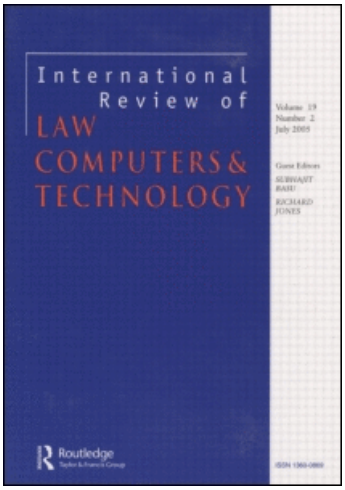

International Review of Law, Computers & Technology
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713427052

Collaborative consent: Harnessing the strengths of the Internet for consent in the online environment

Paul Bernal

Online publication date: 29 October 2010

To cite this Article Bernal, Paul(2010) 'Collaborative consent: Harnessing the strengths of the Internet for consent in the online environment', International Review of Law, Computers & Technology, 24: 3, 287 — 297
To link to this Article: DOI: 10.1080/13600869.2010.522335
URL: http://dx.doi.org/10.1080/13600869.2010.522335

International Review of Law, Computers & Technology
Vol. 24, No. 3, November 2010, 287–297

Collaborative consent: Harnessing the strengths of the Internet for consent in the online environment

Paul Bernal*

London, UK

Consent in the online environment is a crucial issue at this stage of the development of the Internet, and at the same time, in practice it is generally dealt with only on a superficial level. However, while the Internet offers significant challenges in terms of consent, it also provides unparalleled opportunities, which, if grasped, could enable a new level of consent, particularly where consent is required for services such as behavioural advertising systems. Through an examination of the failure of Phorm, the paper introduces a new concept, 'collaborative consent', treating consent not as a discrete, one-off decision but as a collaborative and communicative process, an ongoing relationship between the individual and the enterprise. The Internet provides a medium for immediate and interactive communication that could allow information to be given and choices to be made in real time – a first step to real, informed consent in the online world.

Keywords: consent; Internet; behavioural advertising

Introduction

The current form of the Internet, and in particular the World Wide Web, is one in which the gathering of data from those who surf has become a key part of the economic model. In effect, a symbiosis has developed between businesses gathering data and those from whom the data is gathered; with the data gatherers building business models reliant on this data and the users becoming dependent on access to free services provided by those data gatherers, such as search engines, email, social networking platforms and media provision.[1] In this new symbiotic web, an issue that was already of significance has become even more important: the issue of consent. As the scale, scope and nature of the data gathered from individuals is growing, it has become more important that those from whom the data is gathered give their consent, not just to the initial gathering of the data but to the many ways in which it is used. What is more, pressure has built upon data-gatherers to avoid having to ask for that consent in a way that might mean that their subject could or would refuse – for if they do refuse, the business models become less effective, less profitable, or even unsustainable.

Behavioural advertising epitomises some of these trends – it depends directly on gathering data on those browsing the web, and to a great extent rides roughshod over the whole idea of consent, treating it superficially at best, and often effectively ignoring it or attempting to sidestep it entirely. While this is understandable from a business perspective, it has

*Email: p.a.bernal@lse.ac.uk

ISSN 1360-0869 print/ISSN 1364-6885 online

DOI: 10.1080/13600869.2010.522335
http://www.informaworld.com

also been one of the factors in giving behavioural advertising a somewhat unsavoury reputation. Phorm is a prime example – for though it had an interesting business idea, innovative technology, support from the UK government and some powerful business allies it ultimately seems to have failed. Its failure to address the issue of consent was one of the key reasons behind its failure.

Was this inevitable? Is it even possible to deal with the issue of consent on the Internet in anything more than a superficial level? This paper will suggest that it is – and what is more, that while the Internet offers some significant challenges in terms of consent, it also provides hitherto unparalleled opportunities. If these opportunities are grasped, they could enable a new level of consent, one that while most directly applicable to behavioural advertising could also have implications for some of the primary services on the current, symbiotic Internet, such as email and search engines.

Collaborative consent

A new concept that begins the process of addressing this will be introduced in this paper: that of 'collaborative consent'. Collaborative consent has two key aspects. First, it treats consent not as a discrete, one-off decision but as a process, and second it looks at consent as a two-way agreement – so that the consenter is allowed and enabled to see what they have consented to; to monitor, modify or withdraw that consent in real time, and where the enterprise seeking the consent must communicate and collaborate with the consenter not just at the start of the process but throughout. Collaborative consent requires a two-way process, a form of dialogue between the enterprise and the individual. The Internet provides the kind of medium for immediate and interactive communication that allows such a process to be possible. This kind of consent could be the most appropriate and effective if the symbiotic relationship between data gatherers and data subjects is to be both benign and consensual.

Behavioural targeting and Phorm

Behavioural targeting refers to systems that collect data on web-browsing behaviour – data which might be searches made, sites visited, or more detailed clickstream data such as the time of browsing and so forth – usually in order to select which advertisements to display. Behavioural targeting in one form or other is already common on the Net – among others it is already used by Google, Yahoo! and Microsoft as well as by specialist advertising and marketing companies. The system that Phorm developed, Webwise, took behavioural targeting to a new level, gathering data not just from a small selection of sites and services, as Google and others do, but from all sites and services except those that specifically and actively opt out of the system.

Achieving this depth of monitoring involved two key things: some inventive technology and close working relationships with cooperative Internet Service Providers (ISPs). A full technical analysis of the technology is beyond the scope of this paper – though detailed work has been done on the subject, particularly by Richard Clayton of the University of Cambridge. As Clayton put it:

> The basic concept behind the Phorm architecture is that they wish to take a copy of the traffic that passes between an end-user and a website. This enables their systems to inspect what requests were made to the website and to determine what content came back from that website. An understanding of the types of websites visited is used to target adverts at particular users.[2]

Nicholas Bohm, of the Foundation for Information Policy Research, in his detailed legal analysis of Phorm,[3] suggested that the deployment by an ISP of the Phorm architecture would involve four different forms of illegality, for which the ISP would be primarily liable and for which Phorm would be liable as an inciter, concerning breaches of the Regulation of Investigatory Powers Act (RIPA) 2000, the Fraud Act 2006 and the Data Protection Act 1998, as well as potentially giving the owners of websites spidered by Phorm actions for false implication, defamation, passing off or trade mark infringement.

The strength of these legal arguments has not yet been tested in court, but some of them could, to a great extent, be addressed through a better approach to consent. The Regulation of Investigatory Powers issue was based on the fact that for an interception of communications to be legal without specific legal authorisation, both sides would have to agree to the interception. If the user had properly consented to Phorm's action that side at least of the authority would have been clear. The data protection issue could have been immediately addressed with proper consent. The other two issues, concerning fraud and potential civil actions by website owners, could also have been addressed through proper consent – though in this case the consent would have to have come from the owners and operators of websites, and that is a somewhat different issue, which though of great importance is not within the scope of this paper.

The fall of Phorm

Hackers, digital rights and privacy groups reacted strongly from the moment the proposed service became known, not least because of the apparent absence of concern for either people's consent or their privacy. The Open Rights Group, among the most respected of these groups, started a 'Stop Phorm' campaign, while Professor Ross Anderson, quoted in the Evening Standard, said 'The message has to be this: if you care about your privacy, do not use BT, Virgin or Talk-Talk as your internet provider'. Tim Berners-Lee told the BBC that he would change his ISP if it introduced a system like Webwise.

One of the most contentious issues was the discovery that in 2006 and 2007, prior to the existence of Phorm's Webwise becoming public, BT had carried out 'secret' trials of the system, involving tens of thousands of end-users. These trials were carried out without the consent of the end users, and when their existence became public, through a report leaked onto the Internet, there was not just an outcry from privacy groups but legal investigation. The City of London Police met with BT representatives to informally question them about the trials and though nothing followed immediately, in February 2010 it was reported in *The Register* that the Crown Prosecution Service was considering a criminal prosecution.

Consent once again was the key – and an apparent sense that users' views and opinions were neither important nor respected. Phorm's defence to the attacks consisted mostly of attempting, with some success, to get the UK government on their side, to keep their powerful business allies (particularly the three ISPs: BT, Virgin Media, and Talk Talk) onside, as well as suggesting that they were actually 'privacy friendly', since their records were linked to a randomly generated 'user identity number' (UID) rather than to people's names or Internet protocol (IP) addresses. This last point remains legally contentious, but in some ways misses the point. As far as the public were concerned, the technical details did not matter as much as the perception that they were under surveillance and without their consent – something demonstrated very graphically by the secret trials.

Late in the day, Phorm made it clear that they would operate an 'opt-in' system and would ensure that consent was gained, but for Phorm that was both too little and too late. Too late, because it appeared to be grudgingly accepted that consent was important

and too little because even when consent as a concept was accepted, the nature of that consent was unclear and as discussed above, consent on the Internet, even when gained, is not as meaningful as it should be – as was graphically demonstrated by the April Fools' joke played by Gamestation in which they changed their terms and conditions so that all of the 7500 people who bought from Gamestation online on 1 April 2010 effectively consented to the sale of their immortal souls.[4]

Phorm's ultimate failure came about for a number of connected reasons. First of all, in the face of the public outcry a number of crucial websites refused to let it scan them and the business allies that it had gained abandoned it, depriving the business model of its strength. As well as that, it faced potential legal action from Europe and investigation from the UK Office of Fair Trading (OFT) and the All Party Parliamentary Communications Group (apComms).[5] However, that failure might have been avoided if it had grasped the nettle of consent earlier and more positively, and understood that for businesses like this to succeed, they need to take the public with them. Not only does consent need to be gained, but that consent needs to be meaningful and understood by the public.

The lessons to learn from Phorm

The Phorm saga illustrates many of the key drives of the current state of the commercial Internet – the desire to target, the purposes of the targeting, the drive to accumulate and use as much data as possible, the tendency for alliances to build, the sharing of data, the wish to find a way to use data that is being gathered and the difficulties surrounding consent. It is important to understand that though Phorm is perhaps the most extreme to data, it is not an exception, but more of a representative of other cases. Facebook's 'Beacon' advertising system through which it shared data with other commercial websites to allow cross-website targeted advertising, demonstrates many of the same kinds of things, including a lack of transparency and an initial 'opt-out' consent system, and ultimately produced the same sort of results. Facebook was eventually forced to abandon the system completely, after settling a class-action law suit that had been brought in California accusing not only Facebook but a number of its allied retailers of breaching various US wiretapping and privacy laws.[6]

As noted above, there is another way of looking at the reasons that Phorm, and Facebook's Beacon, ultimately failed – by looking at the symbiosis that exists on the web. Symbiosis succeeds when both sides of the symbiotic relationship benefit. Google's model, which epitomises this symbiosis, offer something new or improved in return for information or monitoring – useful services such as search, email or YouTube. That is true even for their more apparently intrusive services like Google StreetView. The users get some kind of benefit in return for the intrusion or the gathering of personal data – so the symbiosis is in balance. With Phorm (and Beacon) the opposite is the case – only Phorm and its advertising partners stand to benefit. Phorm does not improve the services, or offer anything new to the user, but just uses existing services and acts in a way that could even be described as parasitic. Phorm takes, but gives little in return – and in a world in which the value of data is becoming increasingly understood, not just by businesses but by individuals, this, in the end, cannot work and hence Phorm failed. It failed in a painful way for almost all concerned, and particularly for Phorm itself and the UK government. That pain could have been reduced, or even avoided, if the situation had been better understood. What is more, if the issue of consent had been grasped, the nature of the imbalance in the relationship would have been revealed – for if people are to consent to something, they need to be convinced that there is some benefit to them.

Consent

This makes it crucial that the issue of consent is understood better and engaged with directly. At present it is an issue that is often sidestepped, or treated in such way as to make it mere legal form rather than having any real connection with what would be understood in any 'real world' sense as 'consent'. The Data Protection Directive talks about 'express, informed consent' – but what do we mean by 'express' and 'informed'? On the Internet, the kind of consent generally gained is by a user scrolling down a long page of writing that they do not read (and might not understand even if they did read) and then clicking 'OK' at the end to confirm that they have 'read and understood' the terms and conditions. The information thus presented (but rarely read) is deemed to make the consent 'informed', while the clicking of OK is deemed to make it 'express'. This 'click–wrap consent' has been generally found to be legally acceptable, though the key cases have mostly been brought in the United States[7] – but in a more real or ethical sense it is close to meaningless. Lord Denning, in *Thornton* v. *Shoe Lane Parking*, referring back to a number of earlier cases,[8] suggested that 'no customer in a thousand' ever reads the terms and conditions put in small print on a ticket, something that might be equally said about click–wrap contracts – as the Gamestation April Fools' joke referred to above revealed dramatically.

The kind of 'browse–wrap' consent used by Google and others is less legally compelling. As the Article 29 Working Party has suggested, where search engines are concerned, ordinary, anonymous users cannot be considered to have given consent and the 'de facto contractual relationship' when using a search engine in its usual form 'does not meet the strict limitation of necessity as required in the Directive'.[9] Further cases in Britain and Europe, such as *Thornton* v. *Shoe Lane Parking*, and the Italian case of *Playstation* (Tribunal of Bolzano, 31 December 2003), follow a related logic, suggesting that license conditions added after the purchase of goods or services are unenforceable – it might be considered that the kinds of conditions set by the Google, which are accessible only if a user follows a series of links from the Google home page, would be similarly unenforceable.

Many businesses operating on the Internet stretch the consent issue even further, setting their terms and conditions so that by 'signing in' to one service, a user consents to having their data gathered and aggregated for other services provided by the same company. If a user signs in to GoogleMail, for example, and then subsequently uses any of the other Google services (from Google Search to Google Maps to YouTube, etc.), then data is gathered about what is searched for or any places examined in Google Maps, and aggregated with the data record of the individual signed in to GoogleMail. As Google puts it in its privacy policy:

> We may combine the information that you submit under your account with information from other Google services or third parties, in order to provide you with a better experience and to improve the quality of our services. For certain services, we may give you the opportunity to opt out of combining such information.[10]

Whether or not this is legal has not been tested in court, but it is at least something for which an argument can be made. Google, however, do not define precisely which services it is talking about – and not all 'Google services' are labelled with the Google name, YouTube being the most obvious example. If a user is signed in to GoogleMail, does that mean that they have consented to having their YouTube activities monitored and aggregated with their GoogleMail data? YouTube has separate accounts that can be individually

signed in, but will data still be aggregated? A further significant question is whether people understand the linkages between the different services, even if they all bear the same labels – are they aware that by signing in to GoogleMail they are giving Google the legal green light to gather data from all of their services? It does not seem very likely, except for the most 'savvy' of surfers. What is true of Google is equally true of the other big Internet companies such as Yahoo and Microsoft, all of whom have a raft of different services with the capability to monitor and gather different kinds of information if consent has been given through signing in to just one of their services.

The main issue, therefore, is not what kind of consent is currently legal, but the more fundamental issues, and how the law can be used to make sure that legal consent more closely resembles 'real' consent, in the sense that it relates to having made an informed, autonomous decision.

Assumed consent – and opt-in/opt out

The question of when consent is required is also both a legal question and an ethical one. From a legal perspective, the determining factor is generally whether assuming consent is 'reasonable'. In the RIPA (Section 3(1)) for example, as shown through Phorm, interception of communications could be lawful if there are 'reasonable grounds' to assume the communicators' consent. The question, therefore, becomes what is 'reasonable'. At the very least, it is clearly unreasonable to assume that someone will consent to things that most members of a society reject. Where there is doubt, further questions must be asked and further information sought before consent may be assumed – and while doubt still exists consent cannot be assumed. Taking this a step further, it can be argued that if it is 'normal' in a society for something to be acceptable, then using an opt-out consent system *might* be acceptable, but if it is normal in society for something to be unacceptable, then an 'opt-in' system is crucial. As before, where there is any doubt about whether something is acceptable or unacceptable, the rights of the individual should get the benefit of the doubt, and only an 'opt-in' system should be possible.

Behavioural advertisers appear to have a very different understanding of the underlying level of consent to their systems. The behavioural targeting systems of the main players in the Internet world, Google, Yahoo! and Microsoft, all work on an opt-out basis. When Phorm first mooted their system, they left the question of opt-in/opt-out up to the ISPs, seemingly not considering it that important a question and leaving the impression to many that they thought opt-out was probably the most likely solution. The actions of all of them suggest that they believe that, in general, behavioural tracking is not just acceptable, but in fact would be supported by users – while the views of privacy advocates, supported by the first detailed academic survey of behavioural advertising, in a 2009 report by the University of Pennsylvania, suggest the opposite.[11] Indeed, that survey makes it clear that American society as a whole does not find behavioural tracking and the advertising associated with it, to be generally acceptable. The survey covers attitudes in America, but in the absence of similarly convincing studies of attitudes in Europe or the UK, at the very least the opposite – that society accepts and supports behavioural tracking – cannot be assumed. The logical consequence is that opt-in rather than opt-out systems are currently a necessity.

Google's Global Privacy Counsel, Peter Fleischer, speaking at the Computers, Privacy and Data Protection Conference in Brussels in January 2010, suggested that the question of 'opt-out, opt-in' is a bit of a red herring, for two reasons: first, because even opting in is often not very meaningful, as people just scroll and click, without understanding – once

again recalling Lord Denning's remarks in *Thornton* v. *Shoe Lane Parking*; second, because it cannot be expected for one company (in his case Google) to take the opt-in route unilaterally, as it would be effectively shooting itself in the foot. The second objection would be by-passed by a legal requirement for opt-in rather than opt-out. The first objection is a much more important one – but the consequence of it should surely not be that the idea of opt-in should be abandoned, but that a way needs to be found for opting-in (and indeed all forms of consent) to become more meaningful.

Looking at it from the other direction, when can consent from websites to being scanned by businesses like Phorm be assumed? In assuming that its analysis of websites was acceptable, Phorm made strong assumptions about the public nature of the Internet. Essentially, Phorm was assuming that by allowing their websites to be searched by search engines like Google, website owners are giving anyone freedom to examine, analyse and potentially make profits from those websites. By assuming that no specific consent would be requited for this, Phorm are assuming that society – in this case what might be described as 'web society', including both individual web-surfers and those who provide websites – have consented to this on an overall level, and hence do not need to 'opt in' to their system. Has 'web society' done this? It is a big assumption to make and one not currently supported by convincing evidence. If behavioural trackers wish to make their services opt-out rather than opt-in, then they need to provide convincing evidence that this is what society in general supports.

The first step towards getting this kind of acceptance of behavioural tracking and other, similar monitoring or tracking services, could be to promote a better understanding of the positive aspects of the symbiotic relationship of the current state of the web. That, however, would place a duty on the commercial enterprises to be honest about how and why they gather data. At present they appear to wish to short-cut the process, to assume consent before those they are asking to consent have even begun to understand what they are consenting to – perhaps for fear that if the 'consenters' do understand what is going on, they will withdraw their consent, as evidence from cases like Phorm and Beacon, and surveys like that reported in the 2009 University of Pennsylvania study suggest they might.

Informed consent

One of the strongest principles of the Data Protection Directive is the requirement for informed consent. That raises an immediate question – what does it mean for consent to be 'informed'? There are two very different ways to look at it – does 'informed' just mean that information has to be given, or does it mean that an 'informed decision' needs to be enabled, a decision where the information has not only been given but has been understood, and that understanding has been confirmed. The former, where information is given, is what generally happens on the Internet – the information that users scroll down without reading before clicking 'OK' can be said to have been given, but it is rarely read, let alone understood – once more recalling Lord Denning's 'no customer in a thousand'. The latter, where information is not only given but understood, and a genuinely informed decision is enabled, is what anyone interested in autonomy would demand.

How can this kind of an 'informed' decision be enabled? In the field of medical law the concept of informed consent has been investigated and discussed in depth. Harvey Teff introduced a concept he called 'collaborative autonomy' to find a way through the maze of ethical and medical problems surrounding the need for and meaning of 'informed consent'. Teff suggests a process of communication, a dialogue, through which more complex issues are discussed until they are understood, and as the situation develops and

the patient's understanding and views develop, the decision as to whether to continue with treatment or change direction can be made in a manner that is both better informed and more flexible. As he puts it:

> What many patients seek is sufficient understanding to reach an 'informed' decision in the fuller sense of the term; this can seldom be achieved without the kind of dialogue, and the kind of relationship, to which the collaborative model of medical practice alone aspires.[12]

Though the issues involved in medical consent are somewhat different to those on the Internet, there are many similarities and a similarly collaborative model is possible. The idea that consent should be a dialogue, a process rather than a one-off decision based on fixed, provided information, is something of particular relevance in cases like Phorm and can be taken a step further – for what is being consented to is a continuing process rather than a single discrete event and that places particular demands on consent. Furthermore, this does not just apply to systems like Phorm, for though search engines, for example, may appear to work as series of discrete events – individual searches producing individual results – they are better looked at as a network of linked events. The search engine provider not only records what a user searches for and the results they get, but how the user follows through those results, both in terms of links clicked but also in terms of what the user searches for next and so forth, building up a constantly developing and evolving profile. Is this something that can be adequately covered by individual, discrete acts of consent? Consenting for the individual operation might be something very different from consent to the whole process, to the aggregation and profiling, to the analysis and all that follows. What is true for search engines is also true for many of the most popular systems and services in the current form of the Net – social networking platforms, email services, blog services and so forth. They are not the discrete, individual, often trivial events so much as longer term, continuous processes.

How can this be addressed? One part of the answer may lie in the nature of the Internet itself. The Internet is a communications medium and one that lends itself ideally to communicative processes – and a medium in which collaboration is becoming one of the key ways of working, particularly with the rise of Web 2.0. Wikis are a prime example of both collaboration and communication – while the essence of social networking is sharing, blogs function at their best with comments and conversations attached to them, and so forth. When the symbiotic nature of the current commercial Internet is considered, that suggestion becomes even more emphatic. For a beneficial symbiosis both sides must benefit, and that means that what is required is active collaboration between the users and the enterprises gathering the data – the kind of symbiotic active regulatory matrix described in Murray's theory of Symbiotic Regulation.[13]

What is more, the Internet is an 'informative' system – an unparalleled system for provision, communication and verification of information. That ability to inform should be harnessed for the purposes of 'informed' consent. Further, the Internet is an interactive medium, and a 'real-time' medium – so consent has the potential to become an interactive process, working in real-time. When these different aspects are combined, the Internet can allow a very different form of consent.

Collaborative consent

The unparalleled communicative, collaborative, informative and real-time interactive opportunities presented by the Internet can be harnessed to produce a different kind of

consent – a form of consent that allows informed decisions, and a real opportunity for those decisions to be expressed. Using the communicative potential of the Internet can allow consent to become much more of a collaboration between those gathering data or monitoring users and the users themselves – and one that operates interactively, in real time, just as the Internet itself is used interactively, in real time, again, echoing the dynamic model in Murray's theory of symbiotic regulation.

The starting point is to ensure that contracts, Terms and Conditions, End User Licence Agreements and so forth are written in plain, understandable language. Agreed and standardised terms for certain forms of activity should be used, and compliance with agreed minimum standards as to what can and cannot be consented to required – it would not just be the selling of a user's soul in perpetuity, as suggested jokily by Gamestation, that would be impossible. Technical language like Deep Packet Inspection must be described in terms that explain their impact in a way that ordinary users might be able to understand. These contracts would be designed as much to inform the user – to communicate – as they would be to satisfy legal obligations.

The work of the creators of Copyleft, and the Creative Commons movement with their three-part license – the machine readable code, the legal code and essentially the human readable code – give us some clues as to how this kind of thing might work. At a practical level, the code of practice for Privacy Notices issued by the Information Commissioner's Office (ICO) could also provide a useful starting point. Both the privacy notices themselves and the code of practice concerning them are intended to be communicative, and begin the process of using the communications opportunities of the Internet in a positive way. As the ICO puts it:

> It's a lot easier to actively communicate a privacy notice in an online context than in a 'bricks and mortar one. You should make full use of the technology available to you to promote transparency and fairness.[14]

Collaborative consent would take this a step further, using the online context not just to communicate such things as privacy notices, but to include the whole consent process. The provider of a service would engage in a direct dialogue with the user, telling that user all the relevant information as it happens, alerting the user to important changes as they happen, and needing to get direct responses before taking any action. Those kinds of changes could be when new services come online – for example, if a user was signed in to one service provided by a provider and visited another service provided by the same provider, they would be alerted to the fact that this service was now gathering data and given the option to 'turn off' that gathering process.

The dialogue would be supported by further, back-up information – in particular, information about what data is being gathered (and has been gathered) and how it is being used. It is important to remember that this whole process should be a real-time process, and a continuous one – and that consent, once given, should not be considered to apply forever without the user being aware of what is happening. When data is being gathered, the data subject should be being told at all times – the precise method of the alert would depend on the nature of the service. This kind of a system would allow options to be provided wherever possible – so that consent is not a simple 'yes or no' to everything, but that a user can choose a level of consent and a corresponding level of privacy, depending on their personal views, opinion of the data gatherer and even the nature of their surfing at that particular time.

Google has already begun providing some of this kind of information to those users perspicacious enough to search for it; their *dashboard* system allows Google account holders to see what data has been gathered about them from which Google services, while their *Google Ads Preferences* allow users to see some of how Google has used this data in terms of what 'interest categories' Google has placed them in for advertising purposes.[15] Google Ads Preferences allows users to modify their profiles, enable or disable the receipt of targeted advertising, decide whether or how their data might be shared and so forth. If Google can do this, why not other data gatherers? If Google can make the information available indirectly, through a set of links via their privacy centre or their advertising system, why should they not make it available immediately and directly, and in a user-friendly and interactive way?

Once again, Lord Denning in *Thornton* provides some clues to the way forward, when he suggested that in order to give sufficient notice to particularly important and contentious points in the terms and conditions. They would 'need to be printed in red ink with a red hand pointing to it – or something similarly startling'. While Lord Denning's remarks were not really intended as a practical suggestion, on the Internet they could become reality – indeed, the red hand could be illustrated, animated and accompanied by flashing lights and wailing sirens.

The key elements of collaborative consent should be seen as rights: rights to be informed, rights to be consulted, rights to withdraw consent, rights to question and so forth. The principal features of this kind of an approach – most directly that it should provide a regular reminder that monitoring is taking place and give the user the option to withdraw or modify consent – provide a strong step towards supporting the continuation and development of the positive aspects of the symbiotic nature of the current web. If those who are monitoring and targeting people require continued consent from those being monitored and targeted, then they will need to communicate the benefits that those being monitored and targeted are getting. In order to communicate that benefit, they first need to ensure that a benefit really exists, not just in the minds of the providers, but one that the user can understand and appreciate – and hence that the symbiosis is a beneficial rather than parasitical one. That, viewed from this perspective, was the problem with Phorm's Webwise.

A first step

Behavioural tracking is one of the Internet technologies of most interest to those concerned with privacy and autonomy, but it is only one example of what might be possible. While it is not possible to fully anticipate technological developments, it is likely that consent will remain a key issue as the Internet develops. It is important that it is not an issue that is dropped because it is 'difficult' to produce meaningful consent, but is engaged with directly and ways found to address it. Making consent a collaborative process, one that puts demands on those gathering data to both explain and ensure that there are benefits from the data gathering for those about whom the data is being gathered, could be a useful first step.

Acknowledgements

This paper is based on research for my doctorate funded by the Arts and Humanities Research Council.

Notes

1. This theory is described in more detail in P. Bernal, 'Web 2.5: The Symbiotic Web', *International Review of Law, Computers & Technology* 24 (2010): 25–37.
2. First of all in R. Clayton, 'The Phorm "Webwise" System', (2008). http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf (accessed 8 May 2010), and then continuing analsyses in Clayton's blog on http://www.lightbluetouchpaper.org/ (accessed 8 May 2010).
3. N. Bohm, 'The Phorm "Webwise" System – a Legal Analysis', Foundation for Information Policy Reseach, Sandy, Bedordshire, UK, 2008.
4. See http://www.out-law.com/page-10929 (accessed 8 May 2010). The new terms and conditions included: 'By placing an order via this website on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant us a non transferable option to claim, for now and for ever more, your immortal soul'.
5. For the European Action see http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&guiLanguage=en (accessed 8 May 2010), the OFT investigation see http://www.guardian.co.uk/media/2009/aug/20/internet-targeted-advertising-oft-investigation (accessed 8 May 2010), and the apComms report see http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf (accessed 8 May 2010).
6. See for example http://www.concurringopinions.com/archives/2009/09/facebook-settles-beacon-lawsuit.html (accessed 8 May 2010).
7. For example in *ProCD* v. *Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) and *Specht* v. *Netscape Communications Corp*., 150 F.Supp.2d 585 (S.D.N.Y. 2001).
8. *Thornton* v. *Shoe Lane Parking Ltd* [1971] 2 QB 163, referring to *Parker* v. *South Eastern Railway Co*. [1877] 2 CP 416, *McCutcheon* v. *David McBrayne Ltd* [1964] 1 W.L.R. 125, *Watkins* v. *Rymill* [1833] 10 QB 178,188 and *Thompson* v. *London, Midland and Scottish Railway Co*. [1930] 1 KB 41, 47.
9. See Working Party on the protection of individuals with regard to the processing of personal data ('the Article 29 Data Protection Working Party'), Brussels, Opinion 148, p. 17.
10. http://www.google.co.uk/privacypolicy.html (accessed 8 May 2010).
11. J. Turow, J. King, C.J. Hoofnagle, A. Bleakley and M. Hennessy, 'Americans Reject Tailored Advertising'. Annenberg: University of Pennsylvania, 2009.
12. H. Teff, *Reasonable Care: Legal Perspectives on the Doctor–Patient Relationship* (Oxford: Oxford University Press, 1994), 198.
13. A.D. Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Abingdon, UK: Routledge, 2006), particularly Ch. 8.
14. The Information Commissioner's Office (ICO) Privacy Notices Code of Practice, p. 9, downloadable from http://www.ico.gov.uk/for_organisations/topic_specific_guides/privacy_notices.aspx (accessed 8 May 2010).
15. The Google dashboard is accessed through the Google Privacy Center (http://www.google.com/privacy.html, accessed 8 May 2010). For a brief discussion of how it works, see http://googlesystem.blogspot.com/2009/11/google-dashboard.html (accessed 8 May 2010). For Google Ads Preferences see http://www.google.com/ads/preferences (accessed 8 May 2010).