From the blog

Cookies six month solve by date

With Six months to go until the Information Commissioner's (ICO) own moratorium on enforcing the revised Privacy and Electronic Communications Regulations (PECR) - "The cookie law" UK businesses are awaiting further guidance from the ICO of how the law will be enforced and the potential impact.

Following the statement that "*from May 2012 onwards the Commissioner will follow the approach to enforcement set out in his Data Protection Regulatory Action Policy*" it is hoped that a "*Half Term Report*" will soon provide greater clarity.

However as the clock ticks down towards the May 2012 deadline the ability for companies to proactively manage the situation continues to reduce.

This post is aimed at providing a quick summary of the current situation and recommends what we believe website owners should be doing as a minimum.

Look at some of our earlier posts - Waiting to see how the cookie crumbles is not enough or Do a quick Cookie Audit if you fear the Cookie monster for more background.

Quick recap?

Cookies are currently the focus of the discussion and the current target for enhanced awareness. However the real purpose of the legislation and hence any activity should really be around what data is captured, stored and how this is then used.

Cookies are one type of **Locally Shared Object** and the best way to consider them is more as a Fortune Cookie with a raffle ticket inside it rather than as a Biscuit (It's a Dinner Jacket not a Tuxedo anyway!). This concept is more practical because when you access a webpage each of the web servers serving content can set cookies onto and read the cookies they have set on your machine.

Increasingly web pages are made up of various content from a variety of content providers. When you (The Second party) access a destination website (the First Party) they may enable content to be served from other servers (Third parties) - Hence the distinction between cookie types.

Previously websites were effectively brochures and you accessed set content and cookies may have been used to store information in isolation on your machine. Nowadays websites operate supported via database functionality and cookies can provide the link between the database, your machine and ultimately you.

For example I visit a site and on the database my raffle ticket number is stored against when I visited, what I looked at, to record my preference e.g. type of colour preferred for screen resolution etc. As an anonymous visitor this may not be considered an issue but if I then provide personal information the database can store this along with my raffle ticket number. This then provides the ability to retrospectively link any previous data with my personal data.

If the cookie is treated as a Personal Unique Identification Number (PURN) the questions to address to ensure compliance with any legislation are:

- What data is stored?
- Why and where it is stored?
- What is it used for and by whom?
- Does this correspond with what the consumer (the 2nd Party) agreed to or could reasonably expect?

Solutions?

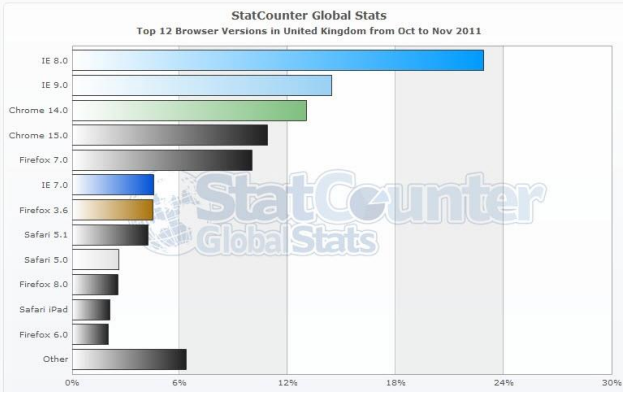
There are various initiatives attempting to respond to the cookies law that each provide different methods of attempting to comply. (I say attempting to comply as what compliance is has yet been set). These range from

1. Behavioural advertising icons

The Internet Advertising Board's European Initiative focusses through its Your Online Choices site upon information being provided after the capturing of data i.e. the ability to withdraw permission for unspecified data relating to digital activity once it has been captured, analysed and used and once you become aware of it!

2. Reliance on the main browsers manufacturers to solve the issue

As recently reported by The Register whilst plans for a Do Not Track Standard are being drawn up this focusses predominantly on 3rd party and this "Cavalry" looks very unlikely to arrive by May 2012.



Even if they did this will only address cookies (Locally stored Objects) set through web browsing (what about emails, Smartphone Apps etc ?) and only when the general population catch up with the latest release of the browsers

3. Use of pop ups – e.g. the ICO website

The ICO website site uses a pop up requesting permission to set cookies to enable tracking which does not preclude people using the site but until opted in stops analytic tracking cookies being set This could prove a solution for businesses where they have only a few simple cookies being set - The ICO is a public body and therefore does not allow third party advertising etc. and so such a solution may become very clunky for some sites

However even the ICO's approach is currently flawed as it makes no allowance for the4th Data Protection principle regarding accuracy and maintaining up to date data because it ignores individuals own capability to adjust cookies and thereby presumably permission.

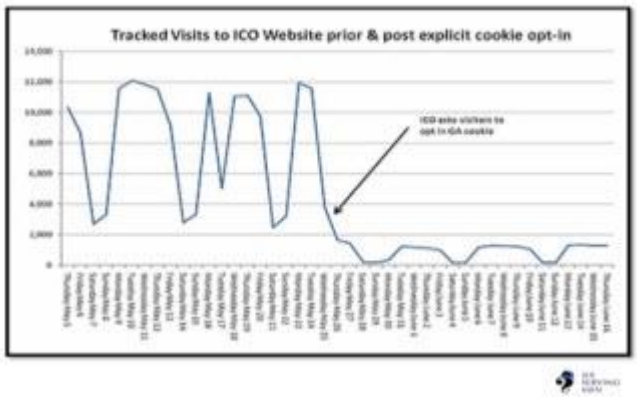
So what should you do?

Whilst any immediate legal risk was temporarily removed, in May 2011 the ICO has stated they urge all UK businesses and organisations to read their advice and start working out how they will meet the requirements of this new law. They also warn that those who choose to do nothing will

have their lack of action taken into account when they begin formal enforcement of the rules. With regard to cookies laws like all changes in legislation it provides three main areas of risks for all business owners that need to be assessed and appropriate actions taken to mitigate against them.

1. Legal risks

The immediate risk of censure from law enforcement and any associated penalty - The ICO have highlighted verbally that initial focus will be on education and specifically targeted against those who have done nothing to mange the situation.



2. Commercial risks

Business can incur costs or lose revenue by making poor decisions. The ICO's own site made an adjustment in May 2011 (to be seen to be doing something) but this meant that they lost the capability to track and understand 90% of their web traffic.

It is not clear what the actual impact was on visitor numbers or user engagement with content due to the presence of a rather unattractive opt in box. Usability and design professionals would suggest that the opt in box would have a detrimental effect rather than a positive effect

An additional commercial risk is that noncompliance or unawareness will highlight poor data protection practices and could result in data held for marketing in other areas being deemed noncompliant and therefore not usable.

3. Reputational risk

People do business with people they trust – Sony recently suffered from losing subscribers information and are more concerned with the loss of brand value as consumer trust diminishes than any fine they may receive.

Mitigating any loss of Trust is the area companies need to focus on particularly as consumers awareness is enhanced. Recent Department of Culture Media and Sport research highlights over 80% of people were unaware of the changes but once aware 70% believed it is very important they know why cookies are being set and how to delete them.

Next steps?

Until the legislation is clear companies should be adopt a Ready, Aim, Fire approach, i.e. Get Ready by understanding what cookies you are responsible for setting (1st & 3rd Party) and why you set them. This then enables you to be in a position to move when things become clearer.

If you need help with cookies or any other aspect of digital marketing for your business you can call us on **(0115) 837 2663** or email us at **help@6sm.co.uk**, we're just around the corner.