I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising
Andrew McStay
New Media Society 2013 15: 596 originally published online 30 September 2012
DOI: 10.1177/1461444812458434

The online version of this article can be found at:
http://nms.sagepub.com/content/15/4/596

Published by:
SAGE
http://www.sagepublications.com

Additional services and information for New Media & Society can be found at:

Email Alerts: http://nms.sagepub.com/cgi/alerts
Subscriptions: http://nms.sagepub.com/subscriptions
Reprints: http://www.sagepub.com/journalsReprints.nav
Permissions: http://www.sagepub.com/journalsPermissions.nav

>> Version of Record - May 24, 2013
OnlineFirst Version of Record - Sep 30, 2012
What is This?
I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising

Andrew McStay
Bangor University, UK

Abstract
This paper assesses implications for the practical and theoretical understanding of consent in light of the coming into force of the European Cookie Directive (2009/136/EC). This Directive shifts behavioral advertising from being an opt-out practice to an opt-in one requiring consent. The aim of this paper is to assess conceptions of consent as detailed by the European Article 29 Data Protection Working Party, the UK government and the behavioral advertising industry. This is achieved through the application of philosophical understandings of consent generated in the first half of the paper that detail the ways in which these have been applied in health, an area that deals extensively with informed consent. The paper concludes by offering recommendations to behavioral advertisers on how best to implement opt-in consent policies so as to progress to ethically sound privacy practices.

Keywords
Autonomy, behavioral advertising, consent, Cookie Directive, Europe, policy, privacy, UK

Introduction
This paper analyzes the notion of consent in a behavioral advertising context, offering suggestions for how advertisers might obtain authentic and morally correct consent from users. The background context for this paper stems from recent legislative changes in Europe regarding the use of cookies. Whereas previously cookies were stored on a user’s
computer on a ‘right to refuse’ basis (opt-out), it has now shifted to one that requires consent be obtained on an opt-in basis. In May 2011 this was implemented locally in the UK. Whereas in the past website owners/managers had to tell users how they used cookies, and how users might opt-out if they objected, they now have to gain consent from users if they are to place cookies on a user’s machine. Exceptions to this rule are restricted to situations where the placement of cookies relates to a service explicitly requested by the user, as with the case of automatic form-filling for example. Third-party cookies, the type employed by behavioral advertising firms, are given special attention by the legislation.

While a paper on legislation and consent may not excite at the outset, its treatment is necessary and worthy for the simple reason that legislation is foundational. This particular change in legislation presents a privacy crossroads and grants us a moment to reflect on what we mean by consent as we progress towards the enforcement of legislation requiring opt-in approaches to cookie use. As is becoming increasingly clear, the most significant developments in advertising have to do with the apparatus of delivery and the control of information flow. It is to these mechanisms and the legislation that guides these that contemporary critical attention should be turned. Such standards represent an analyzable crystallization of power relations and articulation. The remit of this paper is thus to look at one particular development in the shifting sands of privacy, focusing on the implications of the coming into being of the Cookie Directive (2009/136/EC). This is an amendment to three pieces of legislation: the Universal Service Directive (2002/22/EC); the e-Privacy Directive (2002/58/EC); and Regulation (EC) No. 2006/2004 that addresses the enforcement of consumer protection for consumers living in other EU countries. Of particular interest are changes to the e-Privacy Directive (2002/58/EC), the ways in which this has been interpreted and implemented in the UK, the relationship between the UK government and the behavioral advertising industry, and concurrent implications for conceptions of consent. This paper refers to a wide range of organizations, legislative bodies and pieces of legislation, and so to save the reader having to keep track these are summarized in Table 1:

What is behavioral advertising?

Behavioral advertising tracks users’ browsing activities between websites over a period of time for the purposes of serving advertising tailored to what advertisers assume are users’ interests. In addition to advertisers and the owners of media spaces, the process of behavioral advertising involves an additional party in the form of advertising networks. These are companies that connect media owners with relevant advertisers. Their effectiveness stems from the number of media owners/web publishers they have signed up to their services as they collect and use browsing data when an Internet user visits one of a number of websites participating in that particular network. To deliver targeted advertising, systems gather information on sites visited and pages viewed from users’ cookie-enabled web browsers. Cookies are small text files placed on a user’s computer by a web browser that stores credentials that identify each session between a browser and a server (the computer that a browser ‘talks’ with to receive information) and the interactions between a user’s
Table 1. A brief account of salient legislation and organizations.

<table>
<thead>
<tr>
<th>Title</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Article 29 Data Protection Working Party</td>
<td>Constituted by a representative from the data protection authority of each EU member state, the European Data Protection Supervisor and the European Commission, it advises, promotes and provides opinion on data protection.</td>
</tr>
<tr>
<td>European Cookie Directive (2009/136/EC)</td>
<td>This is an update or amendment Directive that requires upfront consent for the placement of cookies on the Internet.</td>
</tr>
<tr>
<td>Data Protection Directive (95/46/EC)</td>
<td>Protects individuals in terms of the processing of personal data and the movement of such data.</td>
</tr>
<tr>
<td>Privacy and Electronic Communications Regulations 2003 (PECR)</td>
<td>UK legislation that regulates direct marketing activities by electronic means.</td>
</tr>
<tr>
<td>Information Commissioner’s Office (ICO)</td>
<td>The UK’s independent authority created to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.</td>
</tr>
<tr>
<td>Department for Culture, Media and Sport (DCMS)</td>
<td>Among other responsibilities, they champion the UK’s digital economy and creative industries (including advertising).</td>
</tr>
<tr>
<td>Internet Advertising Bureau (IAB)</td>
<td>A trade association that supports and promotes the growth of the European digital and interactive marketing industry.</td>
</tr>
</tbody>
</table>

terminal and a given website. They allow web pages to ‘remember’ a user and are commonly described as providing the web with a memory.

As Shah and Kesan (2009) detail, third-party cookies, the type that behavioral advertisers use, came about through a loophole in Netscape’s original design of cookies that were only intended to be matched with a specific website (first-party). The loophole is that Netscape’s cookies’ specification permitted owners of third-party components of a webpage to insert their own cookies. This created an opportunity for online advertisers to be able to track users across affiliated websites who had signed up to their services. Due to this ambiguity, the online advertising firm DoubleClick were able to read and write to a cookie when a user visited websites that subscribed to their advertising services. Recognized as a privacy threat since their inception, third-party cookies run contrary to the original idea of cookies being matched with one web domain only. It is this technological gap that facilitated the growth of the behavioral advertising industry.
Critical conceptions of consent

As Norberg et al. (2009) note, privacy issues represent inefficient information flow and an increase in economic costs that stymie the capacity of a system to deliver maximum benefits and opportunities. For critics of the industry, the case of behavioral advertising privacy revolves around concern with ‘the right to selective disclosure’ (Van Dijk, 2006: 114). This involves deeper consideration about control over one’s personal data and how the data is processed. It also relates to fear of unintended consequences, as data, once captured, may be aggregated, remodeled and sold (Ball et al., 2006; Lyon, 2001; McStay, 2011; Van der Hof and Prins, 2008). The industry’s sincerity towards consumer education is questionable, as it stems from a wish to legitimize itself in the eyes of both policymakers and consumers. Citing Zarsky (2004) and Gandy (1996), education for Baruh (2007) is an ‘autonomy trap’ where communication is fashioned for a given business goal rather that to serve the balanced needs of informed consent. Similarly, in a discourse analysis of US privacy policies, Fernback and Papacharissi (2007) highlight industry tendencies to address the reader respectfully, but breach this relationship through contradictory and vague claims about privacy protection. Another key problem is transparency and informational asymmetry: while our mediated lives become increasingly transparent, those who seek to profit from our data are incredibly opaque (Gandy, 2000). This lack of transparency only serves to create privacy phantoms, and rather than serve the industry, it hinders it.

Viewed rationally, we use privacy as a currency of exchange in that we are willing to give away small amounts of privacy for certain gains, but find other privacy costs too high for the service returned. LaRose and Rifon (2006) make the same point, stating that disclosure is weighed against financial benefit and negative outcomes. This raises questions about responsibility and the extent to which we should look after privacy. In many cases we as participants are partly culpable in our own surveillance, as we offer up personal details for services and rewards although, as Lanier and Saini (2008) highlight, such incentives can only be truly ethical and voluntary when consumers fully understand the nature of the bargain. Conversely, yet related to this, Acquisti and Grossklags (2005, 2007) point out that the rational actor thesis is flawed. This is due to lengthy privacy policies, heuristics and short-term decision-making, and more broadly instant (and longer-term) gratifications that web services offer (for critical accounts of rationality and privacy also see Joinson et al., 2008; Miyazaki and Krishnamurthy, 2002; Munro, 2001; Nehf, 2007; Turow et al., 2008). As research carried out by the European Commission signals, our privacy-oriented behavior tends to be inconsistent, and while we may signal concern about privacy, we tend toward short-term gains over voiced principles (Flash Eurobarometer – The Gallup Organization, 2008). This has to do with the conditions within which privacy choices are made. How are consumers to know what happens to personal data? How can they know with whom it might be shared/traded? How can they guess the lifecycle of their data? How are they to know its value? Without disclosure or transparency, how can consumers know what they are opting into, or out of? Beyond this, we must also consider ways in which the rationality of users is limited by information provided, cognitive limitations, heuristics, behavioral biases, and the amount of time they have to make decisions. Therefore, to view individuals as rational economic
agents who are able to go about deciding how to protect or divulge their personal information is highly misguided on a number of levels.

One might simply argue that consumers do not care about privacy. Indeed, perhaps people simply are not that bothered about their data traces, what sites they visit, what they do on those sites, what they write and post, and how this information is processed and shared. As Nehf (2007) finds, consumer behavior regarding web navigation tends to involve low-effort decisions and the pursuit of goals that render privacy less salient than other aspects of web experience. However, we might also approach the issue from another angle. Perhaps privacy matters are too complicated. Turow’s (2003) empirical investigation of privacy seems to suggest this. His participants were unclear on both the nature of data processing and how to protect their personal information. When the techniques employed by online organizations were revealed to them, participants were unhappy (also see LaRose and Rifon, 2006). Gomez et al. (2009) make similar points arguing that the low number of complaints simply conforms to the hypothesis that users file complaints only when they perceive an invasion of their privacy and they know where to file a complaint.

Conceiving consent

This counter-posing of rational and irrational approaches to privacy is misleading, particularly regarding behavioral advertising. The simple truth is that most people do not understand the mechanisms through which behavioral advertising works. In a report on data sharing for the UK Prime Minister and the Secretary of State for Justice, Thomas and Walport (2008) distinguished between genuine consent and consent that is simply enforced agreement. In many areas of the digital sector the latter has been the modus operandi for some time. Genuine consent means something different. To give consent is to act. Consent is not passive, but rather requires that people do something. This means that people must be informed and able to conceive an educated opinion so as to express will. Without this there is no consent, but rather the application of force. In expressing will there is agency, volition, control, deliberateness and making something happen. To be devoid of understanding is to be unable to give proper consent.

The notion of consent flows from liberal conceptions of freedom. Freedom does not equate to being able to do whatever we want, as plainly we are physically and materially limited. We are also restrained by the duties of one person to another. Freedom then is paradoxically a mutually limiting activity. However, a belief in freedom is underpinned by a belief in autonomy, self-mastery, free choice, voluntariness, privacy and accepting responsibility for our choices. Indeed, privacy serves to guarantee autonomy and the right to personal choice, assuming no conflict with others. In a Kantian (1993 [1785]) sense, autonomy is an end in itself as it underpins freedom, although in accordance with Kant’s universalizing principle we should take care not to restrict the autonomy of others. Kant’s normative theory underpins much policy and applied ethics. It is a deontological notion in that it is not contingent on a consequence or outcome, but rather its value comes from itself. It stands opposed to pragmatism and consequentialism where ends may justify moral means although it should be noted that even for pragmatists such as Rorty, privacy ranks as close to intrinsically important as possible. He remarks that
‘J.S. Mill’s suggestion that governments devote themselves to optimizing the balance between leaving people’s private lives alone and preventing suffering seems to me pretty much the last word’ (1989: 63). In this deontological and liberal account, autonomy is of the utmost importance and is only trumped by egalitarian respect for others and their autonomy (as with other classical liberals such as Locke, Mill and Rousseau). Thus, in building an understanding of consent, we must first begin by acknowledging the right of others to autonomy. This is perhaps best expressed in Kant’s second formulation of the categorical imperative: ‘Act in such a way that you treat humanity, whether in your own person or in the person of another, always at the same time as an end and never simply as a means’ (1993 [1785]: 23). Applied to behavioral advertising, there is nothing wrong in using people’s data as a means of making money (that is, using people as a means to advance one’s goals) as long as people’s rights are also respected − notably, their right to autonomy and privacy. If we freely and voluntarily consent, behavioral advertising is acceptable; if not, it is not.

The right to privacy is an extension of the right to autonomy, which relates to self-determination. According to Locke (2005 [1689]) liberal democracies are predicated on developing civil rights that allow for autonomy as an intrinsic human capacity and character of well-being. Any practice that impinges on this is on shaky ethical terrain although autonomy may be trumped by an appeal to the greater (social) good. Respect for autonomy equates to rights to self-determination, which underpins the principle of informed consent. A useful analogy can be found here in the health literature, where informed consent is paramount (Faden and Beauchamp, 1986). Informed consent is vital to guard against the possibility of bodily intrusion without consent. Indeed, it is here that the absurdity of consent as that which does not need to be gained prior to the event is shown. If one undergoes treatment, the suggestion that consent might be granted mid-way through an operation or afterwards is farcical.

Within health-based conceptions of consent, privacy is not negative (what is being hidden), but positive. It is framed in terms of dignity, freedom and the capacity to manage boundaries regarding what one wishes to share, reveal or allow access to. It is in essence about control and by comparing our informational setting with health, we might better hold to account data-miners and policy-makers that seek to win consent for behavioral advertising by any means possible. Within behavioral psychology research, for example, one must acquire freely given informed consent in order to probe personality, attitudes, opinions, behavior and beliefs. While one should not follow the parallels between behavioral advertising and psychology too closely, as one refers to the mining of aggregated informational mobility and the other to intense solo scrutiny, they are both involved with interiority, access, information-gathering, processing and the putting to use of data in some way.

In health, informed consent is required before treatment, procedures and research. It is paramount that in providing information about treatment, deception of any form should be guarded against at all costs and cannot be justified by any means for a ‘greater good’ (for example, benefit to the wider society or the progress of science). Furthermore, any notion of voluntary consent is impossible when the participant is either a captive audience or unaware that research is taking place. This last proposition is particularly because in the early days of behavioral advertising, when regulation was light-touch so as to
facilitate commercial activity, the industry was predicated on the fact that people were unaware and captive (turning all cookies off led to an inability to use many websites). Having established that clearly informed consent must come from autonomous action, we can say that someone is deemed to act autonomously if they act intentionally, with understanding and without being controlled or influenced by others. The latter two points are connected in that the better the understanding, the less opportunity there is for being controlled, notwithstanding technological coercion (for example, locking people out of websites and/or services). If undue influence and coercion is present, this invalidates autonomous expression and the giving of consent. However, although understanding is important, we cannot state that full autonomy requires full understanding, as this only exists as an ideal and falls short of the experiences of daily life. Perhaps the recognition of imperfect information and choice is best expressed in liberal perceptions of democracy, as explored below.

Lessons from political consent

It is useful to go back to Locke, contract theory, political philosophy, and early discussion about the nature of consent and the constitution of free agents. Here, our property cannot be violated by government or others without our consent. To quote:

Men therefore in society having property, they have such a right to the goods, which by the law of the community are theirs, that nobody hath a right to take their substance or any part of it from them, without their own consent. (Locke, 2005 [1689], §138: 113)

In the context of Locke, consent within a commonwealth (an independent community) is morally binding on the basis that it is voluntary, and undertaken after reflection and deliberation. Indeed, moral authority itself is often understood by dint of common agreements by contractarians. Whether consent is expressed or tacit, being based on rationality and self-interest, it is considered. Tacit consent for Locke involves enjoying the benefits of land, lodging or carriage within the territory of a given government. Tacit consent is defined through the period by which enjoyment lasts and explicit consent involves full membership (Waldron, 1994). In Locke’s account of tacit consent, people are not obliged to remain, and are free to join other commonwealths they find preferable, or even begin new ones in places that do not belong to anyone.

Importantly for our discussion of the digital environment, tacit consent is something in the past that has been given silently. Tacit consent has been the default position of the behavioral advertising industry and the trade associations that represent them. Their argument has been that as users enjoy services and platforms, tacit consent is granted. By dwelling in the dominion or domain of those who use third-party cookies, consent is deemed to have been granted. If people have not actively dissented, then consent has been obtained. Silence and doing nothing has been, until recent changes in legislation, the default position on consent.

There are criticisms to be levied against contractual theories of consent. Most pointed is that as contracts are undefined, the nature of relations between users and behavioral advertisers and third-party operators cannot be characterized by consent. In asking to
what extent the use and enjoyment of media that employ behavioral advertising constitutes tacit consent, we can follow Hume who points out: ‘We may as well assert, that a man, by remaining in a vessel, freely consents to the dominion of the master; tho’ he was carry’d on board while asleep’ (1753: 313). Tacit consent in digital matters is not credible, as the majority of people do not know how to dissent and are ‘asleep’. Plamenatz (1968 [1938]) similarly rejects tacit consent, arguing that it does not follow that being within a given territory constitutes actual consent. That is to say, however we prefix consent, we cannot remove the expressive element of consent that requires affirmative action. Plamenatz’s own definition of consent is useful: ‘We have consent, therefore, whenever the right of one man to act in a certain way is conditional upon another man’s having expressed the wish that he should act in that way’ (1968 [1938]: 4). To be clear: consent cannot be passively given, it can only be actively given. For Plamenatz consent has to be an issuing of permission that informs another that they have been given the right to perform an action of whatever sort. As per the European Article 29 Data Protection Working Party (hereafter Article 29 Working Party), this affirmative action need not be written or signed, but may be oral, a gesture or whatever action is most expedient.

Changes in legislation

Since its inception, behavioral advertising has been predicated on being able to deposit cookies on users’ terminals upfront. If users were aware of their existence and unhappy with this intrusion, they had to opt-out (if they knew how). The coming into force of new legislation requiring users to opt-in has raised questions about the nature of consent in relation to cookie use and consumer profiling. The change in legislation comes from the decision by the Article 29 Working Party that users should not only receive information about cookie use, they should also have to give informed consent.

The reasoning behind this is straightforward: most users are unaware of how to reject cookies, so therefore inaction cannot be taken as unambiguous consent. Implementation of the new Directive requires that users be fully informed about the information being stored in cookies and why they see particular advertisements. The key development relevant to behavioral advertising is the coming into being of the Cookie Directive (2009/136/EC) that delivers an amendment of Article 5(3) of the old e-Privacy Directive (2002/58/EC). The previous version of Article 5(3), with author’s emphasis, states:

> access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.

The new version of Article 5(3), again with author’s emphasis, states:

> gaining of access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.
This has been broadly interpreted to mean that the storing or accessing of information on an end user’s computer is only permitted if the user has given his or her explicit consent. This establishes an opt-in requirement for the use of cookies, but does not apply to all uses of cookies. For the web to work efficiently cookies are essential and many uses are exempt from the new regulations, in particular those that aid online shopping (e.g. the ‘add to basket’ button), automatic form-filling and other non-intrusive web-based activities as conceived in Netscape’s original cookie template. Rather, attention is drawn to the use of cookies not related to the service requested by the user. This applies, for example, to cookies that collect statistical information about visitors to a website, cookies that offer a more attractive personalized experience to a website, or – as focused upon in this paper – third-party cookies.

**Article 29 Working Party and consent**

In July 2011 the Article 29 Working Party (2011) released a document titled *Opinion 15/2011 on the Definition of Consent* detailing their conception of consent so as to clarify a common understanding of consent and what it means in a European legal context. The impetus for this came from the understanding that the views of member states differ as to what constitutes consent. It states that from the beginning consent has been built into the legislative process on data protection and privacy culminating in the Data Protection Directive (95/46/EC). The conditions for consent are that it is freely given, specific and informed. However, it also admits to ambiguity over the ways in which consent may be given.

In outlining the meaning of consent, the Article 29 Working Party states that for consent to be legitimate, it must be informed. As with the definitions and perspectives on consent detailed above, this involves adequate understanding, volition, will and deliberateness. In addition, consent may only be meaningful if it is free from deception, intimidation, coercion or significant negative consequences. It should also be specific and refer transparently and accurately to the scope and consequences of the data-processing. This requires that all necessary information be given at the moment consent is requested, and the implication of the language in the Directive is that ‘consent has to be given before the processing starts’ (2011: 9). While the Directive is relaxed on the form that consent might take, it must involve action and indicate or signify a direction or preference. This stands in contrast to the pre-2011 situation where consent may have been defined and inferred through lack of action, which falls short of the definitions of consent detailed in the first half of this paper.

The Article 29 Working Party is clear that data should not be repurposed, sold on or used for any other purpose than that which was actively consented to. There is flexibility here in that if one subscribes to a service then one might be interested in information about new products from that service. It does not allow for the sending of individuals’ data to third parties without consent. This would contravene deontological requirements for voluntariness, privacy and self-determination that underpin the Article 29 Working Party’s position. Moreover, as with medical consent, affirmative action requires that users be informed and that information must always be provided before there can be consent. The average user or data subject should be able to appreciate and understand
relevant facts, along with the implications of an action. Information should also be given directly, and not merely be available somewhere. Unambiguous consent thus requires that in addition to being informed, the act of consenting is clearly expressed and not passive (e.g. one clicks to assent rather than doing nothing).

In discussion of Articles 6(3), 9, 13 and 5(3) of the e-Privacy Directive (2002/58/EC), the Article 29 Working Party draws attention to implicit and explicit references to prior consent, and rightly point out the logical outcome of what happens when consent is granted after the tracking process has started. They comment that ‘if the individual decided against consenting, any data-processing that had already taken place would be unlawful for that reason as well’ (2011: 31). In regard to means of obtaining consent, the Article 29 Working Party is forthcoming with recommendations suggesting that as browsers are modified to provide better cookie management they should require users to ‘go through a privacy wizard when they first install or update the browser and provide for an easy way of exercising choice during use’ (emphasis in original, 2011: 32). This is less specifically but formally asserted in Recital 66 of the Cookie Directive (2009/136/EC) that states that a ‘user’s consent to processing may be expressed by using the appropriate settings of a browser or other application’. Such a proposal meets the requirement of unambiguous indication and that the data subject is given the opportunity to make a decision and to express it. It also means that the option is conspicuous and cannot be overlooked. The Article 29 Working Party concludes by highlighting that the rules are not intended to be constrictive and that they are open to numerous ways of giving consent. Underlined, however, is the premise that ticked default options that grant consent are not acceptable, as this opt-out approach constitutes consent based on silence.

**UK implementation**

In the UK, the Cookie Directive (2009/136/EC) is expressed in changes to Regulation 6(2b) of the Privacy and Electronic Communications Regulations 2003 (PECR), which itself is the transposing into UK law of the e-Privacy Directive (2002/58/EC). Prior to 26 May 2011 it stated (with author’s emphasis):

6.(1) Subject to paragraph (4), a person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.

(2) The requirements are that the subscriber or user of that terminal equipment –

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

(b) is given the opportunity to refuse the storage of or access to that information.

The amended Regulation now states:

6(1) Subject to paragraph (4), a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.

(2) The requirements are that the subscriber or user of that terminal equipment –
(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

(b) has given his or her consent.

However, there has been confusion among both government and the industry as how to interpret these changes, particularly as browser solutions were not technologically viable in 2011. The British Information Commissioner’s Office (ICO) details a range of means of obtaining consent and that consent need not involve ticking some sort of box as this is only one means among others of giving consent. The key lies in the Data Protection Directive (95/46/EC) in Article 2(h), which defines ‘the data subject’s consent’ as ‘any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed’.

The ICO (2011a, 2011b) suggests that this might mean clicking an icon, sending an email, subscribing to a service, or indeed the use of browsers. The Department for Culture, Media and Sport (DCMS) (along with the ICO) delivered an open letter stating that their interpretation of changes to the Privacy and Electronic Communications Regulations 2003 (PECR) is light-touch and business-friendly, and that they only seek to carry out the minimum necessary to comply with the Directive. The letter points out that the definition of consent is not strictly time-bound as the word ‘prior’ does not occur in Article 5(3) of the e-Privacy Directive (2002/58/EC). As such, there is no constraint on when consent may be given. It suggests that ‘it is possible that consent may be given after or during processing’ (DCMS, 2011c: 3). However, it follows this with the contradictory proposition that informed consent is required. They also suggest in the letter that consent may be given by either leaving browser settings as they are (if the user is provided with adequate information about cookies and what those settings mean), and that ‘they “may” also signify consent through choosing not to amend settings or controls of a browser’ (DCMS, 2011c: 4). It is difficult not to come to the conclusion that this is essentially the situation as it stood before the new legislation came into force. If we acknowledge the absurdity of the proposition that consent could be granted mid-way through a medical operation, it is clear that the UK understanding of consent is untenable. If consent is to be held as a panacea, then by definition it must be acquired upfront. If not, it does not fall within definitions of consent but is rather a subtle application of force. The Internet Advertising Bureau (IAB), the trade association that represents the digital advertising industry, is supportive of both the Directive and UK implementation. Over the last two years it has engaged in a number of educational activities for both industry and consumers. Culminating in their Good Practice Principles (www.youronlinechoices.com), they have sought to stave off opt-in regulations by highlighting the role of choice for consumers and the need for consumers to be notified about behavioral advertising. This is understandable, as information about people is both fuel and enabler for the digital economy. Indeed, as made clear in governmental visions of Digital Britain, which gave rise to the Digital Economy Act 2010, privacy concerns are for many policy-makers and businesses an artificial barrier to industrial growth.

The open letter by the DCMS supports the self-regulation of behavioral advertising, stating that industry is best placed to develop technical solutions that meet the requirements of the Directive. This is also reflected in the April 2011 Impact Assessment by the
DCMS in response to the revised e-Privacy Directive comment that the problem is one of information, and that ‘users do not have sufficient information about the use and management of cookies that is easily accessible’ (DCMS, 2011a, §7: 1). They state that government intervention is here to ‘ensure consumers have optimal information when acting to ensure their privacy’ (DCMS, 2011a, §7: 1). While acknowledging that Article 5(3) of the e-Privacy Directive is to ensure informed consent regarding the potential placing of cookies, the DCMS go on to state that although the UK seeks to increase user awareness of cookies, it also seeks to minimize the burden on business. This is both colloquially and philosophically a pragmatic approach. It is noteworthy, though, that even Rorty (1989), who resolutely stood against moral absolutes, took an interest in privacy and the need for a binary of public and private selves, and the right to be left alone. In contrast to legislating an opt-in solution for cookies, the UK has decided on self-regulation, the use of browser settings and the provision of better and more accessible information. Following self-regulatory approaches, behavioral advertising and web-analytics firms will pay the costs of providing this information to consumers. Browser vendors will meet the costs of reprogramming browsers and providing enhanced settings, and will also take responsibility for communicating the settings and technologies to web developers and third parties.

Section 34 of the DCMS assessment requires close scrutiny. It highlights that if browsers remain at default settings (cookies on) then the indirect impact may be reasonably modest. If they are reversed to reject all third-party cookies, the situation may be different. The report does not offer a way forward, refusing to answer the question of ‘on or off’. Rather, the government suggests that it will work with browser manufacturers to see if browsers can be enhanced to meet the requirements of the revised Directive. It reinforces the informational aspect stating that:

> users will be provided with more information as to the use of cookies … and will be presented with easily understandable choices with regard to the importance of cookies on to their machine, including the ability to refuse consent to all cookies. (DCMS, 2011a, §34: 16)

In presenting the likely outcome if an option to opt-in was given, the DCMS, drawing on research they commissioned by PriceWaterhouseCoopers, remark that half of Internet users would change their behavior and not accept third-party cookies. A question then is raised about the sincerity of the UK’s approach to opt-in arrangements in light of the potential impact on the behavioral advertising industry and the support the DCMS have offered in the past to the behavioral advertising via initiatives to nurture the UK’s digital economy. The DCMS (2011b) also published responses to their proposals for the implementation of Article 5(3). These were very favorable toward business, stating that the use of browser settings has worked well to date, with no evidence of consumer harm, and that this model of providing information within privacy policies to gain consent should continue to be applied going forward. Among responses there were concerns about the sophistication of browsers that are not able to reject some third-party cookies but accept others, meaning that users may be ‘deprived’ of receiving some cookies. The point about harm is a fallacious argument if consent is to be adhered to. Consent is not acquired by dint of absence of harm, but is predicated on affirmative
action, autonomy and expression of will, so as to either allow an action to occur, or to permit another to act on a person’s behalf.

The report also highlights that browser solutions are not viable at present as they would not fit the requirements of the legislation. Favoring self-regulation and industry-based approaches, consumer-focused information involves: the provision of more industry-created information on the use of cookies; a privacy policy notice; a single consumer control page; icons linking to information about each specific Internet advertisement (including the advertiser, the server and who the advert has been customized by); an option to refuse those and other cookies (including an option to refuse all cookies from that server); and a link to further information on privacy and behavioral advertising. Demonstrably the industry has been successful in staving off what is required: truly opt-in legislation where users take prior affirmative action to accept third-party cookies. While self-regulatory activity with the support of the UK government reflects a shift from implied to informed consent, it falls short of the required opt-in means of engaging with behavioral advertising. This would have to do with upfront expressed consent that is stated, not predicated in silence, and is unmistakable.

**Applications for consent**

The privacy crossroads the UK and wider Europe finds itself at provides an opportunity to address concerns through a properly thought-out approach to consent. The simplicity of the IAB’s Good Practice Principles (www.youronlinechoices.com) that are currently set to opt-out provides an excellent template with which to begin to build upfront, informed, opt-in practices. This, in tandem with the Article 29 Working Party’s suggestion of a ‘privacy wizard’, would simplify the process of deciding which cookies to accept and which to reject.

If informed consent may only exist through the perfect knowledge of all details involved in data-processing (if such an idea is possible), then something has to change for it to be meaningful in the real world of time pressure, heuristics and the wish to get things done sooner rather than later. We might look to health once more, where understanding stems from ‘adequate apprehension’ of all relevant propositions or statements, and comprehension of the nature of the action, the foreseeable consequences and possible outcomes as a result of performing or not performing the action (Faden and Beauchamp, 1986). Intended for clinical purposes, the clause of adequate apprehension is useful, but requires qualification due to differing perspectives on privacy among those interested in the practice of behavioral advertising. To find common agreement among stakeholders on what constitutes objective information may be problematic. If we seek to engender understanding, more than one perspective should be presented on cookie use, the gathering of personal information and the ends to which this is put. These perspectives might be granted equal media space in the form of an individual linked page created by the IAB and a recognized privacy group (for example, the Open Rights Group). This is not to achieve objectivity, but to relay differing viewpoints so as to better advise users on their autonomous decision. The other party, to avoid framing that is factually inaccurate or hyperbolic, will vet each perspective for technical accuracy.
In detailing the impact of the legislation on business, the DCMS (2011a) highlight that consumers will need to spend a period of time learning about cookies and browser settings. This presents an ideal opportunity for the aforementioned stakeholders to present their case to users so as to open up a mutually advantageous feedback cycle of trust for both behavioral advertisers and consumers. Indeed, values and interests may coincide to offer users a truly ethical approach to gaining consent that will help build trust in the sector. If such information were available, this would go some way to overcoming claims against the industry that they seek to rob autonomy through consent by silence and one-sided persuasion. In contrast such openness tends toward trust and a transparent online environment predicated on affirmative action. These are prizes for all concerned and the implementing of proper choice would move us toward a deontological realization of consent that privileges autonomy as the basis for informed consent.

**Conclusion**

Privacy regulation helps keep powerful institutions from encroaching upon what is often phrased and pictured in terms of personal space. With regard to pre-digital media industries, these debates mostly had to do with limiting the press so as to ensure autonomy and control over our own lives. In a digital setting, discussion has moved to the ways in which we might manage informational boundaries. As data-mining processes externalize our internal preferences, the personal is once again political and it is prudent to understand the legal scenario in relation to consent that facilitates this.

In this assessment of consent and what it means when consent has been provided upfront ‘with clear and comprehensive information’, as stated in the redraft of Article 5(3) of the new e-Privacy Directive (2002/58/EC), it has been useful to take lessons from health where prior informed consent is crucial in establishing what treatment may be given. Health is also useful in highlighting the absurdity of consent as that which can be granted part-way through an operation, whether this is a medical, psychological or data-mining procedure. An examination of consent and moral philosophy has also helped clarify the meaning of consent in relation to privacy and positive values of autonomy for ourselves and others. We should guard against negative conceptions of consent framed in terms of the proverbial straw man of something being hidden, or the positioning of consent as a hindrance. If the UK seeks to maintain its light-touch policy with regard to data-gathering it is clear that it does not adhere to either common sense or philosophical conceptions of consent. If informed consent is not obtained, a line is crossed, privacy has been breached and an act of force has occurred. To mitigate this scenario this paper recommends that the best ethical way for behavioral advertising to come into line with truly opt-in approaches to consent is to work with privacy groups and become transparent over data-processing. Such a decision requires fortitude yet grants the behavioral advertising industry an opportunity to correct itself for the long term, and to win true consent and trust – something that has been lacking since its inception.

**Funding**

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
References


Department for Culture, Media and Sport (DCMS) (2011b) Implementing the revised EU electronic communications framework: HMG response to its consultation on proposals and overall approach including its consultation on specific issues. Available at: www.culture.gov.uk/images/publications/Implementing_revised_EU_ElectronicCommunicationsFramework_IA.pdf.


Information Commissioner’s Office (ICO) (2011a) Changes to the rules on using cookies and similar technologies for storing information. Available at: www.ico.gov.uk/%7E/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf.


**Author biography**

**Andrew McStay** is a Lecturer at Bangor University, and the author of *Digital Advertising* (Palgrave Macmillan, 2009) and *The Mood of Information: A Critique of Online Behavioural Advertising* (Continuum, 2011). Forthcoming books include *Creativity and Advertising: Sensation, Will and Indeterminacy* (Routledge, 2013) and *Deconstructing Privacy* (Peter Lang, 2014).