affilinet

EU Cookie Law

Understanding the EU's ePrivacy Directive

Foreword

Since 2011 we have seen a significant amount of press coverage for the so called Cookie Legislation.
Initiated by another public debate around the omnipresence of Online Behavioural Advertising (OBA), the European Commission saw the need to act and regulate this specific segment of the online advertising market.
However when in 2009 the European commission published the amendment of the EU ePrivacy Directive from 2002, the implications where much broader then just for OBA. In fact they now have a significant impact on the future of the online advertising and eCommerce industry.
After the Commission ratified the amendment, governments in Europe had until 25 May 2011 to integrate the changes into national law; The UK and Netherlands are the most prominent cases to have implemented the Directive, however most Western EU countries in which affilinet is present, have also implemented the Privacy Directive, except Germany, Portugal and Italy so far (August 2012).
The UK was among the first to act via *The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.* The Netherlands implemented the Directive into the Dutch Telecommunications Act in May 2012. Although the 2 pieces of legislation are both based on the EU Directive, they show substantial differences; the differences continue in the other implementations and will be shortly discussed in this paper.
The paper will offer a pan-European perspective on the current status of the implementation of the ePrivacy Directive, focusing in part on the existing implementations in the Netherlands and the UK but also other countries where appropriate or diverging. We based the paper in principle on a current best practice example from the UK's Information Commissioner's Office (ICO), the "Guidance on the rules on use of cookies and similar technologies", May 2012, v3.
This overview (not legal advice) will be broken down into practical steps which will help you move towards achieving compliance in all European markets you operate, we hope you find it useful.

In case you have further questions do not hesitate to reach out to me directly!

Chris R. Hauth

Director Strategy & Corporate Development, affilinet

chauth@affili.net

Understanding the EU's ePrivacy Directive

Contents

Introduction

What's covered in this Paper?

- We start off by presenting some incisive research which demonstrates the current level of consumer understanding when it comes to cookies
- Following that, we define the core-concepts dealt with by this paper
- The new requirements of the EU Directive will be presented in an easy to digest format
- We will consider what the Directive includes, who the Directive is aimed at, and how businesses and individuals can work towards achieving compliance
- We focus on what has already happened in the UK and the Netherlands, and provide initial indications on all other significant implementations throughout the paper.
- The paper concludes by highlighting how the law will be enforced in the countries that have currently transposed the Directive to local law
- At the very end you will also find a handy FAQ which will should answer any additional questions you many have

1. Market and consumer perception of the EU Privacy (cookie) Directive

In the run up to the local implementation of the ePrivacy Directive (2009/136/EC) there has been a lot of effort put into research by private and government organizations to justify the individual story around the Directive. While some tried to prove that the limited consumer understanding of cookies begs for a more detailed regulatory approach, others wanted to underline that the consumer is much savvier than politicians tend to think.
In the UK the Department for Culture, Media and Sport commissioned PricewaterhouseCoopers LLP (PwC) to conduct research on this topic. PwC surveyed over 1,000 individuals in February 2011, many of these were classified as intensive users. The results illustrate that even 'internet savvy' consumers have limited understanding of cookies and how to manage them. Those who use the internet less regularly, or have a lower level of technical awareness, are even less likely to understand the way cookies work and how to manage them. The report concluded that:

In Focus: PWC Study on Cookies

37%

Had heard of internet cookies but did not understand how to use them

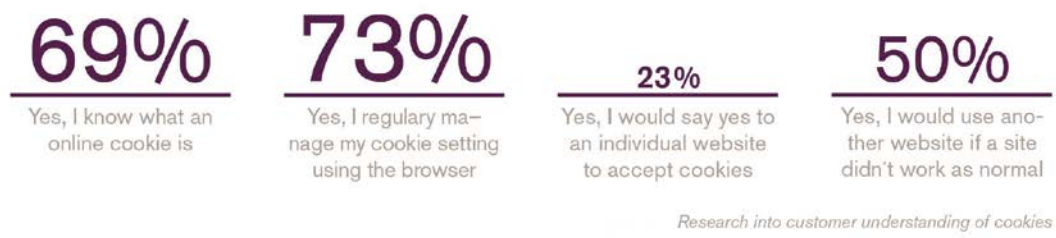
"(…) Broader consumer education about basic online privacy… could go a long way towards making users feel more comfortable online and also enable them to take more control of their privacy while online… Online businesses will need to evolve their data collection and usage transparency in order to illustrate to consumers the benefits of opting-in." *(Source: Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the EU Electronic Communications Framework. PwC, 2011)*
While we do not question the general presumption of this survey that the knowledge of cookies is.

In Focus: PWC Study on Cookies

13%

Indicated that they fully understood how cookies work

Figure 1 – research into consumer understanding of cookies

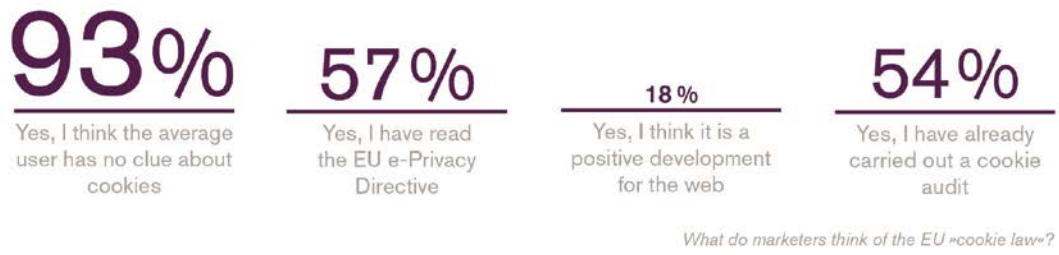


Source: eConsultancy, May 2012, http://econsultancy.com/de/reports/eu-cookie-law-the-conundrum-in-numbers, 1.500 respondents

indeed limited on the user side, there is similar research that differs in its findings. eConsultancy did another survey in May among users but also among online marketers and the results are astonishingly and fundamentally different to the study done by PWC.

In the eConsultancy study the perception of cookies in the market is much more advanced than in the PWC study. Although both are not directly comparable as the subset of users is in both cases not clearly and analytically defined, it shows that the understanding about the basic functioning of the internet is much more diverse on the end-consumer side than politicians and marketers would like it to be.

Figure 2 – what do marketers think of the EU 'cookie law'



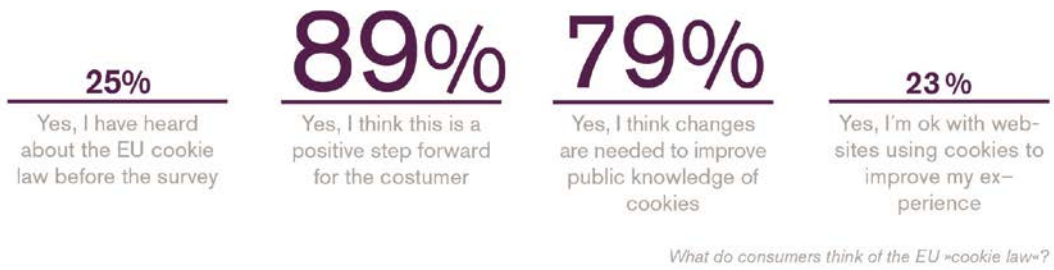
Source: eConsultancy, May 2012, http://econsultancy.com/de/reports/eu-cookie-law-the-conundrum-in-numbers, 700 respondents

Another take at the consumer opinion comes from eDigitalResearch/IMG also with a UK focus, and here the questions are much more centered around the actual implementation of the EU Directive. We agree with Graham Charlton from eConsultancy[1] regarding the interpretation of this study; it is hard to look behind those numbers and the way the questions were posed, but nevertheless it highlights the public confusion about cookies.

If the term "cookies" and "privacy" or "tracking" and "privacy" lead to a critical mindset on the

[1] Source: http://econsultancy.com/de/blog/9819-89-of-uk-consumers-think-the-eu-cookie-law-is-a-positive-step-but-is-it#

Figure 3 – what do consumers think of the EU 'cookie law'



Source: eDigitalResearch / IMG April 2012, http://www.edigitalresearch.com/news/item/nid/547500445, 2.000 respondents

consumer side, it is not the question and the way it was posed we should worry about, but the fact that we, as an industry, let this happen.
Thus from a consumer and market research perspective we need to see this as a chance to improve the public perception of cookies or online tracking technologies and less as a legal issue.
In parallel it is important that we take an active part in working with the regulators in making decisions based with clear consumer AND business focus. Sadly with the ePrivacy Directive we only had the former and now need to battle our way back into the game.
In the following chapters we will try to lead you in to the core concepts of the EU ePrivacy Directive and at the same time provide an overview of the current status of implementations and discussions in the EU countries that affilinet does business in (DE, FR, UK, ES, IT, AU, NL, PT).

2. Core Concepts

The core concepts center around some of the key terms referred to in the ePrivacy Directive. The ICO in the UK also gives a nice wrap up of the most commonly used terms and is the basis for the table below.

Figure 4 – the ePrivacy Directive: Core Concepts

What are Cookies?

Cookies are small txt files that are stored on your device when you browse the web. Cookies can do various things among those transfer information from one page to the other, remember certain settings, or transfer certain actions.
The EU Directive applies to all methods of storing and retrieving information on a user's terminal. Classic browser cookies, local shared objects (commonly referred to as "Flash Cookies") and any other method will be collectively referred to as cookies throughout this paper.

Session vs. Persistent Cookies

The term "first" or "third" party refers to the website or domain placing the cookie. First party cookies can be cookies set by the website visited by the user. Third party cookies are cookies that are set by a domain other than the one being visited by the user. If a user visits a website and another company sets a cookie from a different domain this is considered a third party cookie.

Terminal Equipment

Terminal equipment is the device a cookie is placed on – independent if it's a computer or mobile device.

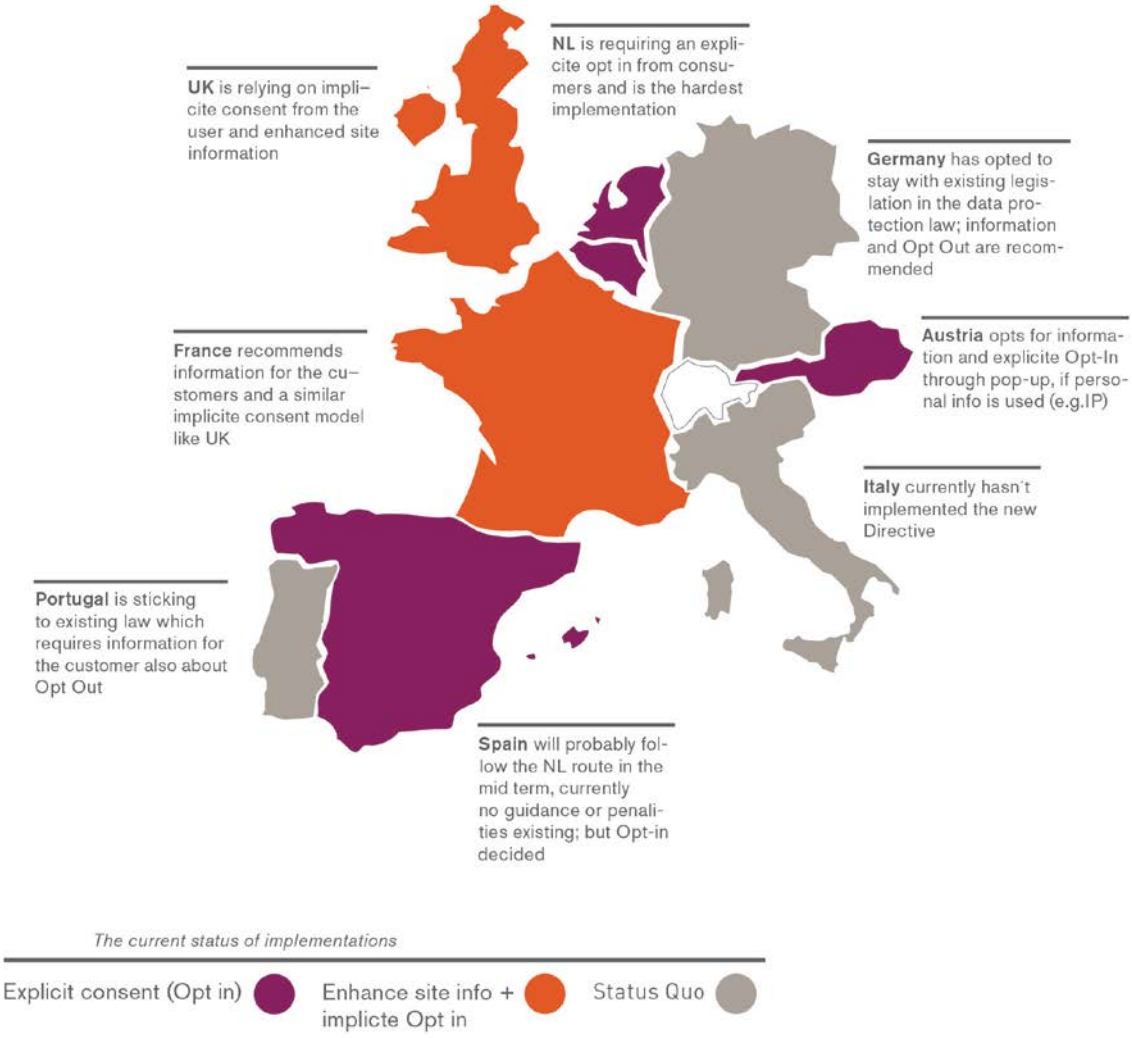
Subscribers vs. Users

A "user" is any individual using a public electronic communications service. In this context a user would be the person sat at a computer or using a mobile device. A subscriber pays for the Internet connection of the device in question. *Source: ICO "Guidance on the rules on use of cookies and similar technologies", affilinet*

3. Status quo of regulation

Since 2002 anyone using cookies has been required to provide clear information about them. This is laid out in Section 25 to the General Provisions of the EU Directive on privacy and electronic communications (Directive 2002/58/EC). This directive was amended in 2009 within the Directive

Figure 5 – the current status of implementations



Source: Internet World Business 17/12, DLA Piper, IAB Europe, affilinet research

2009/136/EC. Most of the content from 2002 remained unchanged, but some specific areas where significantly enhanced. The local legislators had 2 years to implement the EU Directive locally (until May 2011). In most of the local laws there was again a 1 year period after which the local law would come into force. This is why we have seen most of the implementations coming into force at the end of 2011 or beginning of 2012. Under the revised EU Directive the requirement is not just to provide clear information about the cookies but also to obtain consent from users or subscribers to storing and accessing cookies on their device, see Section 25 to the General Provisions of Directive

2002/58/EC, and Section 28 to the General Provisions of Directive 2009/136/EC.
The EU Directive 2009/136/EC now clearly states in the amended Article 5 (3) that "(…) the storing of information, or gaining 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 (…) about the purposes of the processing"

Although this wording is very comprehensive it already highlights the goal of the EU commission: Enabling transparency for the user regarding the purpose of existing tracking methods, such as cookies, in the eCommerce and online advertising world.

3.1 Exceptions from the requirement to obtain consent

In addition, the amended Article 5 (3) does not prevent any technical storage or access, where the use of a cookie:

- has the sole purpose of carrying out communication over an electronic communications network; or
- is strictly necessary for the provision of an information society service requested by the subscriber or user.

In defining an 'information society service' Article 1 (2) of the Directive 98/34/EC as amended by Directive 98/48/EC refers to: " (…) any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. (…) " *Source: Directive 98/48/EC .*
The concrete example that the ICO in the UK gives for a strictly necessary cookie is the following: "This exception is likely to apply, to a cookie used to ensure that when a user of a site has chosen the goods they wish to buy and clicks the 'add to basket' or 'proceed to checkout' button, the site 'remembers' what they chose on a previous page. This cookie is strictly necessary to provide the service the user requests (taking the purchase they want to make to the checkout) and so the exception would apply and no consent would be required. The regulators are aware that some parties have argued that cookies are necessary for IT resource & capacity planning, and the general operation of websites. The difficulty with this line of argument is that it could equally be applied to advertising and marketing cookies (whose activities help to fund websites). The intention of the legislation was clearly that this exemption is a narrow one and the regulators intend to continue to take the approach." *Source: ICO "Guidance on the rules on use of cookies and similar technologies", May 2012, v3, p. 12*
Some of the other European Member States (such as Netherlands, Spain and France) still have to provide the market participants with their concrete view on the exceptions to the rule. The Netherlands have very recently (August 2012) published an FAQ on the most pressing questions regarding the local implementation; however it leaves still much room for interpretation. Unless this happens we should all assume that this exception is going to be interpreted in the narrowest of ways. Hopefully other regulators in Europe will follow the UK example and help interpreting the legislation with more specific guidance and examples.

3.2 Responsibility for compliance

The Directive does not define who should be responsible for providing information about terminal data storage and access. However where a person operates an online service and any use of personal data will be for their purposes, it is clear that that person will be responsible for complying with this regulation.
The party storing and accessing the data is primarily responsible for compliance. Where third parties technology is linked to a web or native app (such as affilinet advertising) both parties will have a

responsibility for ensuring users are clearly informed about data usage and for obtaining consent. In practice it is obviously considerably more difficult for a third party who has no direct interface with the user to achieve this[2].
Although not yet explicitly stated in all countries concerned it is likely that the question of “First” vs. “Third” party cookie is a theoretical one. From what we gathered so far from talks within the industry bodies and lawyers is the following: The user is the point of reference. As the user cannot interfere that if he visits a site a cookie is dropped from another site, he has to assume the cookie is dropped by the site he visits. Thus the site he visits is his “first point of contact” so to speak when he wants to encounter details about the cookies.
This requires the industry to be transparent regarding its use of cookies particularly in the case of third party cookies. In this case the third party should work together with the first party to make the content and the purpose of its cookies transparent to the user.
An organisation based in the EU is likely to be subject to the requirements of the Directive respectively its implementation into local law even if their website is technically hosted overseas. Organizations based outside of Europe with websites designed for the European market, or providing products or services to customers in Europe, should consider that their users in Europe will clearly expect information and choices about data storage and access to be provided and that they can be subject to the local data protection laws, as the case may be (especially depending on the specific implementation of the Directive in the respective country).

[2]see also: ICO “Guidance on the rules on use of cookies and similar technologies”, May 2012, v3, p. 16

4. Consent

The EU Directive requires that users consent to the use of cookies; the data subject's consent has been defined as: " (…) freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." *Source: Section 2 of the General Provisions to the Directive 95/46/EC*
Consent must involve some form of communication where the individual knowingly ("informed") indicates their acceptance. The crucial consideration is that the individual must fully understand that by completing a certain action he/she is giving consent (including to what exactly they are consenting).
The EU Directive 2002 again specifies the way consent can be obtained a bit beyond the Directive from 1995 by: "(…) any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website." *Source: Section 17 of the General Provisions to the Directive 2002/58/EC*

Although the Directive 2002/58/EC and its different amendments do not explicitly state the timing of the consent, i.e. whether a cookie can be dropped before obtaining consent, while obtaining it or only after consent has been obtained, the term "informed" and "freely given" indicate that consent needs to be obtained before the fact, otherwise it would not be "freely given" but rather "silently foisted onto the visitor".
The term "specific" in the current interpretations across the countries considered in this paper refers to the user being clearly aware of the exact subject of what he needs to consent to. E.g. that he needs to consent or not to "cookies" or "tracking methods".
The term "informed" is currently interpreted by local regulators as users being able to understand the exact subject up for decision, e.g. he can clearly understand what "cookies"/"tracking methods" are and what their context is and how they concern his surfing process.
If the user is informed by the site he visits in a way that in laymen terms clearly explains the topic in question (e.g. cookies) and the way they impact him depending on the decision he takes, he can "indicate a whish". If the website is set up in a confusing way, distracting the user from the actual issue, even a ticked box cannot be seen as an "indication of the user's wishes".
The bottom line is: whatever you do to inform the user, do it in a very simple and easy to understand way.

In Focus: Netherlands

If you operate in the Dutch market please be aware that its adoption of the Directive states that consent has to be 'unambiguous'.
The current interpretation by the experts is that a pop-up screen with a tick-box stating "I accept" is the only way to gain consent in this market, meaning that the notion of gaining implied consent is not valid in this market.
It remains to be seen if the Dutch follow through with this as the Directive seeks harmonization across the EU and the Dutch approach would cast them as an outlier. *(Source: SOLV Advocaten: "Cookies under Control", July 2012, p.5)*

4.1 Implied vs. explicit consent

A look at the status quo of current implementations of the EU Directive shows that those countries who implemented it favor an explicit, opt-in style consent for every cookie which is set for the first time on a specific user's device.
Currently only in the UK this differs slightly: the Information Commissioner's (ICO) guidance points out that although an explicit opt-in mechanism might provide regulatory certainty it is potentially not the only means of gaining consent[3]. There is currently still a 2nd path to basic compliance. In some circumstances those seeking consent might consider implied consent as an option that is perhaps more practical than the explicit opt-in model.

[3] ICO "Guidance on the rules on use of cookies and similar technologies", May 2012, v3, p. 6

For implied consent to work there has to be some action taken by the individual from which their consent can be inferred. From the ICO's perspective in the UK this might be visiting a website with specific further information about tracking or clicking on a particular button. The key point is that when taking this action, the individual must have a reasonable understanding they are agreeing to cookies being set.
This brings us back again to the information requirement in the EU Directive. Also in this case it is mandatory to inform the user first in a transparent and very clear way, before being able to assume implicit user consent.
The issue we are facing here as an industry is that you need to again "drop a cookie" in order to check whether a user has clicked on the information site or whether the user has clicked on the "No Thanks"-button on your info-pop-up about cookies. However currently there seems not to be an alternative to this as you need to prove that you received an "implicit" consent from the user.

In Focus: User vs. Subscriber

The directive mentions both "users" as well "subscribers" as the two recipients of the directive's implications (Directive *2009/136/ EC § 5 (3)*). As the two are usually not interchangeable and technically as an industry we cannot decide whether user and subscriber are one and the same or separate or more persons, we have to assume that if we get consent from a device, it doesn't matter who uses it. If in a household a computer is used by the one paying the subscription (=subscriber) bill of the internet access and his/her spouse we cannot distinguish as an industry whether it was one or the other who used the device. Unless of course we are talking about services that require a log-in and a password from the actual user. But in the case of a classical affiliate network cookie, we will not be able to distinguish between the two. The only thing you can do is inform the users about your cookie policy and assume if someone gives consent it is valid for everyone using his/her device.

5. Practical Suggestions for Those Trying to Comply

We suggest a 3 step approach to a potential compliance with your local implementation of the EU Directive:

- Conduct a Cookie and Tracking Audit
- Prominently provide clear and simple information to your users about Cookies (and other tracking mechanisms
- Implement a method or technology to acquire the consent from the users of your site or service

These three steps, if conducted properly and according to local regulatory practices, should help you on your way to compliance. It is important that this is not a one off exercise, but rather a recurring project. The three steps need to be repeated as soon as something fundamentally changes in your technical or procedural setup regarding your deployed tracking technology (i.e. a new parameter in your cookies, a new cookie or a new tracking method).
The next chapters will quickly walk through the three steps in a bit more detail.

5.1 Conducting a Cookie Audit

The cookie audit helps you to get a transparent overview of the cookies your website/service uses and for exactly what purpose they are used. Currently the ICO in the UK is the only body who has published a detailed suggestion on how such an audit should be carried out and we rely in this paper on the suggested ICO structure[4] at the end of this paper.

The cookie audit is the basic step and determines for each and every cookie placed by your site/service the concrete content and purpose. It lays the foundation for establishing a cookie hierarchy or categorization which might make it easier for you to communicate with your users.

- Identify which cookies are operating on or through your website
- Confirm the purpose(s) of each of these cookies
- Confirm whether you link cookies to other information held about users - such as usernames
- Identify what data each cookie holds
- Confirm the type of cookie – session or persistent
- If it is a persistent cookie how long is its lifespan?
- Is it a first or third party cookie? If it is a third party cookie who is setting it?
- Double check that your privacy policy provides accurate and clear information about each cookie

Although you should have a detailed overview of each and every singly cookie as also detailed out in an example in our 2nd whitepaper “affilinet tracking cookies – deep dive”, it might make communication with your users simpler for both sides if you cluster the cookies for the user’s information in specific functional categories.

In Focus: British Telecom

An example for a categorization of cookies, instead of a simple long-list, represents the implementation of British Telecom plc. (BT) on their UK website (www.bt.co.uk). BT simplifies the categories and groups its cookies in the following categories:

- Strictly necessary & performance
- Functional
- Targeting

Whether this example prevails in the eyes of the regulator remains to be seen, equally the stance of the other EU regulators on this remains unclear.

[4] ICO “Guidance on the rules on use of cookies and similar technologies”, May 2012, v3, p. 16

Figure 6 – an example categorization of cookies proposed by the ICC in the UK

Strictly necessary

Generally these cookies will be essential first-party session cookies, and if persistent or third party, there should be a good justification for this.
Typical use: Tokens for the implementation of secure areas of a website

Performance

These cookies can be first or third party, session or persistent cookies. To fall within this category their usage should be limited to performance and website improvement.
Typical use: Affiliate tracking cookies (such as those offered by affilinet) allow publishers to improve the effectiveness of their site by identifying which content drives sales for the advertiser.

Functional

These cookies can be first party, third party, session or persistent cookies. These cookies will typically be the result of a user action, but might also be implemented in the delivery of a service not explicitly requested but offered to the user.
Typical use: Fulfilling a request by the user such as submitting a comment.

Targeting

Targeting cookies will usually be third-party, and persistent. They normally contain a unique key that enables (via other 3rd party integrations) browsing habits to be established. This ultimately leads to the targeting business being able to create automated 'intent-based' advertising.
Typical use:This approach is often associated with OBA
Source: ICC UK Cookie guide. International Chamber of Commerce United Kingdom, 2012

5.2 Providing Information

Currently only the UK administrative bodies, the Information Commissioner's Office (ICO) and the International Chamber of Commerce (ICC) are explicit about the sort of information that should be provided. The Directive itself does not specify the depth or the content of the information to be provided, but Section 25 of the General Provisions to the Directive 2002/58/EC states that users are to be provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using.
According to Section 38 of the General Provisions to the Directive 95/46/EC, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection. Furthermore, Article 2 (h) of the Directive 95/46/EC states that the consent must concern personal data relating to him and being processed.

Figure 7 – possible ways of making Information about Cookies more prominent

Positioning is important – simply moving the link from the footer of the page to somewhere more likely to catch attention is important.

Simple formatting can help – this might include changing the size of the link to the information or using a different font. The key is whether the link to this important information is distinguishable from "normal text" and other links.

Making the hyperlink more than simply "privacy policy" : this could involve a link to some explanatory text, i.e."Find out more about how our site works"

Source: ICO "Guidance on the rules on use of cookies and similar technologies"

For most users it may be helpful to provide a broad explanation of the way cookies operate and the categories of cookies that you use on your website. A description of the types of things analytical cookies are used for on the site will be more likely to satisfy the requirements than simply listing all the cookies you use with basic references to their function. However it might be helpful to have both ready and available on the site, the general overview on a category basis, as well as a deep dive into every cookie you use. We cannot give you a legally binding advice as to how exactly you need to setup your page to be compliant; it is the clear domain of the local regulator to provide this to local businesses. The ICO in the UK has taken a first stab at making detailed wording suggestions on how to best inform your users. The ICO's "Guidance on the rules on use of cookies and similar technologies" is a document that is continuously updated as soon as new insights and information becomes available[5].
If you are a UK business or you do business in the UK we suggest you have a detailed look at this document before considering any implementation of the local Directive regulation.
For all other countries the ICO guide cannot serve as a legally binding recipe, but as a well-developed example of a regulator who is willing to closely cooperate with all participants in the market, with the user's best interest in mind.

In Focus: British Telecom

The official wordpress website offers you a simple Plug-In that you could download and install and that displays a bar that informs about the EU cookie legislation.
http://wordpress.org/extend/plugins/eu-cookie-law/
In any case of legal insecurity please contact your local lawyer for an official compliance check.

[5] http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx

5.3 Getting Consent in Practice

In practice there is currently only one technique so far for obtaining consent that could for the moment be seen as sufficient in most member states: via pop-ups or pre-sites. In this case a cookie should not be dropped before consent is actively given. This can be seen as the smallest common denominator.

However going forward, some member states in their local implementation of the Directive explicitly expect that future browser settings will also be a viable way to obtain consent (e.g. Spain, France, NL).

Thus we will only discuss in this paper these two alternatives that have a pan-European reach regarding their validity.

In Focus: Germany

Although the Directive has not yet been implemented in German law, there are diverging opportunities on the interpretation and necessity to do so at all:

- The opposition tried to get the Directive transposed into law at the beginning of 2012 but failed
- The current government sees the existing Data Protection Regulation (DPR) as sufficient and does not necessarily plan to implement the Directive locally
- The Data Protection Commissioner in Germany however is of the opinion that the Directive is directly applicable in Germany even without a transposition in German law

5.3.1 Consent via Pop-ups & Similar Techniques

Pop-ups and other methods may all be used to ask a user directly if they agree to you storing data on their computer. If they are informed and click yes, you have their consent. In order to prove you have consent you might need to set a cookie on the user's device saving the information that he has given consent. The cookies run-time is nowhere described by any regulator, thus should probably for now be oriented on what is providing the best user experience. Using this technique you could ensure you are compliant by not switching on any cookies unless the person clicks I agree.

However some users might not click on either of the options available and simply continue browsing the site. If you are doing business in the UK, you might decide, in a case like this, that you can set a cookie and infer consent from the fact that the user has been given a clear notice and actively indicated that they are comfortable with cookies by continuing to use the website[6]. It needs to be very clear that this is an option that is not compliant in most of the EU countries covered in this paper, except the UK, as it relies on the "implicit" consent construct discussed earlier. If you choose this option you should potentially continue to show a notice elsewhere which reminds users that you are setting cookies as long as they do not opt out.

In order to make this solution compliant in all countries (France, Spain, NL, Austria) you need to either overlay this pop-up over your normal site, so the user has to click on "Opt In" or on "Opt out" in order to continue, or you have to use a landing page that is loading before the user can access your actual page. You will need to do this for every user who has not yet consented to your site using cookies. In this case it might make sense to carefully A/B-test several potential user flows through the acceptance procedure and find the one less intrusive and user friendly for your customers (Directive 2009/136/EC § (66)) and the one less harmful to your business.

[6] ICO's "Guidance on the rules on use of cookies and similar technologies", p. 19

Figure 8 – additional ways of making Information about Cookies more prominent

In addition to a new persistent header category, we suggest using a dynamic (e.g. JavaScript) based pop-up that anybody sees who is visiting your page for the first time.
In a first step (which will not make you compliant in any country) you use this pop-up to further actively push information to the customer. In a second step, this pop-up should probably contain the option to accept or reject the use of cookies.

Source: CO "Guidance on the rules on use of cookies and similar technologies", affilinet

5.3.2 Consent via Browser Settings

This method of consent, using the actual settings of the existing browsers has been suggested by the EU commission itself in Section 66 of the General Provisions to the Directive 2009/136/EC. Here the EU states, that
"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".
However all of the local regulators or local Data Protection agencies that have adapted the Directive so far into local law have deemed the existing browser settings as insufficient to act as a proxy for gaining consent from the end user. Currently it is unclear of how the browsers would need to be amended in order to function as a compliant mechanism according to the local regulators.
As a preparation for a future use of the browsers for gaining compliance, you should make sure that your side is reacting to a future W3C standard "Do Not Track" header. Whether you decide if you want to react to any non-W3C standard header (e.g. the potentially new one from Microsoft in the next Internet Explorer version) is up to you, but might create more confusion than help your cause.

In Focus: France

The regulator passed the EU Directive into local law in August 2011, allowing the use of the browser settings as a legitimate way to gain consent. However the local Data Protection agency (CNIL) has made it clear that it is not accepting browser settings as a way of gaining consent, but rather a dedicated page or banners before the actual page to collect the consent of the users.

5.3.3 All other potential versions of gaining consent

As indicated in the ICO's "Guidance on the rules on use of cookies and similar techniques" there might be different forms of gaining consent, e.g. through terms and conditions, through "preference settings" or "feature settings". In reality however all of these different forms need explicit user consent, thus you need to show the user through a pop-up or a specific site that you intend to set cookies and for what purpose. So in practice it will always need to be a specific site or pop-up that informs the user about this, independent of the purpose of the cookies or the location where you explicitly talk about what you like them to consent to. Under no circumstances is it sufficient to change your T&Cs or your privacy information on your website and not explicitly inform your user about this and explicitly gain his consent for that particular change. Always use a pop-up or a specific site that is prominently based in the user flow (e.g. before the user starts to interact with your site) in order to gain consent.

In Focus: CivicUK.com

Before you try to come up with a technical solution yourself if you are not using wordpress, we recommend you search for already existing independent solutions.
One of the most advanced can be found on the side of CivicUK.com.
http://www.civicuk.com/cookie-law/index
Although you should always check with your lawyer if this is appropriate in your case, the CivicUK framework is a good example for an independent and free solution.

Of course a change in regulatory frameworks also needs to be considered in your T&Cs, so make sure you adapt them appropriately in addition to making users aware of cookies and gaining their consent.

5.4 Changing or withdrawing consent for cookies

From a Directive perspective there is no concrete reference on how the process of withdrawing consent or the process for regaining consent in case you change your tracking should work. However the ICO in the UK suggests[7] you…

- make the information transparent to the user how he can revoke his consent and
- provide the user with a renewed request for consent whenever you have changed something regarding your use of cookies or any other tracking technology.

For any of the other countries we do not have any indications yet on how to deal with these cases, but could potentially assume they are setting at least similar standards.

5.5 Alternatives to Cookies

The ePrivacy Directive has mostly been associated with cookies as a very specific tracking technology, but the actual wording of the legislation refers to any type of "(…) storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user (…)" *(Source: Article 5 (3) to the Directive 2002/58/EC).*

In Focus: Netherlands

The most recent and relevant law given that it closely relates to the Directive is the new Dutch Data Protection Act that will enter into force in 2013. In addition to the requirements of the Directive this legislations asks companies who place cookies or otherwise track users to:

- Notify the Dutch Data Protection Authority that they are processing personal data
- Ensure that they have adequate security measures in place to secure personal data
- Offer users the ability to check and correct data relevant to them
- If data is being processed by a third party, a data processing agreement must be signed
- Data can only be processed if at least one of 6 grounds (one is unambiguous consent) has been met

[7] ICO "Guidance on the rules on use of cookies and similar technologies", May 2012, v3, p. 25

The legislation thus focuses in its wording on tracking technologies that rely on placing information on the terminal equipment. If you think this gives you a way out using alternative tracking technologies, this is sadly not the case. The interpretation is not focusing on cookies but on any technologies used to track actions online[8].

This includes using technologies that are using other input to enable the analysis of visits to a website (e.g. fingerprinting technologies). Similar to the guidance provided by the UK regulator recent talks in NL and Germany have hinted at a very similar interpretation from a regulator perspective.
In short: Even if you use other tracking technologies you should probably start to make them transparent for your users in a similar way to the cookies.

5.6 Cookies and Personal Data

Where cookies are linked to personal data there are greater privacy and security responsibilities. Performance Marketing activity does not tend to fall into this catchment, but advertisers & publishers engaging in more intrusive activities such as OBA to do online targeting should be careful.
Please bear in mind that all EU member states require varying levels of data protection, and that these are likely to be amended further. In January 2012 the European Commission presented the concept of a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. The changes are expected to take 2-3 years to be fully implemented. The difference of this regulation compared to the directives is that it is directly applicable in all EU countries and does not need to be transposed into local law. Currently the lines between the expected new Data Protection Regulation (DPR) and the EU Privacy Directive are not clear right now and it remains to be seen how far reaching the new DPR will become.
We will also keep you up to date on these developments. Please refer to my twitter feed (@chrishauth) and the affilinet website (www.affili.net) for further information in the future.

[8] e.g. ICO, “Guidance on the rules on use of cookies and similar technologies”, May 2012, v3, p. 25

6. Enforcement & Penalties

All member states of the EU implementing the Directive into local laws hopefully will have also put processes in place that support local businesses to become compliant; where compliance does not voluntarily occur they will enforce their individual recitals by issuing penalties. So far (August, 2012) except of Germany, Belgium, Portugal and Italy all other major Western European countries have taken steps towards enacting the new legislation. The most advanced from an enforcement perspective are currently the UK and the Netherlands.
Enforcements in other countries differ between the countries. Although in Spain the law for Online Services has been amended according to the EU ePrivacy Directive the penalty and enforcement section was left open and is to be filled within the coming months. In France the regulator disagrees with the legislator in regards to the sufficiency of existing browser settings and sees the existing browsers as not sufficiently set up for obtaining explicit user consent.
The enforcement and penalties outside of the UK and Netherlands are less clear. In Spain, there is currently no framework set either for necessary measures to become compliant or for resulting enforcements and penalties. However the legislation hints at a stricter model according to the NL example. France is currently potentially leaning towards a similar implementation as the UK from a legislative perspective; however the local data protection authority is obviously trending towards an NL model.
To be compliant in your relevant country it is necessary to consult with a local lawyer specialized in Data Protection and Privacy Regulation. Your local IAB institution can refer you to such a dedicated professional.

Figure 9 – enforcement & Penalties: The United Kingdom vs. the Netherlands (example)

United Kingdom

The Information Commissioner's Office (ICO) is responsible for enforcing the UK's implementation of the ePrivacy Directive. It has made it clear that it does not want to have to take action and levy penalties as it realises how important the digital economy is to the country! This considered approach does not mean that the law can be ignored though. Higher profile businesses and individuals should be particularly careful. In cases where a party fails to comply the ICO has a range of options available to take formal action when necessary.
Actions range from agreeing to an *Undertaking* (this commits an organisation to a particular course of action) to receiving a **Monetary Penalty Notice:** these require an organisation to pay a penalty up to a maximum of £500,000. This power can be used in the most serious of cases and if specific criteria are met. For example; if the contravention was of a kind likely to cause substantial damage or substantial distress to the end user.
Other countries tending towards UK approach: France

Netherlands

In the Netherlands the Directive has been implemented into the Dutch Telecommunication Act. The enforcement of the Directive is primarily being handled by The Dutch Independent Mail & Telecommunication Authority (OPTA).
The OPTA (like the ICO in the UK) has the power to levy significant fines, but hopes to steer local businesses down a path which enables them to be compliant without heavily impacting business as usual. The OPTA has made it clear that it will target those activities that most threaten the privacy of consumers. However without clarifying what does "most threaten" mean.
In the 2nd phase of the implementation in NL the Dutch Data Protection Authority (CBP) may also get involved, particularly when cookies are used to collect, combine or analyze information regarding user's online surfing behavior. The CBP also has the power to enforce penalties, though these currently at lower levels.
Other countries tending towards NL approach: Spain (potentially, but not yet)

Source: ICO, SOLV, affilinet

7. Summary

Some of the current implementations have the explicit potential to harm the online industry. The Dutch implementation is the most aggressive and the explicit Opt In is technically and logistically a challenge. The fact that we now need to gather even more data about the user as we have to drop cookies in order to remember whether he Opted In or not is just a very clear example of a not fully thought through legislation.
From a business perspective it can make certain business models unviable, and this might be true for the complete online advertising industry if we continue down this route. Painting cookies generally in a bad light is not a helpful approach. The ePrivacy Directive lead to further confusion and unclarity and thus failed to reach the initial goal of the EU regulator to harmonize privacy laws across the membership countries. For an international industry, such as the online industry, this is the worst of all outcomes.
Our goal as industry partners now needs to be to openly and transparently educate the end-user about what we do if we say we “track” someone. affilinet does this for example with its Whitepaper “The affilinet tracking cookies – a deep dive” and with proactive educational speeches on trade fairs or customer events. We will continue this strategy of customer and user education on our web properties and within our social media channels. We, as an industry, need to become a very active part of the discussion around privacy and data protection in the online universe.

8. FAQ

Based on the IOC FAQ but amended by the international perspective.

Question	Answer
Will the regulators in the individual markets produce more specific guidance on what I need to do in future?	So far only the UK and NL have issued specific guidance on their recitals of the Directive and how to comply. All others who have or will implement the Directive locally will follow with detailed guidelines regarding the operational implementation. Also NL will provide more detailed guidance than in their latest FAQs (see section “Further Information”).
If browser settings in principle are seen as a valid way to gain consent, can I wait for browser settings options to be changed, so they can be used?	According to the UK’s ICO you should not wait, in all other countries we are waiting for further guidance on how to implement and whether an explanation for the user of how to use the browser setting for adjusting your privacy settings will be sufficient.
What happens if I do nothing right now?	In the UK and NL, as well as France, Austria and Spain the Directive has been put into local law. Thus it is your legal obligation to be compliant to the local regulation. It will sooner or later be implemented in all EU membership countries (potentially to a different degree of aggressiveness). Only the UK regulator so far has expressed an initial positive view towards businesses operational needs and that it will at least try to consider them in the implementation guidance. However in all other countries this has not been the case. So independent of how problematic and confusing the current situation looks, you need to find a solution that makes you compliant to the existing regulation.
Does the law apply in the same way for mobile and or tablet devices?	Yes, the requirements apply to all cookies set on any kind of device (Mobile, Tablet, Console, TV, etc.)
Can I copy the various regulator solutions?	If the local regulator issues a guidance you should of course try to stick to it. If he also publishes sample solutions regarding a technical implementation or deploys one himself, you might be able to use that too. You should probably make sure that in any case you
If we only use cookies for analytic purposes are we still required to comply with the Directive?	Yes, the directive is applicable irrespective of the type of cookies. Analytical cookies have so far not deemed “strictly necessary” by any of the local regulators. Unless that happens, you will need to treat them like any other non-strictly necessary cookies.

Further Information

affilinet Documents

- affilinet Whitepaper - “The affilinet tracking cookies – a deep dive”

The UK approach

- The revised ePrivacy Directive: What is it & what should you be doing to comply?
- The Consumer Transparency Framework (a guide for publishers to aid compliance)
- The IAB Performance Marketing Explained Website (Good to link out to)
- Launch of the ICC UK Cookie Guide (an interpretation of the law to aid compliance)

The Dutch approach

- A helpful White paper published by SOLV advocates (dissecting the status quo in NL)
- The FAQ from OPTA on the cookie regulation (the first official information from OPTA)

Contact Us If you have any questions please don’t hesitate to contact us via this email address: privacy@affili.net

About the Author

Chris R. Hauth

Director of Strategy & Corporate Development

chauth@affili.net

Joined affilinet to build its strategy team from Telefónica, where he worked in the new business and innovations department. Chris started his career as a senior consultant at Solon Management Consulting, Munich and AltmanVilandrie, Boston. At affilinet Chris is responsible for driving forward all strategic initiatives, M&A and Lobbying acrossEurope