Department for Business Innovation & Skills

Implementing the Revised EU Electronic Communications Framework: Overall approach and consultation on specific issues

Response of the Computer and Communications Industry Association

Introduction

The Computer & Communications Industry Association (CCIA) is a not for profit trade association dedicated to open markets, open systems and open networks. CCIA members are active in the computer, IT and telecoms industries and range in size from small entrepreneurial firms to some of the largest in the industry. CCIA members employ around one million people and generate annual revenues of over £130 bn. Many of CCIA's members are active in the UK[1]. A complete list of CCIA's current members is available online at www.ccianet.org/members. CCIA is committed to vigorous competition in every market and submarket of our industry. CCIA supports open interfaces and non-discriminatory access to networks. We believe that no one company should dominate any network and that the barriers to entry should be reduced to foster free and open markets. CCIA recognizes the measures the UK Government has taken in this regard and believes that the UK has a role to play in Europe leading other countries through similar liberalization.

In responding to the consultation CCIA canvassed the views of its members and submits this reply on behalf of the CCIA rather than any of its individual members. We have not replied to all of the questions you asked but rather concentrated on those where we know CCIA can add the benefit of its collective experience.

General Comments

We thought it might be helpful if we set out a few general comments before turning to the specific questions asked in the consultation:

The Importance of Technology

The CCIA agrees with the general tone of UK Government policy stressing the fundamental need for the Government to support technology businesses and e-commerce. We welcome many of the commitments the Government has made this month in its Blueprint for Technology. We agree that care must be taken to simplify the regulatory position and make the UK business friendly. Unnecessary regulation also creates barriers to entry. Increased regulation in this area does not in the main protect consumers. It simply denies them access to the ability to use technology in their daily lives with the benefit of choice, accessibility and price that that brings.

Technology Neutrality

[1] If we had any numbers on that that would be ideal.

CCIA believes that to understand fully how to regulate the online space it is important that distinctions are made between cookies and similar technologies. We also feel that particular distinctions should be made between browser-side technologies (such as cookies), which an internet user can control, and server-side technologies (such as Deep Packet Inspection (DPI)) over which the individual user has little or no control. While DPI can be a useful technology for network operators to ensure the integrity or security of their networks, CCIA is concerned about the use of DPI for end user tracking at the network level for the purpose of targeted advertising or other illegitimate purposes. By use of DPI, Internet Access Providers (IAPs) are in a position to collect huge amounts of data on customer's activities, both commercial and non-commercial, as they travel over the provider's infrastructure from emails to chat to financial information. The lack of major competition among broadband access providers in the UK poses challenges for consumers and businesses alike. Whilst customers have an element of freedom of choice should they object to browser-side privacy – they can simply download, for free, a new browser - it is harder to switch IAP if server-side technology is the worry. In addition experience suggests that there is also less visibility of server-side activity. Many users know how to disable cookies by using the toolbar on their browser. They are much less able to control server-side technology even if they do know it is happening.

The Benefits of Online Targeted Advertising

The CCIA believes that on balance targeted advertising is a necessary part of the internet. We believe the benefits of targeted advertising include:

- Low-cost Services – Online advertising has greatly benefited consumers by underwriting the rich variety of online content choices and services available, enabling applications providers to offer their services at little or no cost to the consumer.
- More Relevant Ads – Online targeted advertising allows businesses to create a more convenient and personalized experience for consumers. Consumers are served relevant ads that are tailored to their online interests.
- Low Barriers to Entry – Small businesses and entrepreneurs now have more opportunity to engage with consumers compared with more traditional methods, creating robust competition and innovation online.
- Expansion of Free Speech Applications – Advertising revenue has helped support new online applications, ventures and publications, such as blogs and social networking sites. Online publishers are better able to generate revenue from advertising, allowing them to offer free or low-cost services and better serve their customers. As a result online advertising has helped to level the playing field for small businesses and entrepreneurs, which leads to more opportunities for free expression.
- Competition Supports Consumer Choice – Because online advertising has both helped to preserve the low barriers to entry and underwritten the cost of services, consumers enjoy a competitive online environment that offers robust choices in products and services. Not only will this robust competitive environment encourage companies to innovate in the types of services and products they offer, but it will also drive them to compete over privacy practices in order to please customers.

Specific Questions in the Consultation

3. **Do respondents believe that a detailed inventory of infrastructure would be desirable in order to facilitate infrastructure sharing and if granted access, would this inform investment decisions?**

   The CCIA has worries about the proposal to have a detailed inventory of infrastructure on two levels.

   Firstly, we are worried from a security prospective. We appreciate that cosmetically a detailed inventory makes sense but at times of tighter need for national security, given the threats which have been made to the UK and its critical national infrastructure, we think it unwise to compile this log given the potential that it may be compromised. We appreciate that appropriate steps can be taken to secure this type of information however, even the most secure databases can be subject to compromise – for example, the alleged Romanian based hack that the Royal Navy suffered this month.

   Secondly, we think that the additional administrative burden that the compilation of a detailed inventory could bring could serve as a barrier to market entry. Whilst the expense of creating a detailed inventory of infrastructure might be something that the larger players in the industry can bear, this is not likely to be the case for new market entrants and smaller businesses.

4. **Do respondents believe that requiring undertakings to provide information to enable Ofcom to compile a detailed inventory of the nature, location and capacity of all UK infrastructure is proportionate, or should the powers only be exercised where there is an imminent prospect of infrastructure sharing in that particular location?**

   Please see our answers to question 3 above.

5. **Do respondents believe it is appropriate for Ofcom to be the sole authority that is able to require this additional information from undertakers in relation to infrastructure? If not, which authorities should be able to require this additional information?**

   If information like this is to be gathered (and for the reasons given in question 3 we think it should not) we do agree that the fewer people who are involved the better, as that should make the process more secure.

7. **The Government welcomes any general observations on its proposed approach as set out in this section of this document and in particular the proposals in paragraph 111 to implementing Articles 13a and 13b of the Framework directive which address "Security and Integrity of Networks and Services". We would also welcome your views on what needs to be covered in any Ofcom guidance.**

   CCIA clearly supports enhanced security measures. We would caution against measures being too prescriptive however firstly as this can create a barrier to entry if there is a lengthy and detailed security accreditation or audit process and secondly as there is evidence that over reporting of less consequential breaches in the US has led to notification fatigue.

We appreciate that the risk of breach notification fatigue is lessened by the obligation being to report to Ofcom rather than end users but Ofcom can itself insist on end users also being notified. They should be encouraged to do this only in the most serious cases where loss to the individuals concerned is likely, for example where their personal details have been compromised and they are at risk of identity theft. It would be sensible to make sure (as you currently propose) that Ofcom and the ICO work together on this to ensure a consistent and joined-up approach should a report to end users be necessary.

As far as the audit process is concerned then we believe weight should be given to existing standards such as to an ISO 9000 series standards which were developed from the UK's BS5750 standard. Ofcom should not favour its own processes or its own auditors as again to do so could create barriers to entry and increase the expense for existing operators. CCIA would draw parallels with the PCI auditing measures where significant costs have been added for those handling credit card transactions whilst not preventing major security breaches.

12. **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.**

The CCIA responded earlier this year to the Information Commissioner's consultation on the Personal Information Online Code of Practice and we welcome the balance that the ICO achieved in the Code of Practice.

Technically it is generally not possible to take meaningful consent before the delivery of a cookie. For example, a cookie might be used the instant a user visits a website to determine how the user is likely to want to view the site, such as determining whether the user is looking at the site on a mobile device or whether the site should be configured for use on a particular browser. Cookies can also be essential in assisting with access issues – for example a cookie can be used to identify those accessing the internet with the help of a reader to assist the blind or partially sighted so that the site can be served in the best way for them. As more browsers and more ways of accessing the internet become available this is all the more necessary. It is challenging technically to do this without the use of a cookie.

As well as the ICO's Code and data protection legislation there is already significant consumer legislation in place which offers substantial protection for consumers. For example the Consumer Protection from Unfair Trading Regulations 2008 give the duty to act when a consumer is deceived about the presence of cookies even when the information they have been given is correct. These powers are similar to those used by the Federal Trade Commission in the US so successfully in the Sears case . The penalties include fines or a prison term of up to 2 years. In most of the UK trading standards offices and the Office of Fair Trading are under a duty to enforce the Regulations. They have special powers to seize documents and conduct dawn raids where they believe an offence has been committed. It is clear then that the powers which already exist are strong enough to police, with criminal sanction, companies who use cookies in a misleading way.

In our view there are discrepancies between the text of Article 5.3 and Recital 66 of the 2009 Directive. Article 5.3 says that the user should have "given his/her consent".

Recital 66 refers both to the "right to refuse" and the "user's consent". We do not think that this is helpful particularly given the fact that other countries in the EU have been less able to recognize the value cookies have in today's information society. Article 5.3 should not just be copied into UK law as that would be to incorporate vagueness and uncertainty into the law. It would also likely lead to judicial challenge as has been the case recently with other technology legislation. Additionally this would be in direct conflict with the Government's policy in the Blueprint for Technology of being *"committed to bringing new discipline to the implementation of EU rules, so that British businesses are not disadvantaged …."*

The Directive rightly says that consent should not be required when the cookie is strictly necessary to deliver a service which has been explicitly requested by the user. We think that it would be helpful if the UK were to clarify the implementation of Article 5.3 and give order to the qualification that consent is not required when a service is explicitly requested by the user. This could be done by adopting a simple presumption that when:

1. cookies are properly disclosed in a website's privacy policy giving clear and comprehensive information about the purpose of the storage of, or access to, the information which is stored on the cookie, and
2. a user has taken affirmative action to get to the site, for example by clicking a link to the site or typing the relevant url into his browser, and
3. a user has his privacy settings set to accept cookies

It would be presumed that consent had been given.

This simple 3 step test would help set out a manageable standard for providers to achieve and would increase transparency. It would be in keeping with the Government's stated aim in the Blueprint for Technology to have the *"emphasis on regulation as a last, not a first resort*" It would allow for clear prosecutions against those who abused the rules under consumer protection legislation. It would also be of more benefit to consumers by providing them with a simple way of finding out what each site does. This could be coupled with an education program telling consumers about the simple test and how to find out more about and disable cookies. In our view the UK should take the lead and imply consent in the manner we have outlined above. The implied consent would also as a result properly reflect the 'right to refuse' concept of Recital 66.

The CCIA believes that the study last year by the Center for Democracy and Technology that explored competition amongst the privacy settings and consumer controls offered by the companies responsible for the five leading web browsers is relevant to browser-side technologies. It has been possible to disable cookies for example in Internet Explorer for some time. Most users, however, even if they disable cookies for a short period, automatically ask their browser to accept them again. The internet experience without cookies can be less rewarding, for example a user may find that the website does not display well or she may become irritated by having to input her country of origin each time she logs on. CCIA believes that as the choice of browsers has increased in Europe, partly due to the agreement which the European Commission made with Microsoft, there should not be a legal requirement to offer turned off services, although there should be a legal requirement to tell individuals when information is being stored on their computer and to tell them that their browser can be configured to prevent this happening. Due credit should be given to opening up of the browser market and the regulatory environment should reflect these changes. As an illustration of the recent changes to browser availability in March Reuters reported that one browser, Opera, had tripled the number of downloads from the UK in just one week following the Microsoft change of policy. In October it was reported that Internet Explorer's share of the European browser market has now fallen to less than 40% . Given the general comments we have already made about the economic business model for many e-commerce services, we do not believe that websites should be obliged to provide a turned off service.

We do believe that a distinction should be made for server-side technologies. Here the consumer has less choice and less mobility. We believe that server-side technology should require opt-in consent in addition to a legal requirement to tell the individual where their information is being stored and the data processing that is being performed on their personal data. In addition customers should be given the opportunity to refuse data processing and be provided with an equivalent turned off service.

It is unrealistic to expect an innovative online business to take detailed measures to track user's consent. The most successful businesses in this space operate globally. The economic model for many of these sites dictates that they operate with limited internal resources but a significant number of users. For example in March Facebook had a little over 1,000 employees and 400 million users and LinkedIn had around 60 million users and just 480 employees.

CCIA would additionally like the UK to make it clear that the use of browser side technologies does not constitute the use of equipment in the UK. Some EU member states have suggested that the use of cookies does constitute a presence in the jurisdiction for the purposes of data protection law. If that were to be the case the consequences could be potentially disastrous. Many e-commerce operations rely on being lean to provide free services to end users. UK consumers have gained considerable benefit from this, for example free email accounts are now commonplace, when just 12 years ago a consumer would expect to pay a significant monthly subscription to send emails. Already there is talk in the industry about Internet 'black holes', talk which has been heightened by the recent difficulties experienced by Google in Italy. The categorization of browser side cookies as equipment in the jurisdiction is likely to lead to those black holes becoming a reality in Europe.

Conclusion

The CCIA believes that consumers are best served in the UK by responsible and proportionate light-touch regulation. This will enable them to have access to the widest range of goods online at the most competitive prices. It will enable them to access many sites and services for free. For businesses it results in freedom to enter the market without artificial and arbitrary barriers. It also encourages innovation and allows those innovators to sell their services both at home and abroad. This in turn supports the UK's technology strategy. In November the Prime Minister said "*We are firmly on the side of the high-growth, highly innovative companies of the future. Don't doubt our ambition*." This is a chance to demonstrate that commitment. The UK needs to act decisively to encourage e-commerce as without that encouragement ground will be lost and the economic prosperity and future of the UK will be prejudiced.

Erika Mann
Executive Vice President
Computer & Communications Industry Association
11 Rond Point Schuman - Suite 417
B-1040 Brussels
Belgium
emann@ccianet.org
15th November 2010