

Current Legislation and the Future

The most important thing to understand about legislation which impacts on the advertising industry is that this legislation is not new and has existed (in most cases) for some time. What we have seen in the past couple of years is a shift in public awareness and attitude with regards to the use of personal data which has led to a renewed focus on many different industries with regards to the collection and handling of personal data.

The Data Protection Act (DPA) is perhaps the most well known piece of legislation with regards to personal data and privacy and even those of us who have not read the Act will have undoubtedly heard it mentioned many times in different situations, particularly when communicating with the commercial sector and having to go through various "security" checks in order to commence those communications (for example when talking to a bank or utility provider on the telephone).

Whereas the DPA is probably the most well known it may be one of the least protective laws currently in place and by the admission of the Information Commissioner's Office (ICO) during a panel at the Convention on Modern Liberty last month, actually provides public authorities with very little enforcement power. They are seeking stronger enforcement powers, at present there is no route for the ICO to prosecute companies who are registered as personal data "handlers", for ignoring the law – a point which is becoming a frequent frustration to members of the public.

With regards to digital advertising we have a number of pieces of legislation which are relevant such as Privacy and Electronic Communications (EC Directive) Regulations (PECR), Regulation of Investigatory Powers Act (RIPA) and Computer Misuse Act (CMA).

PECR also falls under the remit of the ICO and the ICO in a correspondence to a member of the public last year stated that covert trials of behavioural advertising using Deep Packet Inspection technology in 2006/2007 probably breached Regulation 6 of PECR; however the ICO declined to enforce the regulations as they believed there was no damage to the consumers involved.

RIPA covers the interception of communications (often referred to as "wire tapping") so it becomes relevant when we discuss the interception of communications over a network without the consent of all parties.

CMA covers the use of computer technology and resources which belong to a third party therefore in the case of digital advertising CMA would be relevant if the advertising technology has any adverse effect on such resources (such as Spyware or the placing of "forged" cookies onto a consumer's computer).

There is also the Copyright, Designs and Patents Act which is of particular relevance when discussing the use of Deep Packet Inspection models such as Phorm's Webwise, since this model relies on making an identical copy of a

copyrighted works and then making a derivative works during the processing of that data; which is not permitted without license.

Finally, given the nature of behavioural advertising in the future the Protection from Harassment Act may also become relevant – this could certainly be the case where a consumer's choice is determined by a temporary technology such as a cookie. If the consumer is forced to "Opt-Out" over and over again to avoid behavioural profiling this could be seen as a form of harassment.

The regulations above all require the consent of individuals before the collection, processing and use of their data is permitted. Consent must be explicit and informed consent and it is this issue which has come to the forefront over the past 12-18 months.

The Internet Advertising Bureau (IAB) have recently been criticised by Dr Richard Clayton of Foundation for Information Policy Research and the Open Rights Group after launching a set of good practice guidelines for the on-line advertising industry. The reason for this criticism is that the guidelines both fail to understand the issue of consent (stating it as a preference as opposed to a requirement) and also the mechanism from which consent should be determined.

The EU Commission, Home Office, Department for Business Enterprise and Regulatory Reform and Information Commissioner's Office have all made public statements concerning the mechanism for determining consent. It is clear under the law that consent must be informed, explicit and determined on an Opt-In basis – and this is the crux of the matter.

For years corporations have been able to hide behind legalese in the form of Terms and Conditions, Privacy Policies, End User Licence Agreements and other long winded and indigestible contracts between themselves and their customers. It is common knowledge that consumers rarely read these documents and simply agree to what is offered "on good faith" that the contracts will not contain any terms which might be prejudicial to their rights. Unfortunately, this has not always been the case.

With the introduction of the Consumer Protection from Unfair Trading Regulations 2008 and the Unfair Terms in Consumer Contracts Regulations, however, there are some protections in place which should, over time, resolve some of these issues. Certainly the banking industry has been suffering for the past 36 months with regards "unfair terms in contracts" at a cost of tens of millions of pounds in out of court settlements for bank charges.

Opt-Out mechanisms, legalese and long winded contracts are ethically questionable and often designed specifically to increase revenues from an uninformed and frequently apathetic public. Big brand corporations have a certain degree of trust from the public which should not be abused.

If Opt-In is going to have a negative impact on revenues the commercial sector must find stronger incentives to ethically attract subscribers to their services.

The answer for regulators is not so easy given the technical nature of the debate, the speed with which it is evolving and the sectoral dominance of a few powerful ISPs. The challenge for Parliamentarians is to allow the Internet to develop freely and in a commercially viable way, while keeping the privacy of the public protected.