Mark Chipperfield
works at BBC Television Licensing
as Head of Data Management.

Legal and Regulatory Update

Cookies — Transparency and pragmatism

Mark Chipperfield

Journal of Direct, Data and Digital Marketing Practice (2012) **13**, 253–256.
doi:10.1057/dddmp.2011.37

Topic: Cookies Consent Implementations

Who: UK websites

Where: UK

When: End May 2012

Law stated as at: Regulations as defined May 2011

Editors Note: In our last issue (Vol 13 No 2) we published a short article by the Information Commissioner, Christopher Graham, outlining the position of his office on the recent Amendment to the Privacy and Electronic Communications Regulations of May 2011, regarding the use of cookies. Below we publish an article by a leading member of the IDM's Data Council who, both in that capacity and in his day-time job has to struggle with the implications of these Regulations as interpreted by the Commissioner. It seems to us that this raises some interesting questions, and we confidently predict that this one will run, and run. Robin Fairlie.

Introduction

The countdown has started; 2012 is coming and everyone is under Starters Orders. The training's not been easy, and the course is not entirely clear ... oh and the instructions are not that easy to follow ... although the prize is, well, er ... uncertain. By May 2012, organizations must understand the way they use cookies, and where they are not 'strictly necessary' (ie where they are not essential for a service explicitly requested by the customer) organizations must gain consent to store them on the computers of customers or prospective customers. A key part of the 'prize' is undoubtedly transparency and protecting individuals' privacy. However, a concern is that this may not be achieved and that the actual result may be confusion for customers.

As organizations operating websites should be aware, an Amendment to the Privacy and Electronic Communications Regulations in May 2011 required website owners to gain consent to store their cookies on users' computers. The first step is to audit where you are, what cookies you have and what they do — from the necessary through to levels of intrusiveness. By next May you're supposed to be clearly explaining

your use of cookies to users, and be collecting consent (unless the cookies are strictly necessary). The ICO is likely to take a very dim view of organizations that have not carried out such an audit and have either not put consent collection in place or got a very robust plan to implement it, as necessary, soon after.

It's all about transparency

Central to the objectives is transparency, but organizations will also want to ensure that customers are not negatively impacted in their customer experience. How do you Inform, clearly, not disrupt and collect a considered view? The ICO's own website has made a valiant attempt on its website, one of the early implementers of 'something'.¹ But to the layman, what does this all mean? What is this about storing information on my computer? Having clicked this one, I notice I don't then get an opportunity to change my mind, not that I could find anyway — is this transparent and offering choice?

While businesses have long been required to be clear about how cookies work on their sites (ie since the original PECS regulations came into effect in 2003, and the DP Act also requires information to be processed in accordance with the rights of data subjects, not excessive, obtained for specified purposes), this is another level of clear and transparent. It requires explicit consent for all but the most essential cookies.

The ICO says it has left solutions open to creative ideas and does not wish to prescribe. It is very possible that due to this invitation to freedom of design, that confusion could be the result of what was supposed to be a mission of transparency.

The path to implementation

Theoretically, the more advanced web-based businesses will have the most experience and technical know-how to develop something that communicates to both their customers and prospective customers what they do with cookies and why. And to collect and store the required consents in a way that, if anything, 'enhances' the customer experience — provides reassurance, demonstrates how it works and so on — *although one can imagine many a savvy user being flummoxed by references to 'intrusiveness' in relation to their favourite website experiences*. Such websites are the most likely to be carrying out 'intrusive' behavioural advertising, using lots of third-party cookies etc, and it's right that this exchange of data is acknowledged, made transparent to consumers, and that an informed choice opportunity is made easily accessible. To date, though, I personally haven't seen one example of this on a live website yet ...

Also in theory, those whose sites are mainly information only, or transactional but not really engaging in behavioural marketing, will be primarily in the 'strictly necessary' bracket. However, currently the requirement is for informed consent, that is, at the very least a 'proactive opt-out' for those cookies at this less intrusive end of the scale — even for a basic component that many mainstream websites

operate, such as, capturing Management Information (MI) about the number of site visitors, for example. To put this in the same bracket as, for example, behavioural advertising is probably the factor that is most taxing for those tasked with addressing the regulation changes in their organizations. It appears quite an imposition on customers to even be asking for consent '*so we can carry on doing stuff that you probably don't mind us doing anyway*', or even expecting them to have an understanding of the meaning of cookies.

What must not happen is that these requirements become a battle ground of commercial freedom v privacy. This should be about transparency and effectively and intelligently enabling those interested in amending what organizations glean from them. But it should not hamper what for many is a route to information, services and products, who care little about those organizations trying to learn about them as customers other than that it will improve the service experience over time.

Equally, it is going to be hard to find the right balance if this is not thought through sufficiently. While it's great not to be prescriptive about the solutions for Consent, what is trying to be communicated is, let's face it, not something that most people think about, and having hundreds of different ways of describing the same thing to customers is possibly not the best approach. Customers could be the biggest losers in this if we're not careful. The Internet Advertising Bureau (IAB), the Article 29 Working Party, the International Chamber of Commerce Working Group, Government and the ICO *et al.*, are all working on the challenge, including developing standards and improved browser settings, branded trusted icons and so on. But if browser settings won't work on users' mobile devices or are not synched, and the whole Consent experience needs to be carried out a second time or can't be delivered at all, this may be a sign that we need to pause for breath on this? — And in the meantime, ensure that privacy policies are updated and comprehensive, carrying out those cookie audits, then prepare to highlight intrusive cookies and explain how to switch off, taking stock in May to see where browsers, internet security software and other common standards have got to in helping to offer an integrated and clear set of choices to consumers.

Freedom of choice — The balance of control

It absolutely makes sense that those actively or occasionally or just at some point becoming interested in privacy and the use of their data should be given access to how any website they use is working, and be able to effect change, understanding any impacts on their experience. The current climate of information being constantly collected from us with little or no transparency and sometimes a degree of commercial exploitation should rightly have a balance reset. For example, the farcical Hobson's choice way in which the collection of terms and conditions acceptance consent has been abused, the fact that I can't stop a company recording my call or keeping my email address if I email them — at least not easily — and can't stop myself being recorded on CCTV and so on. This Amendment marks the start of a *re-balancing of control*

between consumers and organizations appropriating something with little awareness and no choice of what they have just gifted to a website.

However, as noted earlier, there are already checks and balances DP, PECS as they stand, increasing general awareness about privacy and settings — people being enlightened and empowered at their own pace, organizations increasingly realizing the value of clear privacy policies. Non-intrusive cookies may be quite low down the list of privacy breakers, and we do need the regulator to take a measured approach to the mechanics used to gain consent. Privacy is part of a landscape, not something that stands in isolation from everything else, and it should not be artificially drawn out in a way that results in confusion and annoyance, and no real value.

The ICO is the regulator, not the enactor or legislator; they are trying to assist, and they do plan to publish more guidance. We shouldn't shoot the messenger, but compliance resources need to be used and applied sensibly. So let's hope the ICO is pragmatic beyond May 2012, and focuses its pursuit of compliance (and certainly any strong sanctions) on those whose businesses are based on more intrusive cookies, digital tracking and messaging, who are not being clear and straightforward with users. Also that the ICO continues to work with Government, industry and other stakeholders in the development of recognizable mechanisms for making choices that those consumers can have confidence in managing.

Note

1. The ICO would like to use cookies to store information on your computer, to improve our website. One of the cookies we use is essential for parts of the site to operate and has already been set. You may delete and block all cookies from this site, but parts of the site will not work. To find out more about the cookies we use and how to delete them, see our privacy notice.
☐ I accept cookies from this site.

*Mark Chipperfield,
BBC Head of Data Management*

Did mass-mailing to 6,000 nurses breach database right?

Stephen Groom

Journal of Direct, Data and Digital Marketing Practice (2012) **13**, 256–257.
doi:10.1057/dddmp.2011.39

Topic: Direct marketing

Who: Beechwood House Publishing Ltd v Guardian Products Ltd & Anor

Where: Patents County Court, England

Law stated as at: 5 September 2011