

write news

Clear, pragmatic and commercial legal advice on
all aspects of IT

-
- 01/02 Will your cookies crumble under changes to the Privacy and
Electronic Communications Regulations (2003)?
03 Geo-Location Services: Is this a Smart Move?
04 IT/IP Round Up



Will your cookies crumble?

Will your cookies crumble under changes to the Privacy and Electronic Communications Regulations 2003 (“the Regulations”)?

As a result of European law, the Regulations came into force in the UK on 26 May 2011. They alter how cookies can be used within websites. Previously, website owners/operators simply had to tell website users how they used cookies and how users could “opt out” from having cookies installed on their computers. However, Regulation 6 now prevents a person from storing or gaining access to information stored in terminal equipment of a subscriber or user unless the subscriber or user:

- (a) is provided with clear and comprehensive information about the purpose of the storage of or access to that information; and
- (b) has given his or her consent.

This means that users now have to “opt in” and consent to the installation/use of cookies. Regulation 6 (4) sets out two circumstances where consent will not be required. These are: where the technical storage of, or access to, information:

- (a) is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
- (b) where such storage or access is **strictly necessary** for the provision of an information service requested by the subscriber or user.

The Information Commissioner’s Office (the “ICO”) has been tasked with implementing and enforcing the new rules. It has the power to fine any person found in breach of the Regulations up to £500,000 (depending upon the nature of the breach). Therefore it is imperative that all

website owners/operators undertake a review of their website for compliance with the Regulations.

How can you obtain informed consent?

The most problematic area for website owners/operators is how and when to obtain informed consent. The EU Working Party is of the view that consent must be given before a cookie is installed or information stored. However the Department for Culture, Media and Sport (the “DCMS”) is of the view that such prior consent is not required and in some circumstances it may be impracticable to do so. The ICO has not helped with this uncertainty as it is silent on when consent should be obtained. Therefore it’s likely to be best practice for the time being for website operators/owners to obtain prior consent in all circumstances.

The ICO states that “the fact that an individual must “signify” their agreement means that there must be some form of active communication between the parties”. A further problem in obtaining consent is that different ways of obtaining consent to cookies may be required by a website if it uses multiple cookies for different purposes. Therefore the ICO suggests that a website audit should be undertaken to:

- 1) check what type of cookies and similar technologies are used;
- 2) investigate how intrusive the use of cookies is (the ICO states that more priority should be given to obtaining meaningful consent where the cookies are more intrusive);
- 3) decide what solution(s) are best to obtain consent.

New Regulation 6 (3A) states that: “For the purposes of paragraph (6(2)), consent may be signified by a subscriber who amends or sets controls on their internet browser which the subscriber uses or by using another application or programme to signify consent”.

Although it is hoped that browser settings will provide a solution to obtaining consent, the Government and ICO agree that current browser settings are not sophisticated enough to deal with this and the Working Party is currently working with browser developers to see if consent can be given effectively by this method. However, a viable solution along these lines may be some time off and, in the interim, alternative forms of consent will need to be considered and implemented.

The ICO has suggested the following as alternatives to browser led consent:

1. **Pop ups & similar techniques** - express consent provisions displayed in pop up tick boxes or similar techniques.
2. **Terms & conditions** - consent provisions in website terms and conditions that must be accepted when users sign up to or register with a website for the first time. However this does not mean that website owners/operator can simply amend their current website terms and conditions without taking any further action as positive steps will need to be taken to ensure users have agreed with and accept the amended terms and conditions.
3. **Settings led consent** - this would involve obtaining consent each time or at the point the user makes a choice about how they wish the website to operate for them (where such choices would involve cookies being installed). A common example of this is where the website has the option for the user's information/login details or passwords to be remembered.
4. **Feature led consent** - this would involve obtaining consent at the time a user wishes to use a particular feature on the website that requires cookies.
5. **Functional uses** - the ICO notes that although analytical cookies may not be as intrusive as other cookies, they still require consent and that prominent information about the use of such cookies should be displayed on websites. The ICO have suggested (and indeed adopted this approach on their website) displaying text in headers or footers on webpages which in turn opens up full text on how cookies are used, lists what cookies are used on the website and

allows the users to consent to the various cookies.

6. **Third party cookies** - although the ICO acknowledges that this area may cause website owners/operators the greatest difficulty, its advice is that when using third party cookies on your website, users must be made aware of what information is being collected and how such information will be used by the third party.

Although the ICO's guidance goes some way in providing practical steps that website owners/operators should take, it falls short of providing an in-depth list of workable solutions for compliance. In fact the ICO confirms that it does not intend to provide prescriptive lists on how to comply. Many website owners/operators may find themselves in an impossible situation of not being 100% certain that the methods they have deployed will be sufficient to meet the consent requirements under the new Regulations. There is some comfort in that the ICO is allowing a period of 12 months to get things in order and if the ICO receives a complaint about a particular website before May 2012, it will provide advice to the owner/operator on how they can comply. A word of warning however: the ICO may issue warnings in the interim if it is of the view that adequate preparations for compliance are not being taken and should a complaint be received after May 2012, warnings will be taken into account by the ICO for the purposes of determining whether to issue an enforcement notice. The underlying tone of the ICO's guidance notes is that inaction is not an option. It is expecting businesses to show they have considered the new requirements and are taking positive steps to comply.

If you would like assistance when amending your website to ensure compliance with the Regulations, please contact a member of our IT team.

For more information on the ICO's approach and guidance notes visit <http://www.ico.gov.uk/>

Geo-Location Services: Is this a Smart Move?

Hot on the heels of the changes to consent requirements for cookies, the Article 29 Working Party (“the Working Party”) has published its opinion on consent requirements for geo-location services on smart mobile devices.

Geo-location data is data which refers to the location of a person or an object. Many “smart devices” such as i-pads, laptops and mobile phones use a variety of techniques to capture this data and can determine the location of a person or object. This new technology has led to an influx of new services which use such data for example maps showing your proximity to places of interest, restaurants etc. Never has the phrase “Big Brother is watching you” been truer.

Providers of such services do not have a free reign on how they can use such data and if you are developing or considering implementing such systems within your business you should consider the implications of the Data Protection Act (which implements the Data Protection Directive) especially as such data may be “personal data” if it could be used to identify a living person.

The Working Party’s view is that smart devices are inextricably linked to living individuals and because geo-location services can provide details of a device’s movements, this could provide intimate details about an individual’s private life. Therefore, location data will on the whole be personal data and governed by the Data Protection Act.

The Working Party is clear that consent to the processing of data cannot be obtained by general terms and conditions; and it must be specific and for the purpose which the data is being processed. Users must be provided with clear and understandable information on such matters at the time consent is given. The Working Party goes further, suggesting that consent needs to be time specific and providers of such services should remind users (at least every year) that they are processing such data.

We shall have to wait and see if any further guidance is issued or procedures are implemented. We will keep you posted – for current reaction as it happens.



IT/IP Round Up

Data Retention Directive

The European Data Protection Supervisor (the “EDPS”) has published its opinion on the European Commission’s Evaluation Report on the Data Retention Directive (the “Directive”). The Directive, which came into force in May 2006, was intended to harmonise national legislation governing the retention of data. It requires all providers of electronic communication services to store traffic and location data of communications for use by national law enforcement agencies and was in response to the major terrorist attacks in Madrid in 2004 and London in 2006. The EDPS concluded that not only has “the Directive failed to harmonise national legislation”, it “does not meet the rights to privacy and data protection as:

- the necessity of data retention (as provided in the Directive) has not been sufficiently demonstrated;
- data retention could have been regulated in a less privacy-intrusive way; and
- the Directive lacks foreseeability”.

We shall wait with baited breath as to what extent (if any) the European Commission implements the EDPS’s opinion particularly as the EDPS suggests the repealing of the Directive as an option. To view the EDPS’s opinion in its entirety visit www.edps.europa.eu.

New Strategy for IP rights

The European Commission has published its strategy on Intellectual Property Rights in its snappily titled “A Single Market for Intellectual Property Rights” communication. In it the Commission sets out its detailed plans for the next few years to deliver a unified structure for the protection and commercial exploitation of Intellectual Property Rights. The strategy is part of the Commission’s bigger Europe 2020 strategy

and its focus is on utilising Intellectual Property Rights and initiatives to aid the EU’s economic growth.

We shall provide further updates on this as and when the various elements of the strategy are implemented or come to fruition.

Following this communication, the Commission has published the draft counterfeit-goods regulations and the Commission’s proposals for a unified EU patent.

The draft counterfeit-goods regulations set out the procedure for Customs to follow in relation to goods that are suspected of infringing Intellectual Property Rights, streamlining the procedure for destroying counterfeit or pirated goods.



IT Team - Key Contacts



Carl Newton
Managing Partner & Head of IT Law

Carl, the firm's Managing Partner, is an experienced company/commercial lawyer with considerable expertise in the IT sector. He is the head of our IT team. Carl has particular expertise in advising on acquisitions and disposals of IT companies and businesses, joint ventures and the financing, exploitation and development of IT and Internet technologies and products. He is a member of the Society for Computers and Law.

carl.newton@neilmyson.co.uk



Tim Norman
Partner

Tim is a partner and is an expert in IT and commercial litigation. He has many years of experience in dealing with disputes, arbitration and court proceedings involving complex IP and IT issues.

tim.norman@neilmyson.co.uk



Carla Murray
Solicitor

Carla is a solicitor in our Company/Commercial Department, specialising in IT, intellectual property and commercial law. She has particular expertise in advising in software licensing, e-commerce law, outsourcing, franchising and data protection matters.

carla.murray@neilmyson.co.uk



Charlotte Gilbert
Solicitor

Charlotte is a solicitor in our Employment Department dealing with all aspects of Employment Law including both contentious and non-contentious matters. Charlotte's expertise includes providing advice on HR and Employment related legal matters both to IT businesses and contractors including advice on status issues, contracts, IP rights, home and out of office working issues, post termination restrictions and employment related disputes.

charlotte.gilbert@neilmyson.co.uk

**NEIL
MYERSON
LLP**

SOLICITORS

Neil Myerson LLP
The Cottages Regent Road
Altrincham Cheshire WA14 1RX

T (0161) 941 4000
F (0161) 941 4411
DX 19865 Altrincham
E lawyers@neilmyson.co.uk
W www.neilmyson.co.uk

