COM(2010) 609 final, 4 November 2010; available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

of compliance with data protection requirements may exceed the potential value of a fine. Better deterrents may have to be put in place in relation to this type of data controller.

A decision by the Home Secretary to exercise her power under section 77 of the Criminal Justice and Immigration Act 2008 to issue secondary legislation to introduce custodial sentences of up to 12 months on summary conviction, and up to two years imprisonment for a conviction on indictment for those involved in the illegal trade of personal information may also contribute to improved compliance with the data protection framework. The threat of custodial sentences often serves to "concentrate the CEOs mind" and the introduction of such sentences may therefore motivate the company officers which may be liable under the relevant provisions to put in place more effective procedures for compliance with data protection requirements. However, in view of the government's plans to reduce the prison population and to limit the use of custodial sentences as much as possible, it is at least questionable whether the adoption of criminal sanctions is desirable from a public policy point of view.

It would therefore be useful to consider other types of sanctions directed, among other things, at the way in which violations of the framework are policed, the way in which they are publicized and the way in which company officers are incentivised to ensure compliance by their company.

Policing of violations

Currently, the Information Commissioner may only serve an assessment notice under section 41A(2) of the Data Protection Act 1998 on government departments or on a public authority or a person of a description specifically designated for that purposes. As part of the notice, the Information Commissioner can impose a requirement on the data controller to submit to a compulsory audit. This permits him, among other things, to enter specified premises at little or no notice. The majority of private data controllers are currently exempt from this provision which considerably affects the Information Commissioner's ability to carry out unannounced audits of those private controllers data processing activities where he suspects a breach of any of the provisions of the Act. The government should therefore consider to expand the Information Commissioner's powers under section 41A(2) of the Act to private data controllers. Such an expansion of powers should be accompanied by an increase in funding for the Information Commissioner to ensure that the Commissioner can carry out his obligations adequately and effectively.

Notification of data security breaches

Article 4(3) of the ePrivacy Directive as revised requires member states to ensure that certain data controllers must notify a personal data breach to the competent national authority (and, where appropriate to the data subjects affected by the breach) without undue delay. As set out in the Impact Assessment, the notification of data breaches is designed to provide consumers with information about which service providers have suffered breaches, so they are able to make informed decisions when deciding to whom to give personal data.

At the moment, the notification requirement is limited to providers of publicly available communications services. The effectiveness of this notification regime should be kept under

review. If it proves effective, the UK government should advocate the extension of the requirement to all other data controllers in the context of the upcoming review of the 1995 Data Protection Directive. In this context that Information Commissioner's office should be encouraged to collect the necessary statistical information that will enable the government to compare the effectiveness of the new system in accordance with a number of pre-agreed indicators.

Incentivising company officers

It is widely accepted in professions that the threat of losing the right to practice or be commercially active in that profession acts as a strong incentive to comply with the rules of conduct of that profession. In addition, in the context of company law, various provisions of the Company Directors Disqualification 1986 provide for the disqualification of a company director in cases where he is convicted of an indictable offence, where there has been a persistent breach of the company's obligation to comply with provisions of the companies legislation requiring any return, account or other document to be filed with Companies House, or where the director is seen as unfit to lead a company for other reasons.

The government should consider whether provisions should be introduced which allow for the disqualification of a company director if the company is found to have been in serious or persistent breach of any of the provisions of the Data Protection Act 1998.

Alternatively, the government could introduce an obligation on companies to include a statement that it has complied with its obligations under the Act as part of its annual return under companies legislation. Such a statement should be based on an annual internal audit of the company's data processing activities. Any breach of this obligation may result in the disqualification of the director responsible under section 3(1) of the 1986 Act.

This approach would not only strengthen enforcement, it would also encourage companies publicly to take responsibility for their data processing activities. It would also complement an approach recently suggested by the Article 29 Working Party that the revised Data Protection Directive should include a new "accountability principle"[15].

Cookies

Q 13 We welcome views on our proposed approach to implement the amendments to the Directive in relation to cookies by way of copying out the Directive text.

While the implementation of the amendments to the Directive by way of copying out the Directive text would ensure the UK's compliance with its obligations under EU law, the text in question is ambiguous and open to a variety of interpretations. Many of the industry standards to be developed in this area will depend on the guidance provided by relevant data protection authorities. The Impact Assessment seems to suggest that the UK government expects much of this guidance to be developed by the Information Commissioner's Office which, the government concludes, should be given "the flexibility to adjust to changes in

[15] Article 29 Working Party Opinion 3/2010 on the principle of accountability, 13 July 2010.

usage and technology". However, if interpretation of the relevant provisions is left to the national regulator, it is likely that national regulators in different EU member states will exercise their discretion in different ways. Given the global nature of the electronic communications market such an approach is therefore bound to create a number of practical problems for data subjects as well as online providers.

Protection of individuals' privacy

Although the ePrivacy Directive is generally viewed as forming part of the EU's data protection framework designed to protect the personal information of data subjects, the provisions of that Directive that regulate the use of cookies are unique insofar as they do not depend on the assumption that cookies themselves, or the information they collect, necessarily constitute "personal data" as defined in Article 2(a) of the 1995 Data Protection Directive[16]. This reflects the widely accepted view that:

a) while cookies and/or the information they transmit may not be able to identify a living individual on their own, they may well be able to do so in combination with other information held by the recipient of the transmitted information or a third party. This is particularly true in the case of "first party cookies" which are commonly used by online providers for session management, personalisation and recognition purposes where the information transmitted by the cookie is later combined with the personal information the internet user has provided to the provider in the course of a sale or other contact.
b) the use of anonymous cookies by the website owner or by online advertising companies ("third party cookies") for the purpose of tracking an internet user's personal browsing habits can still affect individual user's rights if the information gathered about the user allows for the potential identification of the user through ever more sophisticated systems of profiling and data mining[17].
c) online behavioural data generated by individual users and collected and mined by online providers and online advertising networks may cause economic harm to the user in question despite the fact that the user's actual identity may never be "reverse engineered". This may be the case, for example, if that behavioural data is used for the purpose of automated, dynamic pricing[18] where the price quoted to an individual

[16] 1995/46/EC

[17] See, for example, the ease with which technology experts managed to identify individual users from a pool of anonymised web search queries published by US search engine AOL in 2006, "A Face Is Exposed for AOL Searcher No. 4417749", New York Times, 9 August 2006, available at http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482. See also, P Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (August 13, 2009). University of Colorado Law Legal Studies Research Paper No. 09-12. Available at SSRN: http://ssrn.com/abstract=1450006; and Korff, Douwe, New Challenges to Data Protection (Study for the European Commission), Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments (January 15, 2010), Section 4.1, sub-section on personal data and data subject, and the issues of anonymisation, pseudonymisation, re-identifiability and profiling, in particular pp. 48 – 51. Available at SSRN: http://ssrn.com/abstract=1638949.

[18] See, for example, C R Taylor, "Private Demands and Demands For Privacy: Dynamic Pricing and the Market for Customer Information", RAND Journal of Economics, Volume 35, No.4, Winter 2004, pp. 631-650.

> user for certain goods or services is based on the provider's expectation of the amount that user is willing or able to pay. Such pricing is likely to be discriminatory if the individual user has no means to discover that the price quoted to him is different from that quoted to another internet user.

The government's statement that "*cookies are not dangerous*"[19] therefore ignores the increasingly intrusive nature of cookies that comes from recent improvements in data mining and profiling technologies and the extent to which businesses are beginning to use the data collected by cookies as the basis for new and in some cases exploitative or discriminatory revenue generation strategies. These practices need to be taken into account when a regulatory response to the use of cookies is developed

The government's assessment that "intervention is needed to ensure consumers have optimal information when acting to ensure their privacy"[20] also overlooks that Article 5(3) of the ePrivacy Directive in the form adopted in 2002 already contains an obligation on providers to provide internet users with "clear and comprehensive information" about the purposes of storing cookies and other devices on the user's equipment, and the user's right to refuse.

In practice, as the Article 29 Working Party pointed out in its recent Opinion on online behavioural advertising[21], only one of the four most popular commercial browsers rejects third party cookies by default. The majority of browsers are therefore set up to accept cookies unless the user makes a conscious decision to change those settings. The information that online providers give to internet users in order to comply with their information obligation under Article 5(3) reflects this reality. It usually consists of an acknowledgement in providers' privacy policies that

- cookies are stored on the users' equipment; and
- a more or less detailed description of how to change browser settings from the "accept cookies" default to a "reject cookies" setting[22].

The government's contention in the Impact Assessment, that following the introduction of the revised provision "*users will be able to make informed changes to the browser settings to suit their individual privacy needs and should therefore feel more confident using the internet*" therefore ignores the fact that users are already able to make those changes based on the information provided to them now. The only practical change that the government's proposal is likely to bring about is a change in the wording of the providers' privacy policies. Where, currently, providers inform users on how to exercise their right to opt out of receiving cookies, under the government's proposals, providers would most probably use their privacy policies to inform

[19] Impact Assessment, p.153.
[20] Impact Assessment, p.146
[21] WP171, 2/2010, 22 June 2010.
[22] See, for example, the Privacy Notice of the largest online book retailer Amazon ("What about cookies?"), available at http://www.amazon.co.uk/gp/help/customer/display.html?nodeId=502584#c; the Privacy Policy of the most widely used search engine, Google, available at http://www.google.co.uk/intl/en/privacypolicy.html; and the Privacy policy of social media service Twitter, available at http://twitter.com/privacy.

users of the browser's likely default setting to accept cookies and to imply the users' opt-in consent to those default settings.

The basic problem with this approach results from the fact that, as is widely recognised, internet users do not, as a rule:

- read privacy policies before using an online services. These policies are usually complex documents which users often find difficult to understand. Users also feel that as these policies are non-negotiable, they have little to gain from familiarising themselves with their content if their decision to use the service in any case has already been made.
- make changes to the browser settings even where the way in which this is to be achieved is explained to the user in plain English. This is partly because of user inertia and partly because of a well-known propensity for accepting default settings of technology for fear of upsetting the functioning of that technology. The latter is particularly understandable in the case of cookie settings as most providers' privacy policies make it abundantly clear that refusing cookies may result in a loss of functionality of the online service.

It is true, as the Impact Assessment points out, that an increase in users who block cookies may result in a loss of revenue generated by behavioural and interest based advertising which enables many online services to be provided at no financial cost to users. Any changes to the current set-up will therefore have to balance the internet users' right to privacy with the online providers' commercial objectives and the internet users' interest in being able to obtain online services at low or no cost. However, the "loss-of-revenue" argument must be seen as only one of the elements that should be taken into account when deciding on the level of regulation required in this context. In particular, it should not, of itself, be used to justify the continued and unchecked right of online services to base their revenue models on such a privacy-intrusive technology. To do so would not only mean that the government values the interests of businesses in revenue generation above the interests of consumers. It would also provide online providers with no incentive to develop other, less privacy-intrusive means of generating income from the services they offer. Consumers will often be willing, out of a lack of knowledge or because they are in an inferior bargaining position, to agree to contractual provisions which ultimately harm their interests. This problem has been recognised and much of consumer protection legislation is aimed at preventing sellers and service providers from exploiting this situation by prohibiting the inclusion of certain provisions in consumer contracts. There is no reason, why similar considerations should not play a part when looking at internet users' ability or willingness to protect their own privacy, given that many users will not be able properly to evaluate the full consequences of the decisions they are making (or, in the case of default settings, they are choosing not to make).

An interpretation of the revised Article 5(3) of the ePrivacy Directive which allows providers to continue to benefit from users' failure to read privacy policies and from their inertia when it comes to changing default browser settings is therefore unlikely to fulfil the spirit of the amendments to Article 5(3) of the ePrivacy Directive even where it pretends to comply with its letter. The revised provision was never aimed at improving the information provided to users about their use of cookies. Rather, it was intended to address issues of user inertia and

lack of bargaining power by ensuring that providers will not be able to store cookies on users' equipment in the first place unless they have obtained users' voluntary, specific and informed consent. As the Article 29 Working Party has pointed out, such consent cannot be obtained through the use of default browser settings which do not require any active input from the user to allow the provider to store cookies.

Browser-control-resistant identifiers ("Flash cookies" and similar)

In addition, the use of browser settings is unlikely to address the problems created through the use of identifiers (including user agents, add-ons, plug-ins and other cookie type data collection tools) that cannot currently be blocked by the privacy and security settings of most commercial browsers. These identifiers are often known as "flash cookies" after a plug-in of the Adobe Flash software. Experience has shown that these browser-control-resistant identifiers are more and more widely used, particularly for the purpose of tracking user behaviour[23].

It is clear that the use of browser settings to obtain user consent that is envisaged in Recital 66 of the Citizens' Rights Directive is unworkable in relation to browser-control-resistant identifiers. Although users of such identifiers might argue that an internet user's consent to accept cookies – as expressed through his browser settings – should also permit the storage of those identifiers, from the user's perspective, this expectation is unreasonable. A device that will not be affected by a clear user choice to block it, should not be able to benefit from a general user choice to "accept cookies" which will often be made without the user even being aware of the existence of such browser-control-resistant agents.

As current technology is incapable of dealing with these identifiers, regulatory or self-regulatory intervention may be necessary to achieve the policy objective set out in Article 5(3) of the revised ePrivacy Directive. Although it is likely that personal data collected by those agents will always be collected in contravention of the Data Protection Act 1998 and the ePrivacy Regulations (unless those who use those agents obtain consent by other means), detection of the use of those agents is difficult and time-consuming. In practice, it will therefore be almost impossible for the Information Commissioner's Office to enforce the law against everyone who uses browser-control-resistant identifiers to collect personal data in contravention of the user's browser settings.

"Zombie cookies"

In addition, many browser-control-resistant identifiers have the ability to reinstate ("re-spawn") traditional cookies connected to them even after the user deleted those traditional

[23] "You deleted your cookies? Think again!", Epicentre - Wired.com, 10 August 2009, available at http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/, last visited, 26 November 2010. See also K McKinley, "Cleaning Up After Cookies, Version 1.0", 31 December 2008, available at https://www.isecpartners.com/storage/white-papers/iSEC_Cleaning_Up_After_Cookies.pdf. In some cases it is possible to block browser-control-resistant identifiers through the installation of browser add-ons, although this usually requires a certain level of technical expertise that is unlikely to be present in the majority of internet users. In some cases, those identifiers may also be disabled or deleted by changing the flash cookie's settings or visiting the website of its manufacturer. However, this is a time-consuming approach that, too, that should not be imposed on internet users.

cookies. Because of this ability "to bring back the dead" they are often known as "zombie cookies". This is a deceptive practice, which clearly contravenes user choice and which circumvents existing browser technology. The government's proposals set out in the consultation document and the impact assessment would have no effect on the continued use of this technology.

Legal certainty and European harmonisation

Because of the global nature of the internet, online providers and online advertising providers are likely to use cookies to gather data about internet users from countries other than the one(s) in which they are situated and with whose laws they are obliged to comply. Although UK providers may seek to rely on the country-of-origin principle set out in Art. 4(1) and (2) of the E-commerce Directive (2000/31/EC), the processing of personal data collected online from consumers may be seen as falling within the consumer protection derogation contained in Article 4(4) of that Directive.

In addition, the Article 29 Working Party has made it clear in its "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites"[24] "*that the national law of the [m]ember [s]tate where [a] user's personal computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk*"[25].

In practice, this means that a UK online provider that uses cookies to collect personal data from users based in another EU member state may be subject to enforcement action being taken against it by the relevant authorities in that member state if the providers' means of collecting that data does not comply with that member state's data protection regime as interpreted by that state's national regulator.

Consequently, providers situated in the UK will not be able to rely on, or benefit from, the relaxed approach outlined in the government's preferred option (Option 2), if they wish to offer goods and service to customers in other EU member states where a more restrictive interpretation of the Directive's provisions may apply.

As a result, providers may prefer a slightly more restrictive interpretation of the ways in which they can achieve compliance with the requirements of Article 5(3) as amended provided that this interpretation represents a harmonised approach across all EU member states which would allow providers to trade freely across EU borders without having to invest time, money and expertise in achieving compliance with the requirements of different legal systems.

Conclusions

The government should therefore refrain from trying to address the problems raised by the use of cookies in general, and by the new provisions inserted into the ePrivacy Directive in particular, in isolation. Instead, the UK government should actively engage in a discussion

[24] WP56, 30 May 2002.
[25] Ibid., p.11.

with representatives from other EU member states (for example through the Article 29 Working Party) and the European Commission to develop EU-wide, harmonised guidance on the steps to be taken by online providers, online advertising providers and browser providers to comply with the new provisions. In these discussions, the government should promote a pragmatic, but balanced approach which takes into account internet users' fundamental right to privacy and convenience of use of online services as well as the providers' commercial interests and their need for harmonisation and legal certainty. In particular, the UK should aim to ensure that:

1) the new provisions are interpreted in a way which ensures that users' decision to change browser settings to "accept cookies" will be accepted as their express consent to providers' processing of the information transmitted by those cookies across all EU member states;

2) providers, including providers of third party cookies, will be required to provide clear, comprehensive and fully visible information about their processing activities;

3) providers will not be permitted solely to rely on default browser settings to "accept cookies". If providers wish to rely on an expression of user consent through browser settings, browser owners must agree to change their settings to a more privacy-friendly default setting. This need not mean that all browsers should reject all cookies by default unless the internet user changes those settings. As the Impact Assessment accompanying the consultation paper clearly recognises, many users value the ease and convenience that is facilitated through providers' use of cookies for session management, personalisation and recognition. However, the use of cookies for tracking users' behaviour is much more controversial, and while some users might welcome the "targeted advertising" that results from the collection of behavioural data by such cookies, the majority of users are likely to object to the use of their data for this purpose. In any case, as shown above, the use of tracking cookies raises much more substantial consumer protection issues than are currently addressed in the Impact Assessment so that even if a majority of users were willing to accept tracking cookies, this should not be the only consideration taken into account when making this policy decision. One way of addressing the substantive differences between session management/personalisation cookies and tracking cookies might be to require browser owners to provide for more sophisticated browser settings which allow users to distinguish between the different purposes for which cookies may be used. From a user's point of view it might then be acceptable if cookies used for the purpose of session management, personalisation and recognition are accepted by default (subject to the user's ability to change those default settings), whereas tracking cookies should be rejected unless the user specifically requires them to be used.

4) it should be made clear that the procedure for obtaining consent set out in Recital 66 does not apply to browser-control-resistant identifiers. Ideally, manufacturers of those agents should be encouraged to re-configure them in a way that allows internet users to control their use via browser settings. Where this is not possible, it should be made clear that the use of browser-control-resistant identifiers to collect personal data and to track internet user behaviour is subject to obtaining the user's express consent (for example, via a tick box or a pop-up window).

5) re-spawning traditional cookies after they have been deleted by users should be prohibited by law.
6) the national regulator should be given appropriate resources to enforce the existing legal provisions against providers who are in breach of the ban on the use of "re-spawning" devices and who use browser-control-resistant identifiers with obtaining the user's express consent. Individual data subjects as well as consumer protection organisations should be provided with enforceable remedies against those providers.
7) while browser owners might be expected to bear the cost of the necessary changes to their default settings, the onus to provide users with sufficient information about the effect of those settings and the way in which they may be changed should be on the online provider that wants to use cookies. The government's assumption expressed in the impact assessment, that the cost of providing information about how to change browser settings on cookies should be borne by browser owners is curious given that browser owners do not benefit from the storage of cookies in any way and will not be considered data controllers in respect of the information gathered by cookies. It is the online providers who will be responsible for the storing of the cookie on the user's equipment, for the collection of the user's data and for the further processing of that data for the provider's commercial purposes. As data controllers, it is therefore reasonable to expect online providers to provide users with the necessary information and to bear the cost of providing that information.

Impact Assessments and Equality Impact Assessment

Q14 The Government invites views and comments from respondents on the impact assessments and equality impact assessment which have been produced to support implementation of the revised electronic communications Framework.

New information provision requirements (IA No: BIS0109)

In Impact Assessment Number BIS0109, the government proposes to insert a new requirement on providers of providers of publicly available electronic communications services "*to have a procedure in place to be able to respond to request for information from the police or security services*" in the Regulations intended to implement the amendments to the ePrivacy Directive in the UK. The decision to introduce such an obligation is surprising given that:

- the government fails to mention this proposal in the Consultation Paper to which the Impact Assessment relates. This runs the risk that it may be overlooked by many respondents to the consultation and that the proposal will not receive the public scrutiny it deserves;
- it is not mandated in any way by the provisions of the Citizen's Rights Directive that the current legislative proposal is designed to transpose but is included in addition to those provisions. This approach is in stark contrast to the government's own promise in the context of this consultation paper, that it "*will*

> *be implementing the amendments associated with the revised Framework … in a proportionate manner to achieve the desired outcomes without gold-plating*"[26].

The introduction of such an obligation in the context of this consultation is undesirable for a number of reasons:

1. Provisions regulating access by public authorities to information held by communication service providers (usually communications/traffic data and intercepted electronic communications) are already included in the Acquisition and Disclosure of Communications Data Code of Practice and the Interception of Communications Code of Practice brought into force under section 71 of the Regulation of Investigatory Powers Act 2001 ("RIPA"). They cover in some detail the steps which service providers must take in order to assist public authorities in relation to information disclosure requests. It therefore questionable whether additional provisions governing the modalities of data transfers from communications services providers to public authorities are necessary in practice.
2. While it would be useful to provide the Information Commissioner's Office with powers of oversight over the extent to which public authorities make use of their rights under RIPA to request individuals' personal information from communications service providers, it has generally been accepted that in the UK this power is exercised by the Interception of Communications Commissioner who addresses this issue as part of his annual report. Although it has been shown in a different context, that there may be gaps between the oversight powers of the Interception of Information Commissioner and the Information Commissioner which need to be closed[27] it seems curious that the Information Commissioner's Office should be required to use its already insufficient resources to police the establishment of procedural rules designed to facilitate the provision of information over which the Information Commissioner lacks jurisdiction. The government should not use the Information Commissioner's Office as an "enforcement agent" for the police and security service whose duties include the obligation to ensure that those services can access the information they request in the most efficient way.
3. The fact that communications service providers will be expected to bear the costs of establishing the relevant procedures contradict the government's frequently published intentions that it intends to minimise the organisational and economical cost of regulatory compliance on business.

If the government feels that the provisions of the existing codes of practice need to be amended or supplemented in any way, it would be prudent that proposals for such amendments should be the subject of a separate consultation. This is true, in particular, given the controversy that arose when the above codes of practice were first published and the impact which the imposition of additional requirements is likely to have, both on the commercial (and hence competitive) position of UK communications service providers and

[26] Impact Assessment, p. 5.
[27] Proposals to close these gaps are currently the subject of another consultation "Regulation of Investigatory Powers Act 2000: Proposed Amendments Affecting Lawful Interception" issued by the Home Office on 10 November 2010, available at http://www.homeoffice.gov.uk/publications/consultations/ripa-effect-lawful-intercep/ripa-amend-effect-lawful-incep?view=Binary.

the rights of individuals to the protection of their personal data. The government should provide a more substantive explanation of why it feels that the existing provisions are not sufficient and why it feels that it must impose more structured requirements on providers. Oversight of the way in which providers comply with their information requirements must be specifically addressed. The government should also make it clear whether the proposed new information requirement is designed to allow public authorities the right to access personal information which may not currently be covered by any of the existing regulations.

Regard to consumer needs

The proposals made are certainly more attentive to the government's Code of Practice on Consultation[28] and the advice of the Better Regulation Executive than the extraordinary method chosen to consult 'stakeholders' on RIPA amendments to assuage the European Commission after the PHORM debacle.

The authors strongly suggest that, for future consultations, the government should improve its consultation practice, taking into account consumer needs by degrouping its list of consultees. 'Interest groups' currently only accounts for business lobbies and a few government funded consumer groups.

The government should add such institutions as the Foundation for Information Policy Research, Privacy International, Creative Commons UK and the Open Rights Group – clearly these are expert and consumer-interest groups whose input would make the government's consultations more effective, not least because they would provide a 'critical friend' role that the Communications Consumer Panel claims but does not always achieve.

A category called 'Civil Society and Consumer' would help the government to identify such general groups, in addition to other 'Third Sector' groups which comprise those representing particular affected constituencies. This would better conform to Impact Assessment state-of-the-art.

End of Submission

[28] http://www.bis.gov.uk/files/file47158.pdf