EU Cookie Law

the definitive guide

Oliver Emberton

silktide®

Version 1.0 – updated June 9th 2011

We'll update this book with new developments – the latest version is free at www.silktide.com/cookielaw

The authors have made every effort in the preparation of this document to ensure the accuracy of the information within. However, the information in this document is provided without warranty, either express or implied.

About this book

We've heard a lot of talk about the new EU Cookie Law, but little real information. So we made this book.

We've aimed to be practical and comprehensive. We cover everything from the fine print of the law to the technologies that satisfy it in detail.

When we started writing we *tried* to be neutral, but that rapidly became impossible. We don't agree with the law – at least in the way it's written now – honestly, it comes over as a technically illiterate shambles. But it is still law and we all have to deal with it.

Just remember: *don't panic.*

About the author

Oliver Emberton is the Managing Director of Silktide, a software company that helps you make sense of your websites. Oliver has been programming since he was 8, founded Silktide when he was 21, and still finds time to write books on EU cookie laws over the weekend for your entertainment.

Silktide's website testing software can tell you what cookies you're using and whether you're likely breaking the new law, among many other things. You can try it for free at www.silktide.com/sitebeam

Disclaimer

This book was not written by legal professionals, although we researched many of their opinions. This book should not be taken as legal advice.

Contents

The law in 5 minutes

If time is short read this or watch our video[1].

What is the law?

From May 2011 a new privacy law[2] came into effect across the EU. The law requires that *websites ask visitors for consent to use most web cookies*.

Nearly all websites use cookies, which are an extremely common technology for remembering anything about a visitor between webpages. Cookies are commonly used for login, remembering preferences, tracking visitors and more.

The new law is intended to help protect people's privacy. For example, if you search for "cars" in Google, they uses cookies to remember this. Later in the day, on another website, Google may target car ads at you because they remember who you are. This might not sound too scary until you think how many thousands of searches you do on Google, and how much they probably know about you as a result[3].

The vast majority of small websites don't do this of course, but they do track visitors to their website, e.g. via a tool like Google Analytics, and they use social media plugins like Facebook Like buttons. As we will see, this law appears to outlaw all of this entirely.

[1] www.silktide.com/cookielaw or search YouTube for cookie law.

[2] http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf

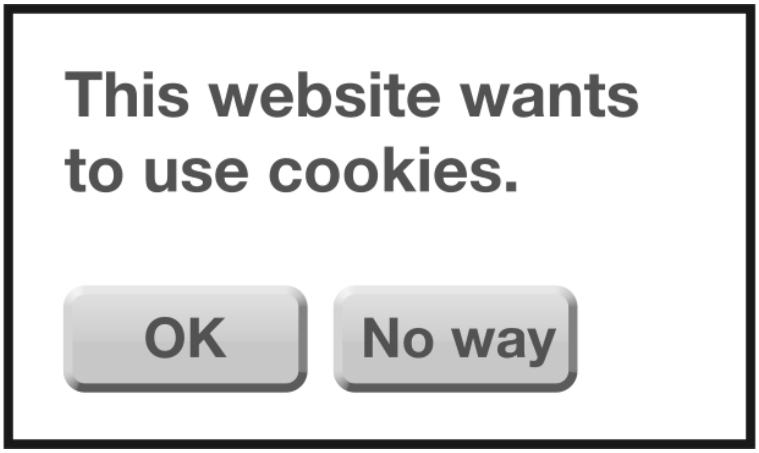
[3] It is worth pointing out that Google goes to lengths to anonymise this information, and also to exclude sensitive portions of it such as race, religion, sexual orientation, health, or sensitive financial categories. http://www.google.com/privacy/ads/#toc-faq

What does this mean for websites?

Most EU websites will need to change, or break the law.

Over 92% of websites use cookies at the moment. They'll either have to stop using cookies, or start asking for permission.

To ask for permission, a website must interrupt their visitors – say, with a popup like this:



This website wants to use cookies.

No one wants to add this to their website, and most visitors are unlikely to be happy about it either.

There are other solutions which we explore later, but they all have a negative effect on the experience of a website. Websites could stop using cookies, but generally only by losing some functionality on their site - and because cookies are so ubiquitous, this isn't easy.

Does this only affect websites hosted in the EU?

The location of your hosting is irrelevant, but the location of your organisation is not.

Your organisation must fall within the legal jurisdiction of the EU. Each member state has their own laws, which are based on the same EU directive, but may differ slightly.

For most small/medium organisations, being located in the EU will mean you must comply.

Are all cookies affected?

The vast majority are - all cookies that are not "strictly necessary for a service requested by a user".

The law allows an exception for "strictly necessary" cookies, such as those used to remember when something has been added to a shopping basket. These cookies would be *expected by the user implicitly* for the action they requested to be carried out. Another example would be login.

The majority of cookies currently in use aren't considered strictly necessary though: particularly cookies for analytics and advertising. Many cookies perform several roles.

What are cookies?

There's much more to cookies than you might realise.

What is a cookie?

A cookie is a technology for remembering information between webpages. Because of cookies, your web browser can remember you are logged in, or have visited a site before, or what your personal preferences are.

In reality, a cookie is a small text file which is stored by the user's browser. The cookie only contains data, not code, so it can't contain a virus or spyware. This doesn't mean that all cookies are harmless in intent, but they can only ever store information.

A cookie remembers information about a specific website, for example.

```
fontsize=large
```

This information is restricted to a specific domain, e.g.

```
www.silktide.com
```

The domain prevents other websites from accessing each other's cookies. However there are ways that websites can share information as we'll see.

Session cookie

A session cookie expires when the user closes their browser, and sometimes just after a certain period of time has elapsed (for example, on mobile devices, where the concept of 'closing your browser' is less relevant).

Sessions are therefore ideal to remember – for example – if a user has logged in to a website. When they close their browser they are automatically logged out. They are usually considered relatively unobtrusive from a privacy perspective.

Persistent cookie

A persistent cookie expires after a fixed date, for example after one year. They are not cleared when the user closes their browser.

A common use of a persistent cookie is the "Keep me logged in" box found beneath many login areas. For this to work, the cookie must be stored after the user closes their browser.

However persistent cookies are also used to track users in unexpected ways. For example, if you visit Google they give you a unique cookie to track you with. They can then use this cookie to recognise and link your behaviour between their many sites – they might for example know what you search for, what websites you visit etc. They can then use this information to target advertising at you on those same sites.

First party cookies

A first party cookie is restricted to the same domain as the website you are viewing. For example, if you were visiting www.silktide.com, a first party cookie would only be readable by pages inside www.silktide.com.

Third party cookies

A third party cookie is set by a domain other than the one the user is visiting. For example, if a user visits www.example-one.com, a third party cookie might be set by www.example-analytics.com. Now if the user visits www.example-two.com, this website could also use the third party cookie set by www.example-analytics.com. In effect, the user is recognised between sites.

The reality is more complex. In this example neither www.example-one.com or www.example-two.com can actually see the cookies being set, only www.example-analytics.com can. However there is nothing stopping www.example-analytics.com from collecting information in this way and sharing it with others, including the other two websites.

Third party cookies are most commonly used for tracking users by advertising networks, search engines and social media sites. For something like the Facebook Like button to work on websites other than Facebook's, third party cookies are essential. However, because they allow tracking between websites that a user may not expect, they are generally frowned upon by privacy advocates.

How browsers control cookies

All major browsers provide security controls for cookies. Generally these allow users to choose to block all cookies, to only allow specific cookies, or to block third party cookies.

The official standards for cookies (RFC 2109[4] and RFC 2965[5]) say that by default browsers should block third party cookies. However almost all browsers permit them, as long as the website setting the cookie has a P3P privacy policy installed, which is a simple system for stating what your website's privacy policy is. In reality, a P3P policy can be empty or unused, allowing third party cookies regardless.

For example, this is Facebook's P3P policy:

> *"Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p"*

Browsers permit third party cookies by default largely because failing to do so would appear to 'break' the browser in the eyes of most users.

The law doesn't just mean cookies

The law isn't actually about cookies, but because it affects them so much people have started calling it the 'Cookie Law'. It's actually about all technologies which store information in the "terminal equipment"[6] of a user, so that includes so-called Flash cookies (Locally Stored Objects), HTML5 Local Storage, Silverlight and more.

In fact, the law appears to frown even more on these alternatives to cookies, because users are even less likely to understand them, and may incorrectly assume that they can opt out of them via traditional browser controls[7]:

> *"Therefore, since flash cookies cannot be as simply deleted as other third party cookies (whether by browser setting or manually) they circumvent the user's personal browser settings and therefore also circumvent the consent issue, i.e. article 5.3 of the e-Privacy Directive becomes applicable. The same goes for other devices, such as HTML5- techniques, Java API, Silverlight or similar technique."*

For simplicity we refer to cookies throughout this book, but this meaning extends to all equivalent technologies.

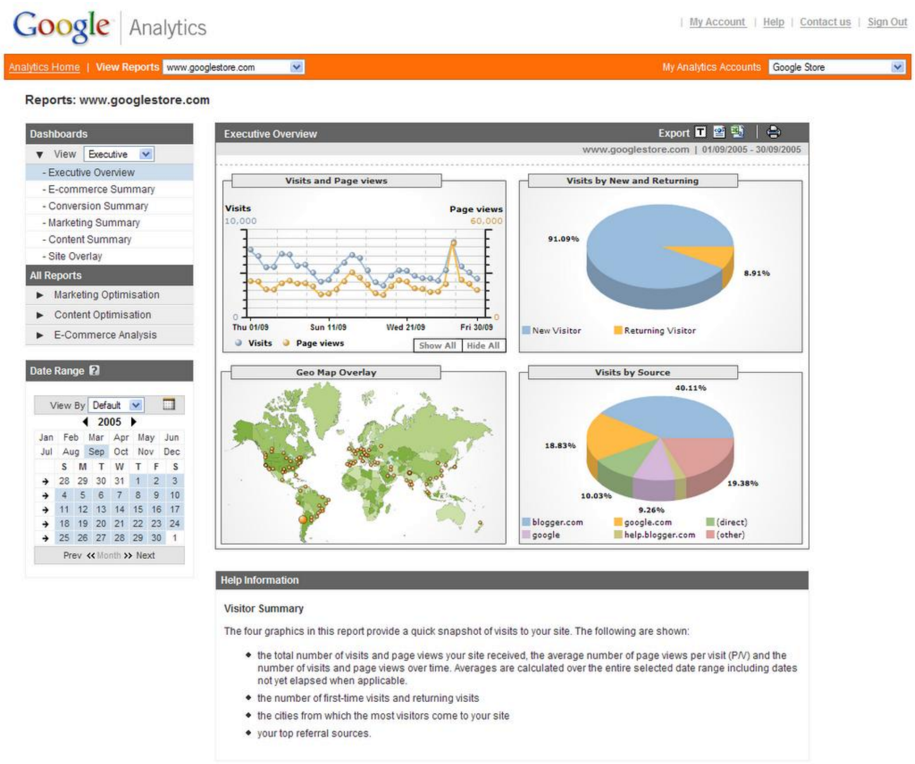
[4] http://www.ietf.org/rfc/rfc2109.txt
[5] http://www.ietf.org/rfc/rfc2965.txt
[6] For our purposes "terminal equipment" means computer or browsing device.
[7] http://admin.campaigner.nl//users/ddma/files/95907289-alexanderalvaroexplainescookies.pdf

What do we need cookies for?

We’ve broken down the most common uses of cookies and explained how the law affects them.

Analytics

Status: Prohibited in UK in current form
Inconvenience: High



View Reports: www.googlestore.com

My Analytics Accounts: Google Store

Reports: www.googlestore.com

View: Executive

View By: Default

www.googlestore.com | 01/09/2005 - 30/09/2005

Visitor Summary

The four graphics in this report provide a quick snapshot of visits to your site. The following are shown:

- the total number of visits and page views your site received, the average number of page views per visit (P/V) and the number of visits and page views over time. Averages are calculated over the entire selected date range including dates not yet elapsed when applicable.
- the number of first-time visits and returning visits
- the cities from which the most visitors come to your site
- your top referral sources.

Analytics software is used to measure the behaviour of visitors on a website, for example the number of people visiting a site, or making it from one part (say your homepage) to another (your checkout). The most famous analytics software includes Google Analytics, Omniture and WebTrends.

To do any kind of analysis of individual *viewers* – i.e. measure a series of pages, not just a single page – cookies are essential. Nearly all of the valuable analysis that analytics does is at this level: for example, determining how long people spent on a website, or working out what search terms resulted in the most valuable customers.

All of this requires using cookies for one purpose only: to track the behaviour of your visitors. The UK's regulator (the Information Commissioner's Office) says[8]:

> *"... some uses of cookies can involve creating detailed profiles of an individual's browsing activity. If you are doing this, or allowing it to happen, on your website or across a range of sites, it is clear that you are doing something that could be quite intrusive – the more privacy intrusive your activity, the more priority you will need to give to getting meaningful consent."*

It would be difficult to argue that tracking your visitors is "strictly necessary for a service requested by the user", and indeed the same UK government body now require their own website visitors opt-in to be tracked with Google Analytics.

(We dive into the meaning of "strictly necessary" in more detail in our legal FAQ, but suffice to say it is meant to be very restrictive).

So it appears the only way to use cookie based analytics in the UK is to ask your visitors for permission.

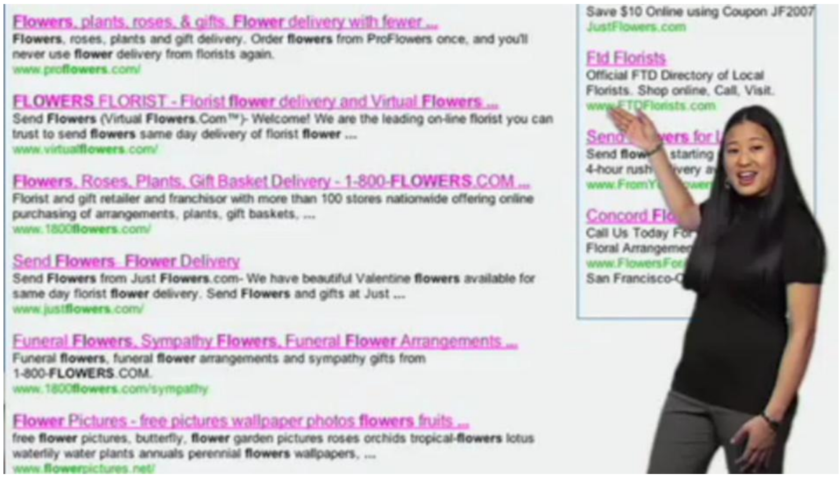
For the rest of the EU, the jury is still out, but early signs suggest that other countries will adopt conflicting approaches. This would create a muddled situation where analytics is enabled or disabled based on the country of the user.

There are some forms of cookie-less analytics as well, such as web log analysis. These appear excluded from this law but offer far less information than their cookie based alternatives. They're also impractical for many website owners to install.

[8] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

Advertising

Status: Behavioural ads prohibited
Inconvenience: Potentially devastating



Flowers, plants, roses, & gifts. Flower delivery with fewer ...
Flowers, roses, plants and gift delivery. Order flowers from ProFlowers once, and you'll never use flower delivery from florists again.
www.proflowers.com/

FLOWERS FLORIST - Florist flower delivery and Virtual Flowers ...
Send Flowers (Virtual Flowers.Com™)- Welcome! We are the leading on-line florist you can trust to send flowers same day delivery of florist flower ...
www.virtualflowers.com/

Flowers, Roses, Plants, Gift Basket Delivery - 1-800-FLOWERS.COM ...
Florist and gift retailer and franchisor with more than 100 stores nationwide offering online purchasing of arrangements, plants, gift baskets, ...
www.1800flowers.com/

Send Flowers. Flower Delivery
Send Flowers from Just Flowers.com- We have beautiful Valentine flowers available for same day florist flower delivery. Send Flowers and gifts at Just ...
www.justflowers.com/

Funeral Flowers, Sympathy Flowers, Funeral Flower Arrangements ...
Funeral flowers, funeral flower arrangements and sympathy gifts from 1-800-FLOWERS.COM.
www.1800flowers.com/sympathy

Flower Pictures - free pictures wallpaper photos flowers fruits ...
free flower pictures, butterfly, flower garden pictures roses orchids tropical-flowers lotus waterlily water plants annuals perennial flowers wallpapers, ...
www.flowerpictures.net/

Save $10 Online using Coupon JF2007
JustFlowers.com

Ftd Florists
Official FTD Directory of Local Florists. Shop online, Call, Visit.
www.FTDFlorists.com

Send
ers for U
Send flow
starting
4-hour rush
very a
www.FromY
wer

Concord Flo
Call Us Today For
Floral Arrangeme
www.FlowersFor
San Francisco-C

Advertising by itself isn't affected by the law, but nearly all web adverts are measured and targeted automatically via cookies, based on the behaviour of that user over time. The reason for this is simple: behavioural ads are vastly more effective – some studies have shown them to be twice as effective[9].

Unfortunately behavioural ads are explicitly prohibited by the EU without prior consent from the user, which is not going to easy to obtain (how do you ask "can we track you to make our advertising more effective?"). This could mean a real financial hit to anyone dependent on online ads.

In the EU's own guidance they acknowledge this problem, but say privacy is more important[10]:

> *"Behavioural advertising entails the tracking of users when they surf the Internet and the building of profiles over time, which are later used to provide them with advertising matching their interests.* ***While the Article 29 Working Party does not question the economic benefits that behavioural advertising may bring for stakeholders, it firmly believes that such practice must not be carried out at the expense of individuals' rights to privacy and data protection."***

[9] http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf
[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

> *"... advertising network providers are bound by Article 5(3) of the ePrivacy Directive pursuant to which* ***placing cookies or similar devices on users' terminal equipment or obtaining information through such devices is only allowed with the informed consent of the users****."*
>
> *EU Data Protection Working Party*

Websites that use behavioural ads will have to consider either untargeted ads, or asking their users an intrusive question. Either option will hit their revenues. Any technical solutions will have to come from the advertising network (e.g. Google AdSense), so most sites can't do much themselves yet other than drop adverts entirely.

A minor note: most online advertising is now based on Google's model of Pay Per Click, where an advertiser only pays when their advert is clicked on. To avoid this model being abused by endless repeated clicks from a handful of users, cookies are used to track the user[11]. We suspect that this use of cookies could conceivably be defended as "strictly necessary" if it doesn't impair the user's privacy, but even this is questionable.

Conversion tracking

Status: Debatable, but we're not hopeful
Inconvenience: Potentially devastating

A common use of cookies is to track conversions from a specific source. Amazon, for example, pay people who bring them customers a small slice of their profit. Many websites track whether a specific ad results in a conversion on their website.

These are popular for clear reasons and it remains unclear whether their use is permitted by the law; sadly we suspect not. In contrast to behavioural advertising, the EU *hasn't specifically stated this isn't allowed*, so we're forced to guess.

Tracking a user without their consent is clearly frowned upon, but you could argue that clicking on an advert made it "strictly necessary" that this would happen. Unfortunately while it may be necessary for the poor website owner, the law is aiming to protect the user. It could be interpreted either way – we suspect that the user wouldn't see being tracked as necessary though.

[11] This is a gross simplification: many other mechanisms are used as well as cookies. But cookies are quintessential.

If that's the case, we can't see any sane way users could be asked for permission for this. Imagine if every time you clicked on an ad you then *had to agree to be tracked in case you bought something*. You may as well force all advertisers to write their copy in Japanese.

This is one of the finest examples of why this law is so confusing.

Anti-spam filtering

Status: God only knows
Inconvenience: Minor

Most websites with a form on them attract an unholy amount of spam. A common technique for reducing this is to set a cookie in the browser using Javascript, which spam bots won't send when they submit a form. The result is less spam for website owners.

We don't see any way in which this compromises the privacy of web users, so we believe it would be protected as a necessary technology, or at least not frowned upon heavily as an invasive one.

Load balancing

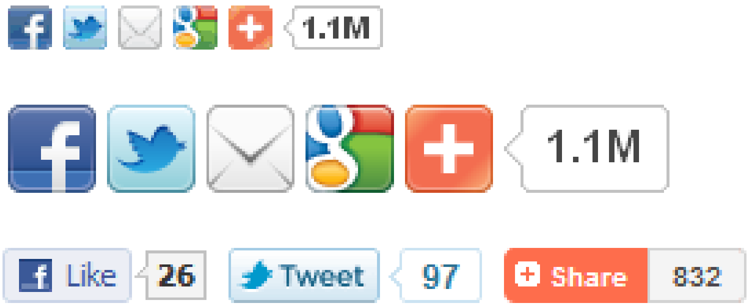
Status: OK
Inconvenience: None

Some websites use cookies to spread the load to their website over multiple servers. The cookie remembers which server they're talking to so their experience is consistent.

These cookies are almost unquestionably permitted as technically essential for the provision of the service that the user would expect. They also tend to be unique, so it's extremely unlikely that a cookie would do double-duty and say track the user as well – you should of course check to be sure.

Social media plugins

Status: Prohibited, but with contentious liability
Inconvenience: Frustrating



Social media plugins – such as the Facebook Like button – almost all use cookies to track their visitors in a way that goes beyond what a user might expect. If you visit a website with a Facebook Like button on it, then Facebook know about it – even if you're not logged in to Facebook, and don't click their button[12].

Of course these plugins have to use some cookies to work. Without cookies these buttons would need to ask you to log in every time you clicked on them. But to justify the cost of providing these buttons, they generally go further and mine for information, which specifically violates the new privacy law.

Future versions of these social plugins could arise which wouldn't do this, but we wouldn't hold our breath.

User preferences

Status: A mess
Inconvenience: Minor

Many websites use cookies to set and recall a user preference – for example, to allow larger text for visually impaired users. Without cookies this would be impossible.

Shockingly, the UK regulator appears to specifically question whether even this is allowed[13]:

> *"The only exception to this rule is if what you are doing is 'strictly necessary' for a service requested by the user ... **The exception would not apply, for example, just because you have decided that your website is more attractive if you remember users' preferences** ..."*

[12] http://news.cnet.com/8301-13578_3-20006532-38.html

[13] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

Try not to spit your own teeth out when reading that.

Qualifying their own guidance, they later say:

> *"It might be useful to think of this in terms of a sliding scale, with privacy neutral cookies at one end of the scale and more intrusive uses of the technology at the other. You can then focus your efforts on achieving compliance appropriately providing more information and offering more detailed choices at the intrusive end of the scale."*
>
> *"The more privacy intrusive your activity, the more you will need to do to get meaningful consent."*

The vast majority of user preferences are privacy neutral – the user's preferred font size, or what order they would like their news articles to be displayed in. We therefore understand that websites would need to do less to comply with user preferences cookies; presumably with a small disclaimer underneath the affected feature.

But wait. The above quotes are from the UK regulator of this law, and seem to contravene what the EU directive allows[14]:

> *"This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as* ***strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service****."*

We would argue that if a user sets a preference for a website – say by clicking on a button – that they "explicitly requested" a service, and that to provide that service cookies are "strictly necessary".

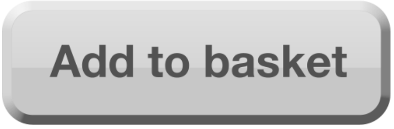
In essence, we think the ICO's mention of user preferences is false or at the very least confusing. But remember, we're not lawyers.

The one thing we know for sure is that no-one seems to know anything for sure.

[14] http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf

Add to basket

Status: OK, with caution
Inconvenience: None



Adding something to a basket is *almost* impossible without cookies[15]. The user clearly expects this action to store something about them for a short while – accordingly cookies are "strictly necessary" and allowed. The ICO even cited this as a specifically permitted use of cookies[16].

> *"This exception is a narrow one but might apply, for example, to a cookie you use to ensure that when a user of your site has chosen the goods they wish to buy and clicks the 'add to basket' or 'proceed to checkout' button, your site 'remembers' what they chose on a previous page. You would not need to get consent for this type of activity."*

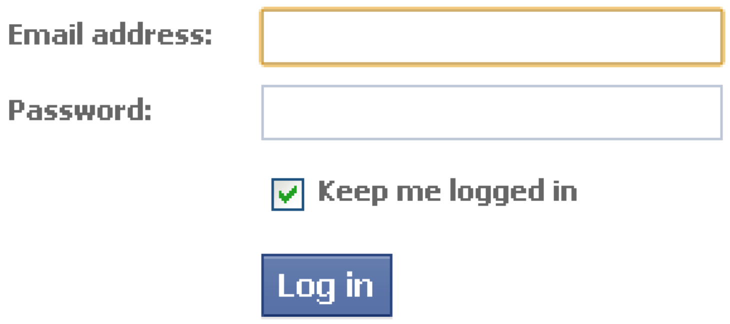
There is a caveat: the cookies which allow adding to a basket sometimes are shared for other purposes. Because many sites implement this through general purpose 'session' cookies, this can be quite common, and you should check to be sure.

Login

Status: OK, with caution
Inconvenience: None

[15] The technically inclined could pass a session ID in the query parameters for each subsequent page, which is generally frowned upon as it embeds security information (your session) in something public (the URL).

[16] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx



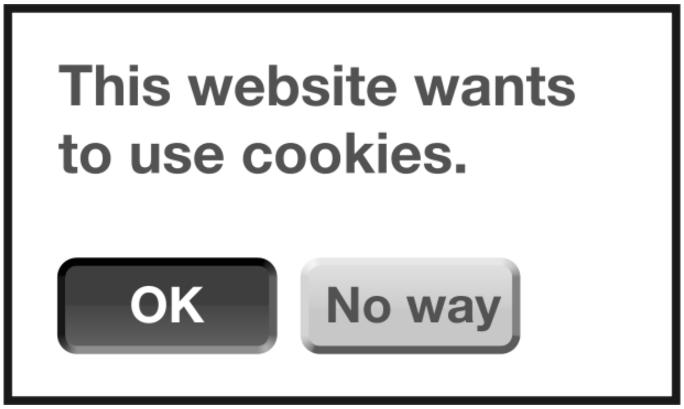
☑ Keep me logged in

Logging in to a website is *almost* impossible without cookies[17], and the "remember me" checkbox that appears below most login forms is entirely impossible. The user clearly expects a login facility to remember who they are for a time – accordingly cookies are "strictly necessary" and allowed in most cases.

There is a caveat: the cookies which allow login sometimes are shared for other purposes. This is particularly true if they don't expire when the user has logged out; the user may still be tracked and didn't implicitly consent to this. Because many sites implement login through general purpose 'session' cookies, this can be quite common.

Remembering whether cookies are allowed

Status: Hilarious
Inconvenience: Moderate



This website wants to use cookies.

So this is at least funny.

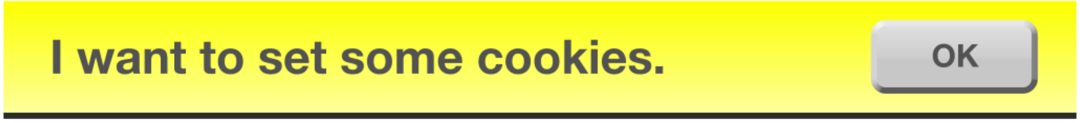
[17] The technically inclined could pass a session ID in the query parameters for each subsequent page, which is generally frowned upon as it embeds security information (your session) in something public (the URL).

Assume you ask a visitor whether they consent to using cookies. How do you remember their response – with a cookie?

If you want to avoid asking the user the same question on every page, you'll have to. Of course if they accept the use of cookies, you can set a cookie and never ask them again. But if they don't, you can't remember, so you have to ask them the same annoying question on every page.

What this means is you can't really show a popup window like the one above. There's no point giving them a "No way" button because you'll have to ask them again, and the popup would appear on top of your page and drive any visitor to insanity.

So you'll probably need an accordion strip like this instead, with a single button:



I want to set some cookies.

The strip would appear at the top or bottom of every page. It would be mildly intrusive of course, but at least the user could dismiss it with a single click.

Nevermind that storing a single on/off cookie that holds no private information whatsoever and specifically recalls that you don't want to be tracked is actually in violation of the law that it would be upholding.

Still, at least it's funny.

The situation in the UK

In brief

- **The law is confusing**
- **Won't be enforced until May 2012**
- **Financial penalties (£500k) / prosecution possible**
- **Likely affects tens of thousands of organisations**
- **Penalties appear unlikely for small organisations**

Who is responsible?

There are two bodies in the UK to be aware of:

The DCMS

Department for Culture, Media and Sport

The DCMS are **legislators**. They write and pass laws.

In this case they're responsible for the specific UK law, based on what the EU required of all member states in the EU e-Privacy Directive.

The ICO

Information Commissioner's Office

The ICO are **regulators**. They police and enforce the laws.

Anyone may raise a complaint about a website to the ICO, who resolve disputes and exercise penalties.

Why the confusion?

Only vague recommendations have been given, and the law is ambiguous.

The UK government copied the confusing EU directive word-for-word without adding any clarification on any issues. They've also intentionally chosen to avoid giving specific recommendations on how to comply with the law[18]:

> *"... we do not think there is any rationale for Government to specify the technical measures needed to obtain consent."*

The theory is that industry will figure out the best solutions themselves over time, but currently the industry remains confused.

When does the law apply?

Enforcement action won't begin until May 2012, but they expect to see action before then.

The UK only partly described[19] how it intends to comply with the EU directive before it came into effect on May 2011. Because of the resulting confusion, the commission responsible has said they will delay enforcement of the law until May 2012[20].

The ICO have said they will take a dim view of organisations that fail to act before then:

> *"This does not let everyone off the hook. Those who choose to do nothing will have their lack of action taken into account when we begin formal enforcement of the rules."*
>
> *Information Commissioner, Christopher Graham*

What fines / penalties apply?

The ICO can fine organizations up to £500,000 if they "seriously breach" the new rules[21].

[18] http://www.dcms.gov.uk/images/publications/cookies_open_letter.pdf

[19] http://www.theregister.co.uk/2011/05/25/cookies_directive_partial_notification/

[20] http://www.ico.gov.uk/~/media/documents/pressreleases/2011/enforcement_cookies_rules_news_release_20110525.ashx

> *"The Commissioner will be able to impose a monetary penalty notice if an organisation has seriously contravened the Regulations and the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the organisation must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it."*

The ICO has wide ranging powers to request information from organisations, audit them, and serve them with enforcement notices. If these measure fail they can issue financial penalties or prosecute those who commit criminal offences.

What is the risk to me?

Tens of thousands of organisations could be affected, but the risk of prosecution or a penalty is low.

Because the law is new, there are no figures for what percentage of cases are likely to be upheld – however, we do have figures for other Acts the ICO has regulated for some time[22]:

Data Protection Act	**Freedom of Information Act**
Cases received: 33,234	Cases received: 3,734
Cases closed: 32,714	Cases closed: 4,196
Prosecutions: **9**	Regulatory and enforcement actions: **3**
Enforcement notices: **15**	

There is no guarantee that the e-Privacy law will be enforced in a similar way, but if so it appears prosecutions and financial penalties are an absolute last resort. However, it also suggests that tens of thousands of organisations may at least be ordered directly to comply with the law.

The risk of penalty or prosecution further depends on how many people your website is likely to affect.

The ICO say they will only enact financial penalties which affect a large number of people: This presumably rules out the majority of small businesses and websites[23]:

[21] http://www.ico.gov.uk/news/current_topics/new_pecr_rules.aspx
[22] http://www.ico.gov.uk/about_us/our_organisation/key_facts.aspx

> *"The monetary penalty powers will apply only to the most serious breaches, such as cases where a large number of individuals have suffered distress"*

The ICO say they intend to issue further guidance on how they intend to use their powers later in 2011.

[23] http://www.ico.gov.uk/news/current_topics/new_pecr_rules.aspx

The situation throughout the EU

In brief

- **Signs point to different laws in different states**
- **Almost none of the EU has any laws in place: only UK, Denmark and Estonia have anything**
- **None of the countries with laws are yet enforced**
- **France, Slovenia and Luxembourg have notified some measures**
- **The 21 other member states have yet to report anything**

What we know

> *The ambiguity of the text will probably lead to the unwelcome situation where some EU countries have implement the stricter or more lax approach, depending on the privacy attitudes of the country.*[24]
>
> *Pascal Van Hecke, technical advisor to the Dutch Data protection Authority*

State	**Current status** (8th June 2011)
United Kingdom	Laws in place[25] but not enforced until May 2012. Have published official guidelines, more detail than any other country so far. See "The situation in the UK" (page 21).
Denmark	Notified the EU of laws but postponed their implementation for an unspecified period[26].
Estonia	Notified the EU, but no further clarification is available.
France	Has notified some measures, rumoured intent to target 3rd

[24] http://eu.techcrunch.com/2011/03/09/stupid-eu-cookie-law-will-hand-the-advantage-to-the-us-kill-our-startups-stone-dead/

[25] http://www.legislation.gov.uk/uksi/2011/1208/contents/made

[26] http://blogs.olswang.com/datonomy/2011/05/31/denmark-cookie-rules-postponed/

	party cookies but specifically *not* to prohibit web analytics. This contrasts with the UK's approach which appears to prohibit analytics.
Slovenia	Has notified the EU of some measures, but nothing is enforceable at this time.
Luxembourg	Has notified the EU of some measures, but nothing is enforceable at this time.
Latvia	Has notified the EU of some measures, but nothing is enforceable at this time.
Lithuania	Has notified the EU of some measures, but nothing is enforceable at this time.
Netherlands	Has not notified the EU yet. Their discussion is ongoing[27].
Austria	No notification, no clarification yet.
Belgium	No notification, no clarification yet.
Bulgaria	No notification, no clarification yet.
Cyprus	No notification, no clarification yet.
Czech Republic	No notification, no clarification yet.
Finland	No notification, no clarification yet.
Germany	No notification, no clarification yet.
Greece	No notification, no clarification yet.
Hungary	No notification, no clarification yet.
Ireland	No notification, no clarification yet.
Italy	No notification, no clarification yet.
Malta	No notification, no clarification yet.

[27] Pascal Van Hecke: http://eu.techcrunch.com/2011/03/09/stupid-eu-cookie-law-will-hand-the-advantage-to-the-us-kill-our-startups-stone-dead/

Poland	No notification, no clarification yet.
Portugal	No notification, no clarification yet.
Romania	No notification, no clarification yet.
Slovakia	No notification, no clarification yet.
Spain	No notification, no clarification yet.
Sweden	No notification, no clarification yet.

We will update this eBook and our website as more information becomes available for individual member states (www.silktide.com/cookielaw)

What does this mean?

Although only the UK has provided firm guidance, it already appears that countries will adopt laws ranging from permissive (analytics is allowed) to strict (it is not).

What does appear clear is that all countries will prohibit the use of 3rd party cookies, and potentially those which persist outside of the browser session (so called 'persistent cookies'), and in particular cookies which are not easily clearer via the use of traditional browser controls, such as Flash cookies[28].

Under even the most permissive legislation, cookies used for targeted advertising are almost certain to be strictly prohibited.

[28] http://admin.campaigner.nl//users/ddma/files/95907289-alexanderalvaroexplainescookies.pdf

Legal questions

We're outside of the EU, are we affected?

Only if you have operations in the EU.

If your organisation falls under the jurisdiction of the EU then it is subject to this law. The regulators who enforce it are based in the member states of the EU. So if your organisation is – say – located solely in the US, but sells to EU customers, we don't foresee this causing problems for you.

If on the other hand you have offices in the EU, or other legal entities, they may be subject to the law[29]:

> *"If you are a multinational company headquartered in the US, you should be doing something to comply with this directive"*
>
> *Dennis Dayman, Chief Privacy Officer at Eloqua*

This is a complex issue for multinational organisations and you should seek appropriate legal counsel.

Can we just host our website outside of the EU?

No.

If your organisation falls under the jurisdiction of the EU, it doesn't matter where your website is hosted. It will be your organisation that is prosecuted, not your hosting provider.

What does "strictly necessary" mean?

It's more restrictive than it sounds.

It is often said that cookies are allowed if they are "strictly necessary". This quote comes from the original EU Directive[30]:

[29] http://www.infosecurity-us.com/view/18242/cookie-monster-new-eu-privacy-law-applies-to-us-firms-with-european-operations/

> *"This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network,* ***or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service****."*

Lets break this down.

1. A user must *explicitly request* a service.
2. Cookies must be *strictly necessary* to provide that service.

So if cookies are set for a service the user did not specifically request, they're not allowed. And if the service they did request didn't need those cookies, they're not allowed.

Analytics, behavioural advertising and conversion tracking therefore seem clearly excluded.

Login, adding items to a basket and most user preferences appear to be allowed.

If in doubt, remember the spirit of the law is to *protect the privacy of users*; if necessary at the expense of website owners[31]:

> *"While the Article 29 Working Party does not question the economic benefits that behavioural advertising may bring for stakeholders, it firmly believes that* ***such practice must not be carried out at the expense of individuals' rights to privacy and data protection****."*

What is clear is that cookies are not permitted just because they are "strictly necessary" for the website owner. They must be explicitly requested by the user as well.

The UK regulator also clarified that "strictly necessary" is a narrow definition, as is unlikely to accept much wiggle room[32]:

[30] http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf

[31] http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf

[32] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

> *"The only exception to this rule is if what you are doing is 'strictly necessary' for a service requested by the user ... **This exception needs to be interpreted quite narrowly** because the use of the phrase "strictly necessary" means its application has to be limited to a small range of activities and because your use of the cookie must be related to the service requested by the user."*

What about states in the EU other than the UK?

They haven't published laws yet, and they could be different.

At the moment only the UK has published any guidance at all, and it is possible that the other EU member states will set different laws. If that's the case, website owners may need different solutions for different parts of the EU.

Isn't this just going to all be ignored?

By small companies, possibly. But services you depend on will likely be affected, and you might be compelled to act.

In effect the law criminalises the vast majority of existing EU websites. Currently there are – by the government's own admission – inadequate technologies to make compliance with the law practical. So change will be slow.

The first people to be prosecuted will also probably be the largest. It'll take a test case or two for more people to take the law seriously.

You may find that services you depend upon – particularly those which use 3rd party cookies, like adverts, social media plugins and analytics – start to change or limit their capabilities for users in the EU.

Technical questions

What exactly is meant by "cookies"?

Web cookies and anything like them stored on your user's computers.

The law isn't actually about cookies, but because it affects them so much people have started calling it the 'Cookie Law'. It's actually about all technologies which store information in the "terminal equipment"[33] of a user. The EU directive says[34]:

> *"Member States shall ensure that the storing of information, or the 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".*

You might be thinking that doesn't even mention cookies, and you would be right. The only reference to cookies occurs later in their clarifying statements[35]:

> *"Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (**such as certain types of cookies**) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access."*

So essentially this law lumps the storage of cookies together with spyware and viruses, for the same regulation.

The UK regulator also clarified that all similar technologies are covered by the law[36]:

[33] For our purposes "terminal equipment" means computer or browsing device.
[34] Article 5(3): http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf
[35] Recital 66. http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf
[36] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

> *"The Regulations also apply to similar technologies for storing information. This could include, for example, Locally Stored Objects (commonly referred to as "Flash Cookies")."*

What about cookies we can't remove?

You probably have wiggle room here, if you can prove it.

Many existing Content Management Systems, programming languages and other technologies set cookies automatically. For website owners and developers who didn't write those technologies, they need updated software with the option to turn off cookies before they can become compliant.

This is likely to be an expensive and time consuming process. The software companies have to rewrite their technology – if they care to – and the website owners have to upgrade to it.

If you look at the UK's regulator (the Information Commissioner's Office) own website, they have two cookies which they freely admit they can't remove just for this reason:

> *"We have recently become aware of this cookie. We are working with the supplier of our content management system to remove it or, if it can't be removed, to find another solution."*

Assuming that the ICO doesn't hold other organisations to a double standard, we would assume some leniency when trying to remove some cookies from their websites.

Can't people turn off cookies in their browser?

Sadly this is not enough.

All modern browsers have the ability for a user to change their settings concerning cookies, and block websites from storing cookies on their machines. Previously, the law said if your website does store cookies, you need to let your users know why you store cookies, and give them clear instructions on how to 'opt out' if they objected. Many websites did this by writing a privacy policy.

The new law however ignores the settings you currently have set in your browser, saying[37]:

> *"At present, most browser settings are not sophisticated enough to allow you to assume that the user has given their consent to allow your website to set a cookie. Also, not everyone who visits your site will do so using a browser. They may, for example, have used an application on their mobile device. So, for now we are advising organisations which use cookies or other means of storing information on a user's equipment that they have to gain consent some other way."*

This means for now it's up to the owner of the website to ask for the user's consent when they visit their website.

Won't future browsers handle this for me?

We don't believe browsers can completely satisfy the law for years, if ever.

We elaborate more in our Future section (page 49).

What about Flash cookies, HTML5 or similar technologies?

All "similar technologies" to cookies are covered by this law.

This includes Locally Stored Objects (so called 'Flash Cookies'), HTML5 Local Storage, Silverlight, Java and anything else which stores information about a user on their computer. For brevity, these are all usually referred to as 'cookies'.

What has been made clear is that websites can't comply with this law by using another technology that does that same thing as cookies[38]:

> *"The Regulations also apply to similar technologies for storing information. This could include, for example, Locally Stored Objects (commonly referred to as "Flash Cookies")."*

[37] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

[38] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

> *Information Commissioner's Office*

It also appears that if anything, these alternatives to cookies are more frowned upon by the law than traditional cookies[39]:

> *"Therefore, since flash cookies cannot be as simply deleted as other third party cookies (whether by browser setting or manually) they circumvent the user's personal browser settings and therefore also circumvent the consent issue, i.e. article 5.3 of the e-Privacy Directive becomes applicable. The same goes for other devices, such as HTML5- techniques, Java API, Silverlight or similar technique."*

Who is responsible for 3rd party cookies?

The website the user is visiting, at least for now.

Websites frequently embed plugins or scripts from third parties which themselves set cookies. Often these cookies are not even visible to the website which embeds them – for example, if you add a Facebook Like button to your site, your website can't access any of Facebook's cookies, and they can't see any of yours.

Your website can't therefore read or write any of the cookies which those third parties set – *but* – your users will still have those cookies set on their devices.

This gets into an awkward situation where you're responsible for cookies which are outside of your control.

The EU said[40]:

> *"... the consent obtained to place the cookie and use the information to send targeting advertising would cover subsequent 'readings' of the cookie that take place* ***every time the user visits a website partner of the ad network provider which initially placed the cookie****."*

Note that they specifically state the permission belongs to the "website partner" of the "ad network provider". So you couldn't just have – say – Google ask one question for all of their adverts on all sites. They'd have to ask for *each and every site that shows Google's ads*.

The UK regulator concluded they don't know how this will work yet[41]:

[39] http://admin.campaigner.nl//users/ddma/files/95907289-alexanderalvaroexplainescookies.pdf

[40] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

> *"This may be the most challenging area in which to achieve compliance with the new rules and we are working with industry and other European data protection authorities to assist in addressing complexities and finding the right answers."*

What about saving a session in a query parameter?

That's probably OK, which is a bit of a loophole.

The law refers to information stored on the user's own "terminal equipment"[42] (e.g. their computer).

Query parameters, like this:

```
www.example.com/?session=1234
```

Are part of the communication mechanism between the user and the server which provides the website. Of course they're also stored on the user's computer, but only in the sense that URLs are needed to visit *any* webpage.

So if websites started to put sessions in their URLs instead of cookies, it is hard to see how they would be covered by this law. They aren't being stored, just passed from page to page.

Of course this approach has numerous problems – it's less secure, less user friendly – and it can't remember a user between visits. But it probably isn't illegal, so expect to see it used as a get-out-of-jail pass.

The only thing more ridiculous than this exception would be if the EU decided to try and prohibit it, so let us be grateful that query parameters don't also require consent.

What about IPv6? Won't that implicitly track everyone?

More or less, yes.

IPv6 is the next generation technology for addressing devices on the Internet, and is being slowly adopted around the world. It provides a frankly insane number of addresses[43] - so

[41] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

[42] Article 5(3) http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf

[43] Approximately 340 undecillion or 3.4×10^{38}

many that in theory, every device on the internet would have its own fixed IP address. (At the moment, your IP address is not a reliable indicator of who you are).

If and when this happens, tracking a user would be almost unavoidable, and cookies wouldn't be needed for many tracking purposes. IPv6 is many years away from being widespread.

Why the cookie law is total clownshoes[44]

It was impossible to research the new cookie law without developing a thorough hatred of it.

My original idea was to write two articles, arguing in favour and against the law. But as the hours passed I simply couldn't abuse enough substances to make me say anything kinder than "well, at least they meant well".

So screw it. Let's give 'em both barrels.

The law criminalises everyone

The law was meant to protect the privacy of people using the Internet. To accomplish this, the EU made *over 90% of websites illegal*.

Let us imagine we wanted to ban bullying at school. Like the EU surveying the Internet, we might look at bullying from afar, conclude that most bullying is verbal, and decide the solution is to ban all children from speaking.

Now if we proposed such a ridiculous notion you might expect people would complain! Perhaps people closer to the problem of child bullying might say:

- But most child speech is harmless!
- You can't ban child speech - it's unenforceable!
- If you ban child speech, other countries will have an advantage!
- Entire industries depend on child speech! We'll go out of business!

[44] Clownshoes: adj. - seeming ridiculous, completely out of place or proportion; utterly impractical.

And so on.

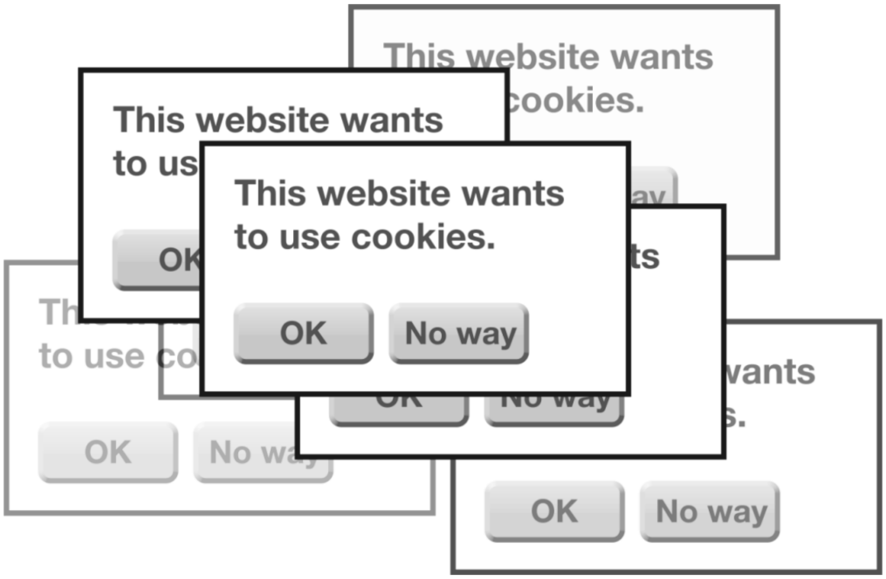
Of course if you replace "child speech" with "cookies", you'll arrive at the situation we have today. Well meaning, but ultimately clueless bureaucrats have made the oldest of law making mistakes – they've *made a law about something they don't understand*.

Most users actually like cookies

Users may not understand cookies, but they'll understand if you start taking them away.

Imagine a new web browser that abides by the EU's law, and requires users to opt into cookies with full consent. Such a browser would start by denying all cookies, and display a popup each time one was needed, allowing the user to opt in.

We would like to take the EU Council and force them to use such a browser for a month, if indeed the majority of them are qualified to operate a mouse.



Even if this browser existed in a perfect ecosystem of well behaved websites and clear privacy policies, it would take twice as long to accomplish anything. The simple fact is *people don't like being interrupted with questions they don't care about when they're trying to get something done*. So they'll just blindly click yes or no and resent your website slightly more.

Think how many people can be bothered to read the fine print in a mortgage application – probably the most important transaction in their life. Now how much do you think they care about your damn cookie policy?

The law is technically illiterate

The law doesn't actually target cookies alone – it refers to 'information stored in the terminal equipment of a user". So anything stored on your computer, basically. They actually lump spyware and viruses into the same description as cookies[45].

Like us banning child speech, they heard criticism from industry and decided to allow a narrow exception for cookies which are absolutely essential to accomplish exactly what the user requested. That's like us saying we'll allow child speech only if it is required for the child to stay alive.

Taken to its logical extreme, the law should prohibit query parameters – or even URLS – without consent, because these *could* be used to track the user (and given the new law, probably will be).

Cookies are going to be exceedingly hard to remove from existing technology, and the one year grace period is not close to enough. The technology doesn't even exist yet, and by the time it does you're not going to force the entire EU to upgrade their Content

[45] EU Directive, Recital 66: http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf

Management Systems, analytics, social plugins, discussion forums, conversion tracking and advertising mechanism in a year.

But any web designer could have told them that already.

The law is economically ignorant

The Internet is an incredible engine for economic and educational growth. Consider a world without Google – a company that makes over 97% of their revenues from targeted ads[46]. The Internet economy we live in means that a child with a smartphone in Africa can use billions of dollars worth of search technology for free *and* Google can create jobs and make a profit.

Similarly, the undeniable impact of Facebook, YouTube or Twitter wouldn't be half as pronounced if they weren't allowed to pay for themselves via efficient advertising. *That is literally their business model*[47].

None of this is possible if we can't track people. I'm not saying this shouldn't be regulated, or that there aren't concerns, but let's not outlaw all music to prevent another Justin Bieber album.

The companies which are building the jobs of tomorrow are increasingly on the Internet. If Europe wants to build the next Facebook, Groupon or Google they can't criminalise the very technology they're built upon.

The law is clumsier than an elephant on greased rollerskates

If you read the law in detail, it's clear it hasn't been written by anyone who understands the Internet. I'd naively assumed when legislating something, you employ experts on that something.

The sheer volume of bumbling, apologetic half-explanations falling from the government mouthpieces is almost as comic as it is tragic[48]:

> *"we are working with industry and other European data protection authorities to assist in addressing complexities and finding the right answers"*

[46] http://www.sec.gov/Archives/edgar/data/1288776/000119312509150129/dex992.htm

[47] Ok, Twitter doesn't have a business model yet. But it'll probably be that.

[48] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

From the official UK regulator's guidance, *released on the day this became law*, entitled "No, we don't know what to do either"[49].

A few alternatives

I will concede that there are genuine privacy concerns posed by the Internet, but the current law isn't the solution. Here are my own thoughts:

1. **Educating users to understand cookies.** Have the advertising industry pay for a brilliantly clear website explaining cookies, with instructions on how to opt out. Require them to show it to tens of millions of people.

2. **Requiring legible cookie policies.** Set a template which is simple, clear and consistent, and require all companies to use it and point to it in a standard way, e.g. at a fixed URL.

3. **Define a viable internet standard.** Websites which use certain cookies could be required to set a new meta tag or header explaining what those cookies do. Browsers would be *happy* to support this, and could provide useful controls to show concerned users information if they wanted it.

The new law means well but gives little consideration to the majority of normal website owners or consumers. Our best hope is that like so many other ridiculous laws, it gets ignored entirely.

Or you could always move to another country.

[49] Actually, it's "Changes to the rules on using cookies and similar technologies for storing information". I prefer my title.

Solutions

The best practical advice on how to comply with the law.

What is the general consensus?

The general consensus is "wait and see" and "we don't know how this will work".

Some of the companies most affected by this are have said nothing, particularly Google. A handful of analytics companies (Omniture[50], WebTrends[51]) have made statements that essentially say "ask someone else for advice", and the UK's governing body has made vague non-committal suggestions about what might be compliant.

Adobe

Who provide Omniture analytics:

> *"... each customer should seek advice from their own counsel. Every business is different and has a different risk tolerance"*
>
> *"Consider using cookies only when strictly necessary to operate the service the user is requesting"*
>
> *"Closely monitor the development of the implementations of the ePrivacy Directive"*

WebTrends

Who provide WebTrends analytics:

> *"With many businesses involved internationally it may be difficult to determine which specific law apply, and you should consult your legal counsel."*
>
> *"Evaluate consent mechanisms, and select what best fits your business."*

[50] http://blogs.omniture.com/2011/05/24/european-union-eprivacy-directive-update/

[51] http://blogs.webtrends.com/blog/2011/05/27/eu-directive-and-cookie-law-qa/

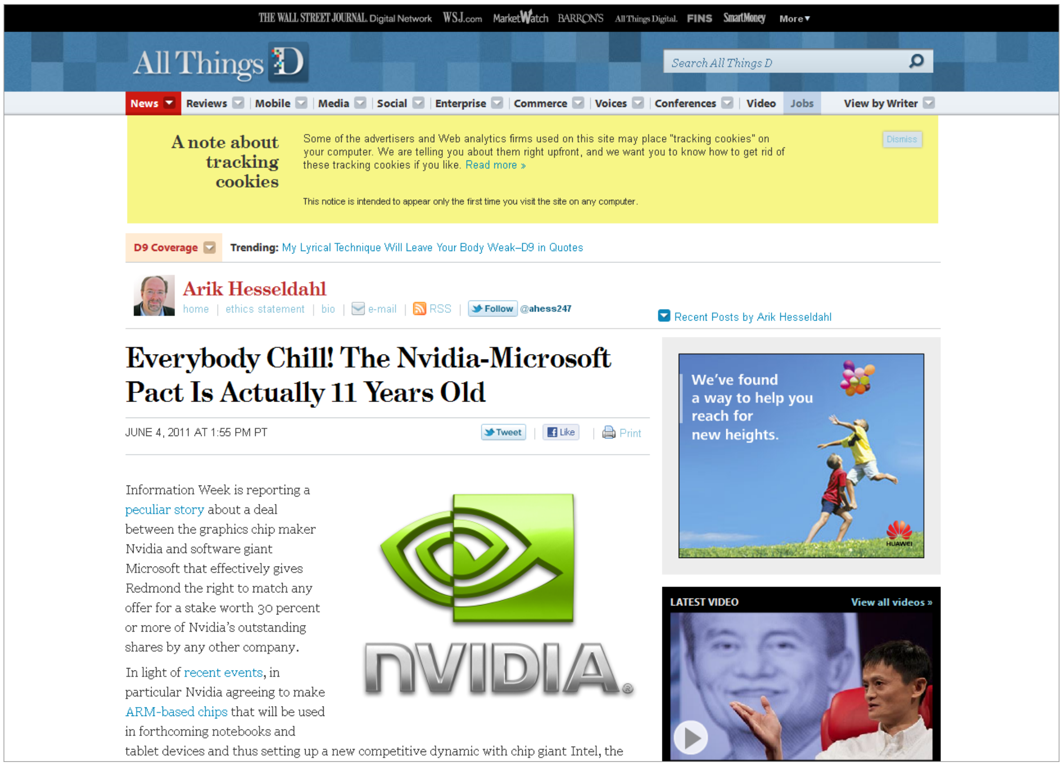
Information Commissioner's Office

The UK's governing body:

> *"We advise you to now take the following steps:*
>
> *1. Check what type of cookies and similar technologies you use and how you use them.*
> *2. Assess how intrusive your use of cookies is.*
> *3. Decide what solution to obtain consent will be best in your circumstances."*

Example solution 1: AllThingsD

This is a popular technology website owned by the Wall Street Journal. Their solution is the most elegant we've seen yet:



A note about tracking cookies

Some of the advertisers and Web analytics firms used on this site may place "tracking cookies" on your computer. We are telling you about them right upfront, and we want you to know how to get rid of these tracking cookies if you like. Read more »

This notice is intended to appear only the first time you visit the site on any computer.

Trending: My Lyrical Technique Will Leave Your Body Weak–D9 in Quotes

Arik Hesseldahl

Everybody Chill! The Nvidia-Microsoft Pact Is Actually 11 Years Old

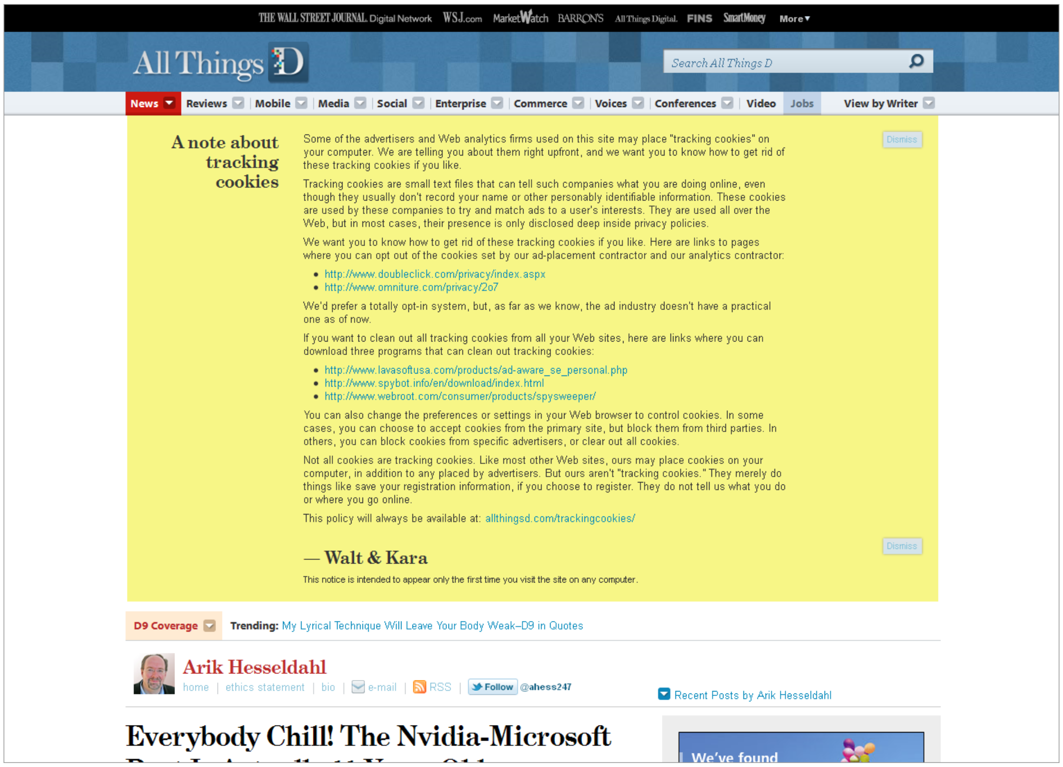
JUNE 4, 2011 AT 1:55 PM PT

Information Week is reporting a peculiar story about a deal between the graphics chip maker Nvidia and software giant Microsoft that effectively gives Redmond the right to match any offer for a stake worth 30 percent or more of Nvidia's outstanding shares by any other company.

In light of recent events, in particular Nvidia agreeing to make ARM-based chips that will be used in forthcoming notebooks and tablet devices and thus setting up a new competitive dynamic with chip giant Intel, the

This yellow panel appears the first time you view their site (it sets a cookie to remember you've seen it regardless of whether you consent).

If you choose to read more you see this:



A note about tracking cookies

Some of the advertisers and Web analytics firms used on this site may place "tracking cookies" on your computer. We are telling you about them right upfront, and we want you to know how to get rid of these tracking cookies if you like.

Tracking cookies are small text files that can tell such companies what you are doing online, even though they usually don't record your name or other personably identifiable information. These cookies are used by these companies to try and match ads to a user's interests. They are used all over the Web, but in most cases, their presence is only disclosed deep inside privacy policies.

We want you to know how to get rid of these tracking cookies if you like. Here are links to pages where you can opt out of the cookies set by our ad-placement contractor and our analytics contractor:

- http://www.doubleclick.com/privacy/index.aspx
- http://www.omniture.com/privacy/2o7

We'd prefer a totally opt-in system, but, as far as we know, the ad industry doesn't have a practical one as of now.

If you want to clean out all tracking cookies from all your Web sites, here are links where you can download three programs that can clean out tracking cookies:

- http://www.lavasoftusa.com/products/ad-aware_se_personal.php
- http://www.spybot.info/en/download/index.html
- http://www.webroot.com/consumer/products/spysweeper/

You can also change the preferences or settings in your Web browser to control cookies. In some cases, you can choose to accept cookies from the primary site, but block them from third parties. In others, you can block cookies from specific advertisers, or clear out all cookies.

Not all cookies are tracking cookies. Like most other Web sites, ours may place cookies on your computer, in addition to any placed by advertisers. But ours aren't "tracking cookies." They merely do things like save your registration information, if you choose to register. They do not tell us what you do or where you go online.

This policy will always be available at: allthingsd.com/trackingcookies/

— Walt & Kara

This notice is intended to appear only the first time you visit the site on any computer.

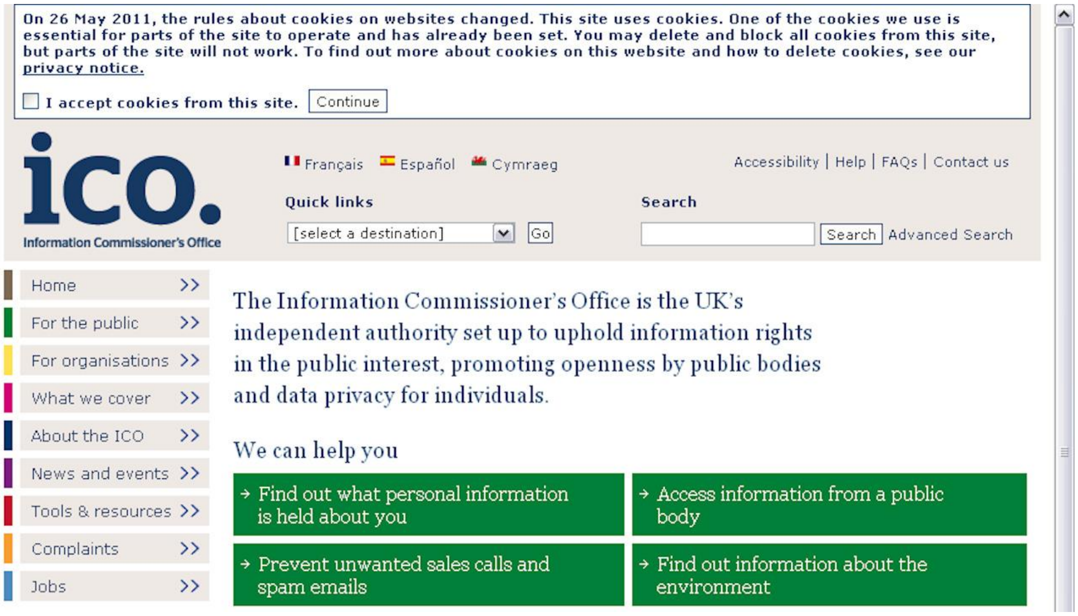
Dismiss
D9 Coverage
Trending: My Lyrical Technique Will Leave Your Body Weak–D9 in Quotes
Arik Hesseldahl
home | ethics statement | bio | e-mail | RSS | Follow @ahess247
Recent Posts by Arik Hesseldahl
Everybody Chill! The Nvidia-Microsoft
We've found

They've clearly taken some liberty with the law here because they use cookies regardless. This message merely tells you what they're already doing, and only appears once.

So in all likelihood this isn't fully compliant, but it is a step towards compliance.

Example solution 2: The Information Commissioner's Office (ICO)

The ICO is the UK regulator and was one of the first websites to comply with their own rules. They display a white box at the top of every page, and it never goes away unless you check the box and click the button to consent to cookies:



On 26 May 2011, the rules about cookies on websites changed. This site uses cookies. One of the cookies we use is essential for parts of the site to operate and has already been set. You may delete and block all cookies from this site, but parts of the site will not work. To find out more about cookies on this website and how to delete cookies, see our privacy notice.

□ I accept cookies from this site. Continue

The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

We can help you

→ Find out what personal information is held about you

→ Access information from a public body

→ Prevent unwanted sales calls and spam emails

→ Find out information about the environment

It's fair to assume this solution is considered compliant, if only because it was written by the regulator. However the text that they use assumes a clear familiarity with the term "cookies" – if you don't know what cookies are, it's meaningless to you. We thought the spirit of the law was to protect precisely the kind of people who don't know what a cookie is, and their text doesn't help those people at all. They also don't say *what their cookies do*, which is track their visitors in Google Analytics.

As the ICO themselves state in their guidelines[52]:

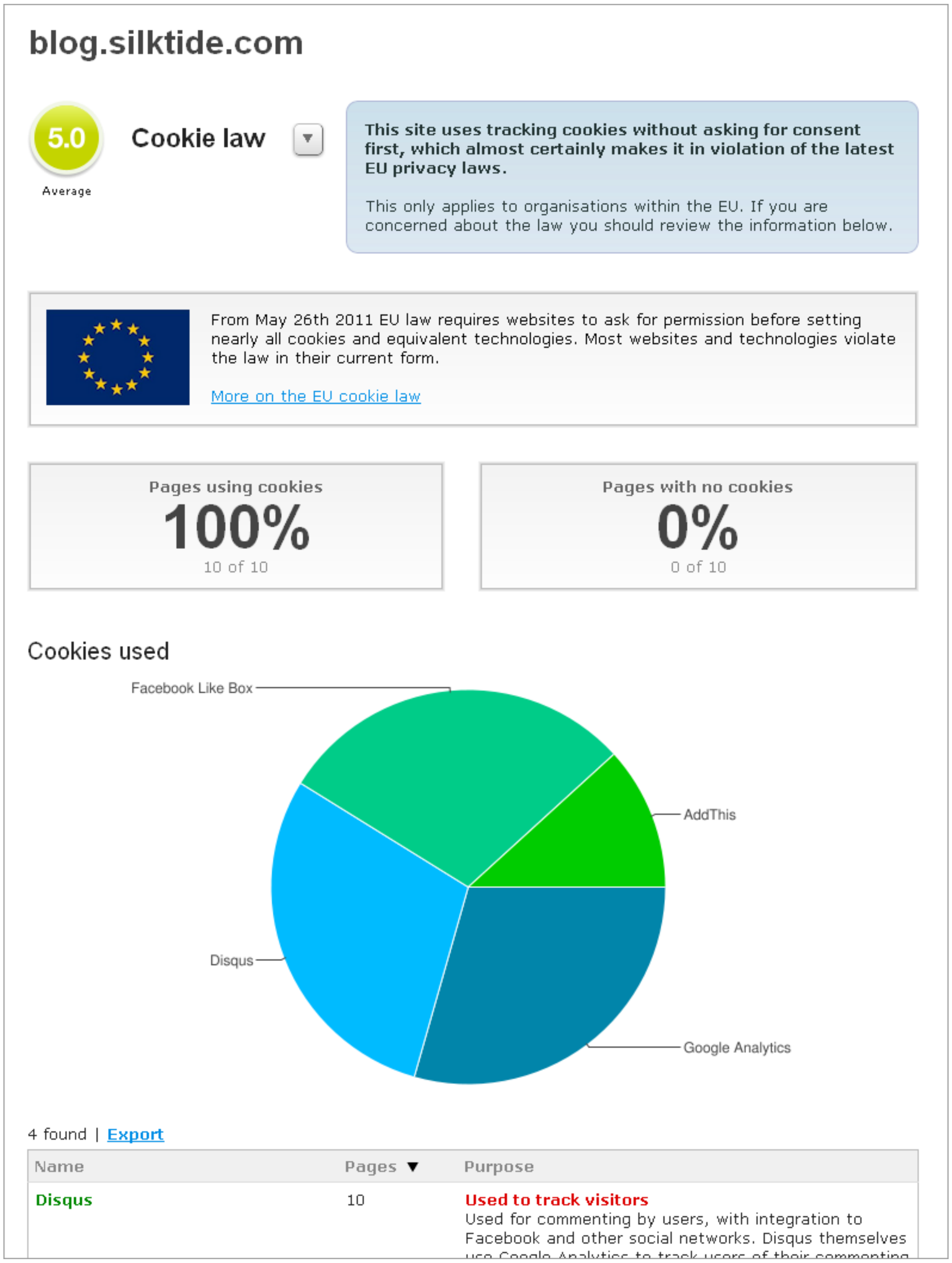
> *"Any attempt to gain consent that relies on users' ignorance about what they are agreeing to is unlikely to be compliant."*

Oh sweet irony.

[52] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

Determining what cookies you use

Silktide - the company who made this book - provide a tool for testing websites called SiteBeam, which can measure what cookies every page in your site uses automatically:



blog.silktide.com

5.0

Average

Cookie law

This site uses tracking cookies without asking for consent first, which almost certainly makes it in violation of the latest EU privacy laws.

This only applies to organisations within the EU. If you are concerned about the law you should review the information below.

From May 26th 2011 EU law requires websites to ask for permission before setting nearly all cookies and equivalent technologies. Most websites and technologies violate the law in their current form.

More on the EU cookie law

Pages using cookies
100%
10 of 10

Pages with no cookies
0%
0 of 10

Cookies used

4 found | **Export**

Name	Pages ▼	Purpose
Disqus	10	**Used to track visitors** Used for commenting by users, with integration to Facebook and other social networks. Disqus themselves use Google Analytics to track users of their commenting

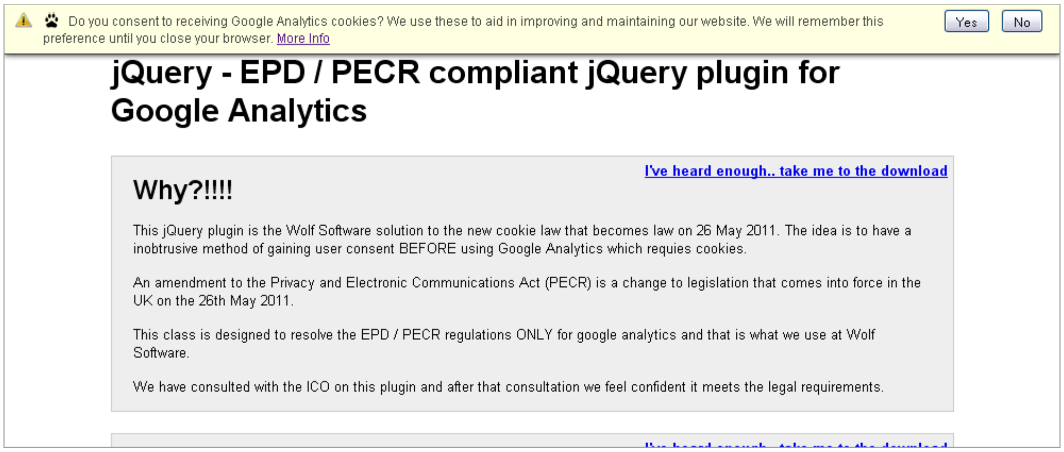
It can also help draft your cookie policy, test your spelling, accessibility, SEO, speed and more.

Try it for free at: www.silktide.com/sitebeam

Making Google Analytics compliant

These plugins have been created which ask a user for permission before enabling Google Analytics. They make obtaining compliance much easier:

Wolf Software: general purpose plugin



Do you consent to receiving Google Analytics cookies? We use these to aid in improving and maintaining our website. We will remember this preference until you close your browser. More Info

jQuery - EPD / PECR compliant jQuery plugin for Google Analytics

Why?!!!!

This jQuery plugin is the Wolf Software solution to the new cookie law that becomes law on 26 May 2011. The idea is to have a inobtrusive method of gaining user consent BEFORE using Google Analytics which requies cookies.

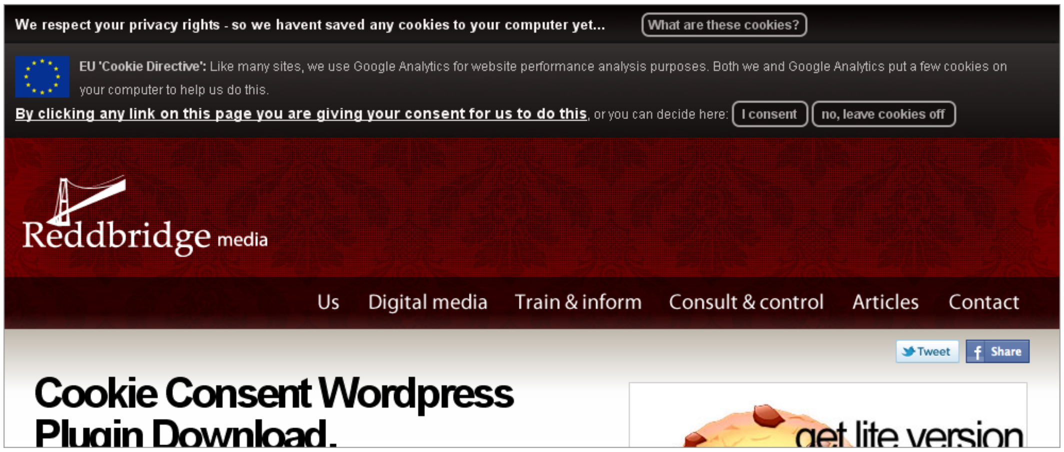
An amendment to the Privacy and Electronic Communications Act (PECR) is a change to legislation that comes into force in the UK on the 26th May 2011.

This class is designed to resolve the EPD / PECR regulations ONLY for google analytics and that is what we use at Wolf Software.

We have consulted with the ICO on this plugin and after that consultation we feel confident it meets the legal requirements.

http://cookies.dev.wolf-software.com/

Redbridge media: WordPress plugin



We respect your privacy rights - so we havent saved any cookies to your computer yet...

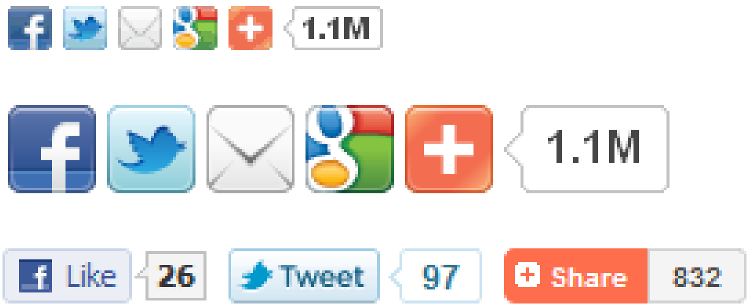
EU 'Cookie Directive': Like many sites, we use Google Analytics for website performance analysis purposes. Both we and Google Analytics put a few cookies on your computer to help us do this.

By clicking any link on this page you are giving your consent for us to do this, or you can decide here:

Cookie Consent Wordpress Plugin Download.

http://www.reddbridge.co.uk/cookie-consent/

Making social media plugins compliant



The standard Facebook Like, Re-tweet plugins all use 3rd party tracking cookies.

To become compliant, you should consider replacing these with plain links to the respective Facebook and Twitter pages. Of course this is detrimental for many reasons:

- Users need at least two clicks just to like or follow you, instead of one.
- Sharing something in this way is much harder: you're relying on them copy and pasting your web address into Facebook in particular.
- Your competitors probably won't do this.

If you're using these buttons to drive up traffic you would be right to be concerned about the effect this would have on your traffic. We expect future plugins or code snippets will provide a cookie-free option that works by passing a URL.

Other third party software

There isn't a lot you can do to change third party software you depend upon, other than ask your vendor.

We expect public sector and corporate procurement policies to require compliance to this law in future, which means companies that sell to them will slowly start to support it. Others – such as social media companies – may not choose to care.

In the meantime, you can use the same defence that the ICO uses and say the issue is currently out of your control, or gradually change your software.

The future

We've looked into our cold crystal ball, and this is what we saw.

Browsers won't fix anything

Officially we've heard a lot of talk about browsers changing in a way that means websites don't have to. We'd argue this is wilful bunk, and never going to happen.

We know why the *theory* is popular – because this change appears to involve the least disruption possible. It's easier to update a web browser than rewrite all the affected websites in the EU.

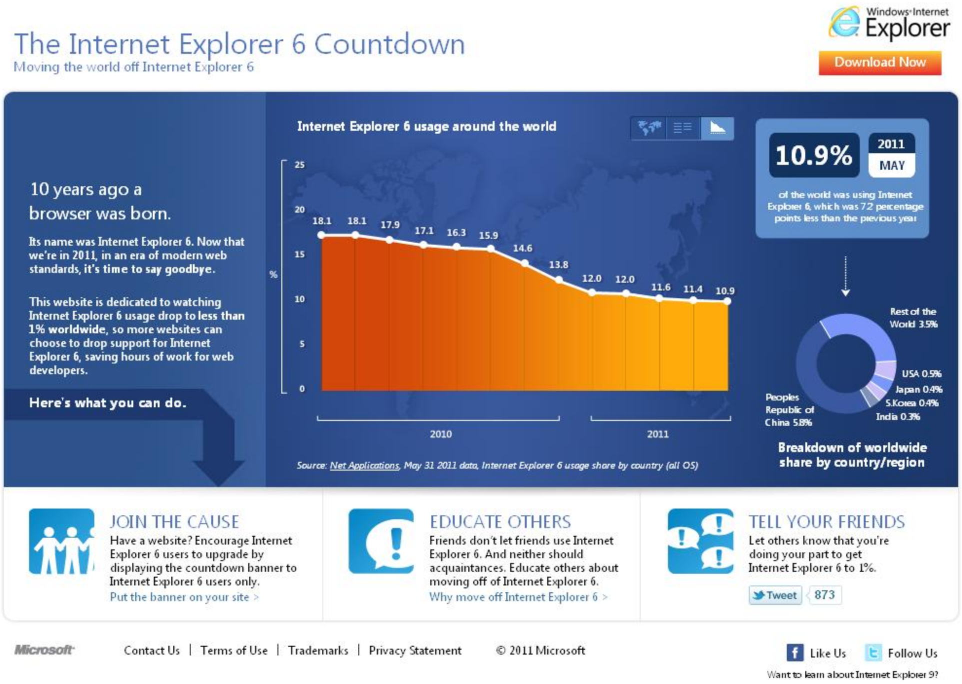
But in reality you'd be asking for two incredibly unrealistic things:

1. **Browsers would have to willingly make their browser more annoying.** If your web browser starts asking the user to confirm every website that uses cookies, then your web browser is going to suck – at least as far as the user is concerned. If Internet Explorer 10 – say – added this feature, a lot of people are going to choose to stick with something else.

   Even if they did do this, we'd expect an explosion of plugins or options to disable the ridiculous new feature, as users would utterly detest it.

   So unless all the major browsers were forced at gunpoint to do this, they'll almost certainly stall and put out weak half measures, or ignore the problem entirely. Which is exactly what we expect.

2. **Almost everyone would need to upgrade their browsers.** Ten years after it came out, 10% of the world still use Internet Explorer 6 – a clunky, insecure piece of crap - even after Microsoft themselves have run a massive advertising campaign saying "it's time to say goodbye to IE6"[53]. Some organisations simply refuse change, some have no choice if they want to run old software, others don't care.



The Internet Explorer 6 Countdown

Moving the world off Internet Explorer 6

10 years ago a browser was born.

Its name was Internet Explorer 6. Now that we're in 2011, in an era of modern web standards, it's time to say goodbye.

This website is dedicated to watching Internet Explorer 6 usage drop to less than 1% worldwide, so more websites can choose to drop support for Internet Explorer 6, saving hours of work for web developers.

Here's what you can do.

10.9% 2011 MAY of the world was using Internet Explorer 6, which was 7.2 percentage points less than the previous year

Source: Net Applications, May 31 2011 data, Internet Explorer 6 usage share by country (all OS)

JOIN THE CAUSE

Have a website? Encourage Internet Explorer 6 users to upgrade by displaying the countdown banner to Internet Explorer 6 users only.

Put the banner on your site >

EDUCATE OTHERS

Friends don't let friends use Internet Explorer 6. And neither should acquaintances. Educate others about moving off of Internet Explorer 6.

Why move off Internet Explorer 6 >

TELL YOUR FRIENDS

Let others know that you're doing your part to get Internet Explorer 6 to 1%.

Want to learn about Internet Explorer 9?

Windows Internet Explorer
Download Now
Internet Explorer 6 usage around the world
25
20
15
10
5
0
%
18.1
18.1
17.9
17.1
16.3
15.9
14.6
13.8
12.0
12.0
11.6
11.4
10.9
2010
2011
Rest of the World 3.5%
USA 0.5%
Japan 0.4%
S.Korea 0.4%
India 0.3%
Peoples Republic of China 5.8%
Breakdown of worldwide share by country/region
Tweet
873
Microsoft
Contact Us | Terms of Use | Trademarks | Privacy Statement
© 2011 Microsoft
Like Us
Follow Us

Microsoft's own website to move people away from IE6

In this case the circumstances are much worse – no browsers currently exist that are compatible with the new law. So instead of getting people to upgrade from just one browser (IE6), we would need almost everyone to upgrade to a new browser. Every company, home and mobile device. Good luck with that.

There's only one vaguely viable solution we could see working, and it looks like this:

Upon loading your new browser, it detects that the user is in the EU, and explains the new law to them. Probably in a detailed manner that satisfies EU legal experts, but completely goes over the gnat-like attention span of the average user.

[53] http://ie6countdown.com/

The explanation concludes with two options:

- I agree to opt in to all evil cookies forever and ever.
- Let me agree to cookies on a site-by-site basis.

If the user chooses to opt in, they get the Internet like they always have, and the law is essentially a joke.

If the user doesn't opt in, they see a popup or similar on every website they visit that uses cookies, asking them if they want to allow that cookie. Or if they'd prefer to opt in to all cookies, and never see this question again, which of course they will do pretty soon afterwards.

> *"Browser settings may only deliver consent in very limited circumstances. Notably, **if browsers are set up by default to reject all cookies (having the browser set to such an option) and the user has changed the settings to affirmatively accept cookies**, for which he has been fully informed about the name of the data controller, the processing its goals and the data that is collected"*
>
> *EU Data Protection Working Party, 2010*[54]

This scenario depends on a questionable interpretation of the law – certainly in spirit, it accomplishes almost nothing. And of course you'd still have the problem that people still have to upgrade to this new, monstrous browser, which would take many years.

In the meantime, website owners will be expected to do something.

Analytics companies have a hard time ahead

Nearly all existing analytics software relies upon cookies that expressly do what the law prohibits – they *track visitors without consent*. We see them as one of the greatest losers under the new law.

Because they're generally large and affect a lot of people, they're also obvious targets for complaints. Even if they themselves are not accountable, their clients are – and no-one wants to sell a product that their clients get sued for using.

So we expect analytics companies to introduce new options to accommodate for the law:

1. **A no-cookie option**, possibly only applying to users located in the EU.

[54] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

2. **An ask for permission option**, which would automatically display a popup or accordion asking users to accept cookies.
3. **A query parameter option**, which passes a tracking session in the URL instead of via cookies. There are countless problems with this, not least copy & pasted URLs being shared.

In all cases, the software would gather less data and have to deal with a confusing mix of cookie and cookie-less data, complicating their software.

We suspect analytics companies will also continue to provide an option which leaves their software as it is now, but with the blame for this firmly in the hands of the website owners. That may be their saving grace.

The biggest infringers may just ignore the law entirely

The people most under threat by this law are generally the advertisers, media, analytics and social media companies. Their businesses depend on cookies, and they won't give them up easily.

In the UK we spend more on online advertising than we do on TV[55]. Losing cookies would mean losing targeted ads, which is essentially the greatest advantage that the booming internet advertising has.

For newspapers and other media struggling to eke out a living on internet advertising, the law is poison. We're pretty sure they won't willingly start serving popups over all their articles asking users if they mind being tracked either.

The maximum fine in the UK is currently set at £500,000. Google nets over £3 billion a year from advertising in the UK alone[56] – they might be wise just to cut the EU a cheque.

The law will be weakly enforced for most

The UK acknowledged that technical solutions to this law don't really exist yet, and that insufficient time has been given for them to come about. With 24 of the 27 member states not yet having even published laws[57], we assume no-one will be prosecuted until at least 2012.

When they do, the regulator is likely to play it soft at first: asking the offenders to take positive steps towards compliance, and exacting the absolute minimum of financial or legal

[55] http://www.iabuk.net/en/1/adspendgrows300909.mxs
[56] http://www.guardian.co.uk/media/2011/apr/15/google-uk-ad-revenue-itv
[57] http://www.theregister.co.uk/2011/05/25/european_commission_cookies_directive/

penalties possible. This still means people will be forced to comply, but they're unlikely to suffer much beyond having to do the work necessary.

If we look at the figures for other Acts the UK regulator (the ICO) has regulated for some time[58], this is what has happened historically:

Data Protection Act
Cases received: 33,234
Cases closed: 32,714
Prosecutions: **9**
Enforcement notices: **15**

Freedom of Information Act
Cases received: 3,734
Cases closed: 4,196
Regulatory and enforcement actions: **3**

There is no guarantee that the e-Privacy law will be enforced in a similar way, but if so it appears prosecutions and financial penalties are an absolute last resort. However, it also suggests that tens of thousands of organisations may at least be ordered directly to comply with the law.

Query parameters will rise

We believe that query parameters, like this:

```
www.example.com/?session=1234
```

Allow for websites to continue to track users whilst still technically not falling foul of the law (this isn't true for other technologies we've researched). The alternative – requiring consent for query parameters – is too mind-bendingly stupid to contemplate.

Although they aren't a perfect substitute for cookies, they allow many of the same things – particularly tracking visitors around a website, and as such we expect to see them rise.

Of course query parameters are a horrible solution to this problem, being less secure and user friendly, but they may become de facto loophole around the whole charade.

Extra work and another fad to follow

Web developers rejoice. The public sector are publicly obligated to abide by the new law, and will likely commission new software and web development to satisfy it.

[58] http://www.ico.gov.uk/about_us/our_organisation/key_facts.aspx

Large companies are likely to modify their procurement rules, if only to be seen to be 'working towards compliance'. They may require their suppliers to meet the laws in future.

Depending on how much attention it gets, this law could filter down to smaller websites, but we doubt it.

Conclusion

There's still much we don't know about this law.

The biggest questions are:

1. What will other EU member states make law?
2. Will the law really be enforced?

At the moment only the UK has published any guidance at all, and our sources tell us that the other EU member states are likely to set different laws. If that's the case, *website owners may need different solutions for different parts of the EU*, which will complicate matters enormously.

We're honestly hoping this law is too stupid to be enforced. At least in its present form, the UK regulator themselves are barely able to comply with their own guidelines, and real technical solutions appear to be years away.

History has shown that whilst the UK regular may process tens of thousands of cases, only a handful resulted in punitive actions[59]. We expect that many websites will be ordered to change, but few will be fined for it.

So there is hope.

In the meantime, try not to panic.

[59] http://www.ico.gov.uk/about_us/our_organisation/key_facts.aspx

Appendix: The law in detail

The relevant extracts from the law explained.

The EU Directive

In October 2009 the Council of the EU adopted a Directive, amending the existing law on electronic privacy. A Directive isn't a law but it compels the member states to create their own laws, these were due by May 2011.

The relevant portion of the directive is Article 5(3) [60]:

> *"Member States shall ensure that the storing of information, or the 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 shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."*

The same document continues with a slightly contradictory "recital". A recital is not part of the law, but can contain context to clarify it:

> *(66) Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to*

[60] http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf

> *refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user.* ***Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application****. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.*

The bold section appears to suggest that browser settings (i.e. leaving cookies enabled, as they are by default in most nearly all) would be sufficient to comply.

The Internet and advertising industry quickly began citing Recital 66 as proof that a website can rely on browser settings to indicate consent to cookies. Privacy watchdogs disagreed, and subsequent events have discredited this interpretation.

EU Working Party clarification

The Article 29 Working Party is a coalition of data protection regulators from across the EU. They met to clarify the official EU position on this Directive.

In June 2010 they published their opinion in a 24 page document[61]:

> *"It follows from the literal wording of Article 5.(3) that: i)* ***consent must be obtained before the cookie is placed*** *and/or information stored in the user's terminal equipment is collected,* ***which is usually referred to as prior consent and ii) informed consent can only be obtained if prior information about the sending and purposes of the cookie has been given to the user****."*

Of importance to people looking for guidance on asking for consent:

> *"In this context, it is important to take into account that for consent to be valid whatever the circumstances in which it is given, it must be freely given, specific and constitute an informed indication of the data subject's wishes. Consent must be*

[61] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

> *obtained before the personal data are collected, as a necessary measure to ensure that data subjects can fully appreciate that they are consenting and what they are consenting to. Furthermore, consent must be revocable."*

They specifically discredited the idea that existing browser settings were sufficient:

> *"… generally speaking* ***data subjects cannot be deemed to have consented simply because they acquired/used a browser*** *or other application which by default enables the collection and processing of their information.* ***Average data subjects are not aware of the tracking of their online behaviour, the purposes of the tracking, etc****. They are not always aware of how to use browser settings to reject cookies, even if this is included in privacy policies. It is a fallacy to deem that on a general basis data subject inaction (he/she has not set the browser to refuse cookies) provides a clear and unambiguous indication of his/her wishes."*

They also acknowledged the impracticalities of asking for consent for 3rd party cookies which are shared between multiple websites (e.g. the cookies which Google, Facebook etc set on many other websites which use them):

> *"The Article 29 Working Party is conscious of the current practical problems related to obtaining consent, particularly if consent is necessary every time a cookie is read for the purposes of delivering targeted advertising. To avoid this problem … users' acceptance of a cookie could be understood to be valid not only for the sending of the cookie but also for subsequent collection of data arising from such a cookie. In other words****, the consent obtained to place the cookie and use the information to send targeting advertising would cover subsequent 'readings' of the cookie that take place every time the user visits a website partner of the ad network provider which initially placed the cookie.****"*

This in itself appears to suggest that the liability for setting those cookies belongs to the advertising provider, if only because they are the ones who would have to ask for permission. If so, it suggests the companies with the most to fear are those who embed their technology into other's websites (such as Google, Facebook, YouTube, plus countless analytics and advertising companies).

Finally they issued specific guidance on the type of disclaimers that people using cookies (in this case, advertisers) would need to provide:

> *Providing highly visible information is a precondition for consent to be valid. Mentioning the practice of behavioural advertising in general terms and conditions and/or privacy policies can never suffice. In this regard and taking into account the average low level of knowledge about the practice of behavioural advertising, efforts should be applied to change this situation.*
>
> *Ad network providers/ publishers must provide information to users in compliance with Article 10 of Directive 95/46/EC. In practical terms, they should ensure that individuals are told, at a minimum, who (i.e. which entity) is responsible for serving the cookie and collecting the related information. In addition, they should be informed in simple ways that (a) the cookie will be used to create profiles; (b) what type of information will be collected to build such profiles; (c) the fact that the profiles will be used to deliver targeted advertising and (d) the fact that the cookie will enable the user's identification across multiple web sites.*
>
> *Network providers/ publishers should provide the information directly on the screen, interactively, if needed, through layered notices. In any event it should be easily accessible and highly visible.*
>
> *Icons placed on the publisher's website, around advertising, with links to additional information, are good examples. The Article 29 Working Party urges the network providers/ publisher industry to be creative in this area.*

Confusing clarification from EU

In November 2010, European Parliament deputy Alexander Alvaro conducted an interview in which he clarified the intent of the EU Directive[62].

He stated it *does not require websites to obtain prior consent for cookies* to be placed on users' computers, saying:

> *"The definition of consent as provided by the data protection directive is very clear. Any further details would rather complicate the matter in my opinion. European legislation should set the appropriate framework for its application at [the] national level."*

He suggests that while browser settings may be sufficient for compliance with the law, because Flash cookies are not controlled by the browser, they may not be:

[62] http://admin.campaigner.nl//users/ddma/files/95907289-alexanderalvaroexplainescookies.pdf

> *"Therefore, since flash cookies cannot be as simply deleted as other third party cookies (whether by browser setting or manually) they circumvent the user's personal browser settings and therefore also circumvent the consent issue, i.e. article 5.3 of the e-Privacy Directive becomes applicable. The same goes for other devices, such as HTML5- techniques, Java API, Silverlight or similar technique."*

He questions some of what the Working Party said:

> ***While the Article 29 WP worr[ies] that adapting the browser settings does not constitute informed consent by the user, I believe that it does precisely that****. True, most browsers are set to accept all cookies by default. Nothing would prevent a relevant notice upon installation of the browser informing the user about this fact.*

At this point it becomes increasingly difficult to know how the law will be interpreted, and all eyes were on the member states to clarify the situation in their own laws.

The UK law passes the buck

In September 2010 the UK announced that they would be copying the EU directive word-for-word into UK law. In doing so they missed an opportunity to provide much sought-after clarification.

The Department for Business Innovation and Skills (BIS) said[63]:

> *"Given the fast-moving nature of the Internet, it would be very difficult to provide an exhaustive list of what uses are strictly necessary to deliver a particular online service and if we implemented in this way it would risk damaging innovation. We therefore propose to implement this provision by copying out the relevant wording of the Article, leaving ICO (or any future regulators) the flexibility to adjust to changes in usage and technology."*

Essentially they passed the buck.

[63] http://www.bis.gov.uk/assets/biscore/business-sectors/docs/i/10-1132-implementing-revised-electronic-communications-framework-consultation.pdf

The ICO issues guidance

The Information Commissioner's Office is the body responsible for enforcing the new laws in the UK. Less than a month before the law came into effect, they issued some of their own guidance[64].

They again clarified that browser settings are insufficient for consent:

> *"At present, most browser settings are not sophisticated enough to allow you to assume that the user has given their consent to allow your website to set a cookie. Also, not everyone who visits your site will do so using a browser. They may, for example, have used an application on their mobile device. So, for now we are advising organisations which use cookies or other means of storing information on a user's equipment that they have to gain consent some other way."*
>
> *"We are aware that the government is working with the major browser manufacturers to establish which browser level solutions will be available and when. For now, though, you will need to consider other methods of getting user consent."*

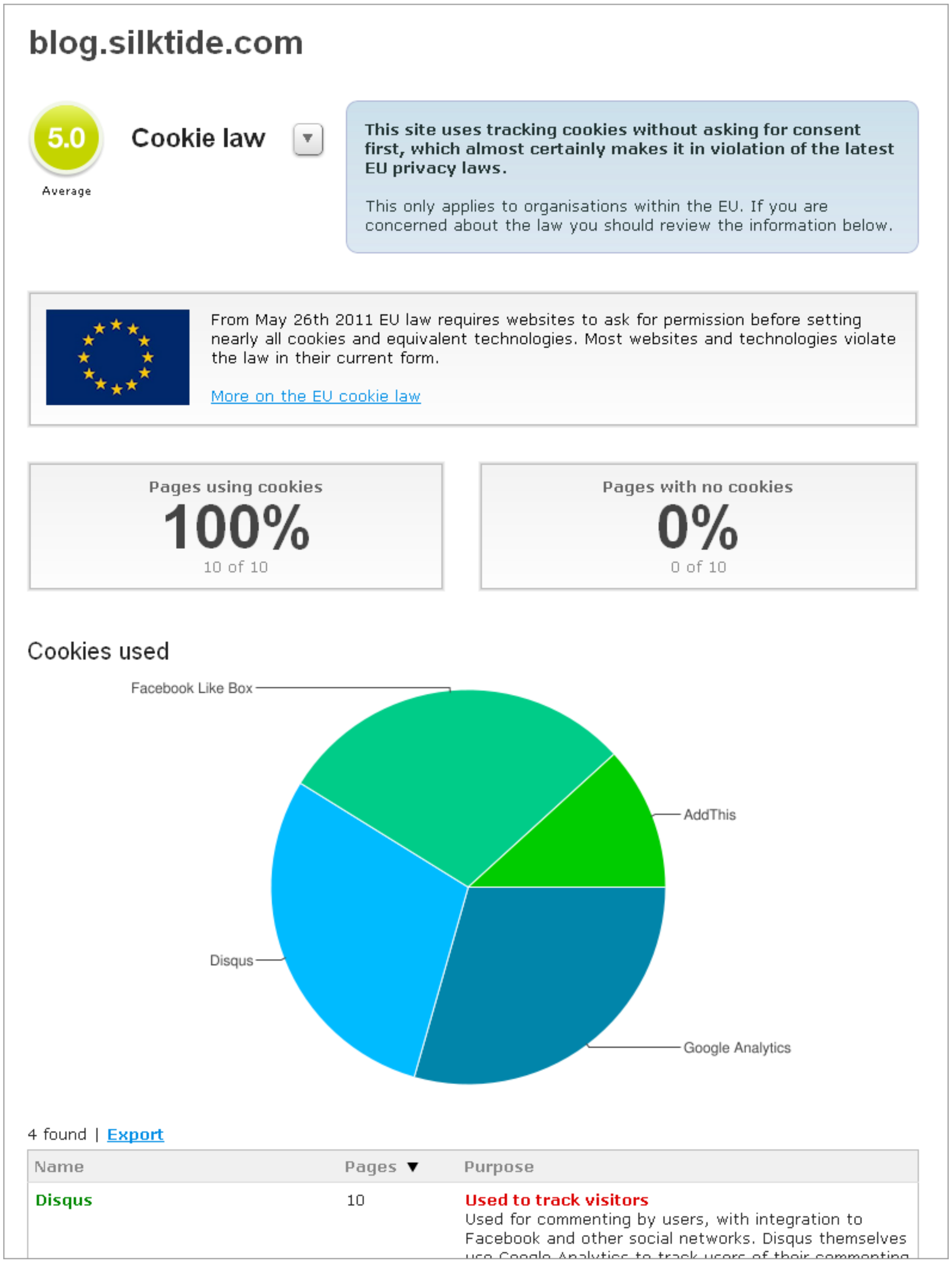
They also clarified that the law covers all "similar technologies" to cookies:

> *"The Regulations also apply to similar technologies for storing information. This could include, for example, Locally Stored Objects (commonly referred to as "Flash Cookies")."*

[64] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx

Does your site use cookies? Which ones?

We provide a tool for testing websites called SiteBeam, which can measure what cookies every page in your site uses automatically:



blog.silktide.com

This site uses tracking cookies without asking for consent first, which almost certainly makes it in violation of the latest EU privacy laws.

This only applies to organisations within the EU. If you are concerned about the law you should review the information below.

From May 26th 2011 EU law requires websites to ask for permission before setting nearly all cookies and equivalent technologies. Most websites and technologies violate the law in their current form.

More on the EU cookie law

Pages using cookies
100%
10 of 10

Pages with no cookies
0%
0 of 10

Cookies used

4 found | Export

Name	Pages ▼	Purpose
Disqus	10	Used to track visitors Used for commenting by users, with integration to Facebook and other social networks. Disqus themselves use Google Analytics to track users of their commenting

It can also help draft your cookie policy, test your spelling, accessibility, SEO, speed and more. **Try it for free at: www.silktide.com/sitebeam**