Information Commissioner's Office

Personal Information Online Code of Practice

Comments of the Computer and Communications Industry Association

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. A complete list of CCIA's current members is available online at www.ccianet.org/members. This response is filed on behalf of the CCIA rather than on behalf of any of the CCIA's members individually.

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:

Technology Neutrality

Whilst the CCIA is broadly supportive of the ICO's position on technology neutrality, we feel that there are important distinctions to be made between cookies and similar technologies particularly when used in online advertising. We also feel that particular distinctions should be made between browser side technologies (such as cookies), which a web 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, the CCIA is concerned about the use of DPI for end user tracking at the network level for the purpose of targeted advertising or 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

Question 1 - Does this section explain clearly what information this code applies to?

It is right to point out in the Code that "the use of cookies or the analysis of Internet Protocol (IP) addresses can allow the accumulation of information". We do think however that there should be emphasis on 'can'. We do not believe that cookies or IP addresses should be automatically put in the same category as personal data. We would like the Code to make it clear that non-personally identifiable data like cookies or IP addresses have the potential only to be personal data when they are associated or can reasonably be associated with a data subject. Whilst we do believe that cookies and IP address information deserve some level of protection, they should not automatically be classed as personal data as users can apply user choice and control.

Question 2 - Have we properly understood the technical issues of collecting personal data online?

Yes, subject to our general comments above about technology neutrality.

Question 3 - Are there any other specific issues relating to online security that you think it would be helpful for us to cover in the code?

The ICO may consider adding in a specific bullet point to cover technology suppliers, especially providers of hosting services and the like. This could cross-reference to the checklists and more detailed section on suppliers in pages 14 and 15. For example, not all third party hosting providers are equal and one of the consequences of the rise of cloud

computing could be that new entrants offer services online with little track record, few resources and possibly with questionable motives. Data controllers should be encouraged to perform due diligence on the third parties they buy from. This will also involve establishing clear roles and responsibilities with those third parties and entering into formal contracts with them. Data controllers should especially be reminded that organisations who seem to have purely an Internet presence should be treated with caution.

The CCIA is especially concerned about fraudsters posing as legitimate service providers to gather customer information. There are suggestions that that information has subsequently been used for phishing and identity theft. These scams are likely to increase and it would be prudent for the ICO to make reference to this to help protect customer data.

In the bullet where you say, "only allow your staff to access the information they need to do their job" you could usefully add "and make sure that any third party who handles the information does the same."

Question 5 - Have we properly reflected the issues relating to the marketing of goods and services online?

Please see our comments above on Technology Neutrality. In practice the CCIA has difficulty with the practicality of 'turning it off'. For many businesses with a significant international footprint this might not be possible, even if it were desirable from the user's point of view.

Turning off IP addresses

In many cases the ability to turn off IP addresses is unlikely to be desirable from a public policy perspective. IP addresses are often needed for compliance purposes – for example to detect DOS and phishing attacks, for national security and to prevent harm. A graphic example this week would be the allegations made by German police that an early disclosure of an IP address could have saved the life of an 18 year old (http://www.telegraph.co.uk/news/worldnews/europe/germany/7360349/German-police-blame-internet-host-for-suicide-death.html).

Turning off cookies

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. The CCIA believes that as choice of browsers has increased in Europe, partly due to the agreement which Microsoft has reached with the European Commission, 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. As an illustration of the recent changes to browser availability on 3rd 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. Given the general comments we have already made about the economic business model for many e-commerce services, we do not believe that data controllers 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.

Question 6 - Should we try to develop specific recommendations relating to default settings? If so, do you have any suggestions on how these defaults could be set? What areas of activity do you think we should cover?

We do not believe that it is necessary to develop specific recommendations relating to default settings as we believe that the situation is much different from say two years ago when there was little effective browser choice. We believe that it should be left to individuals to choose their browser and the privacy settings on that browser.

As we have said we believe the situation is different for server side technologies when the default setting should be that personal data is not processed without the individual's consent.

Question 7 - Are there any other international issues you would like to see covered?

CCIA would like clarification on whether the use of browser side technologies constitutes the use of equipment in the UK. For the reasons we have already outlined in this paper, we believe that it should not and should individual member states in the EU decide that for example the use of cookies does constitute a presence in the jurisdiction for the purposes of data protection law, 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 common place, 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. Should the ICO take the view that merely placing cookies on a user's computer is enough for UK data protection legislation to bite, there is a risk that some services could be withdrawn from the UK market.

Question 11 - Do you think the advice given in this code meets the realities of current business practice?

We believe specifically that the Code could take into account the present situation with regard to browser choice. We have already made comments on this.

We also believe that the section headed 'Collective responsibility' on page 17 needs to be changed to reflect modern business practices. The economic model for many websites dictates that they operate with limited internal resources but significant subscribers. For example Facebook has a little over 1,000 employees and 400 million active users. LinkedIn has around 60 million users and just 480 employees. Commonly social networking sites feature a variety of different applications from different providers. We believe that most

users of social networking sites understand that the site does not provide all of the content and all of the applications itself. The social networking site should not be given the obligation to act as a 'virtual concierge' to help users resolve their issues with third parties.

Question 13 - Do you have any comments on how the code should be presented? For example, by a set of web pages with a related discussion forum?

CCIA would encourage the ICO to look at different methods of bringing the Code of Practice to public attention. The idea of a set of web pages with a related discussion forum is a good one. It is our experience that companies are moving beyond static information and turning to more dynamic solutions with their own privacy policies. The ICO could use this technology and encourage others to do so in the Code. For example Facebook has used its own social network platform to announce major policy changes and has adjusted its policies based on user reactions. Google features video presentations showing the privacy policies for Google and YouTube (http://www.google.com/privacy.html). Yahoo! has a privacy centre which includes regularly updated content and its own privacy blog (http://info.yahoo.com/privacy/us/yahoo/details.html).

Question 15 - Are there any additional features you would like, for example interactive multi-media examples of good and bad practice when processing personal information online?

We do think that multimedia examples of good and bad practice would be beneficial.

Question 17 - Are there any further comments you wish to make?

We believe that the ICO should consider establishing an advisory board which could meet to review the Code of Practice perhaps twice a year and also to help inform the ICO with emerging technologies such as mobile computing, cloud computing and DPI technologies. The advisory board should be comprised of representatives of those with different interests including those involved in consumer protection, privacy advocates, the advertising industry, information service providers who carry advertising, bloggers, IAPs and telecoms providers. The advisory board could also comment on self-regulatory regimes and best practices. If invited the CCIA would be happy to consider being represented on this advisory board.

Erika Mann, Executive VP

Danielle Yates, Director of External Affairs

Computer & Communications Industry Association

Europe Office:

ATEAC Business Center

Rond Point Schuman 11

B-1040 Brussels Belgium

U.S. Office:

900 17th Street NW

Suite 1100

Washington, DC 20006

dyates@ccianet.org

www.ccianet.org

5th March 2010