Finding a cross-border compliance solution for cookie-based web analytics activities should be on the agenda of every company doing business online, as well as web analytics software vendors, online content publishers and online advertisers. This paper focuses on EU cookie regulations, US-based Do Not Track initiatives and other worldwide privacy initiatives, in search of a series of steps to aid us in achieving global compliance.

[Version 3.0 (April 2012)].
INDEX

1 The technical and business need for cookies
   A world built on cookies ................................................................. 5
   Cookie types and threats ............................................................... 6

2 The social dilemma ..................................................................... 9

3 A short history of worldwide cookie-related privacy protection  ....... 11

4 The EU regulatory challenge ....................................................... 15
   Opt-out vs. Opt-in ........................................................................ 15
   Yes I do, Don’t I? ........................................................................ 16
   Calling a spade a spade: national implementations ......................... 17
   Which law applies to you? ............................................................. 19

5 Technical and legal solutions for cross-border compliance of web analytics activities
   A proposed approach to the new legal framework ......................... 21
   Building a minimum common denominator .................................. 21
   Technical and practical solutions .................................................. 23

6 ANNEX: Cookie inventory and classification audit form .................. 25
Global compliance of cookie-based web analytics activities

A world built on cookies
Cookies are essential to the way the web is used today. They enable retention of information for successful shopping cart sessions, registrations and logins, online banking sessions, electronic government applications… and virtually every online action that goes beyond user-dissociated displays of information.

But cookies are also used for other purposes: by allowing us to tie multiple page visualizations to the same anonymous browser, they enable online audience measurement concepts such as “visit” and “visitor”. By statistically analyzing visits to different website sections, products or services, an online business manager is able to choose the most efficient content, format, structure or delivery options. These efforts fall under the realm of “web analytics”.

1. THE TECHNICAL AND BUSINESS NEED FOR COOKIES
1. The technical and business need for cookies

Furthermore, by analyzing visits and visitors, an online service provider is able to isolate the most successful sources in the promotion of his or her own offering, evaluate key points of failure in a checkout or registration process and make a match between, for instance, the most common search terms used by consumers and products sold. This also falls under the scope of web analytics activities.

Well beyond the service-enablement and service-optimization fields, cookie-based services have become a key building block in the evolution of Digital Marketing. Thus, for instance, an “ad server” is able to avoid displaying the same “banner ad” to a specific user more than a given number of times (thus preventing saturation), and an internal promotion on the advertiser’s home page may automatically display the design that performs best for a given traffic source out of a group of tested alternatives.

Cookie types and threats

Cookie variations have, since their creation, been extremely complex\(^1\) and we must now also consider their more sophisticated alternatives, which have been created to achieve the same objective.

“Traditional”, HTTP\(^2\) cookies (consisting of text files stored in the user’s browser file system), can be classified under two criteria: level of relationship with the end user and depth of storage. Under the former, cookies can be first-party and third-party. Whereas first-party cookies are directly served by the very website the user is visiting (this is mostly true for shopping carts, registration and web analytics), third-party cookies are linked to third-party domain names or external suppliers specialized in campaign management, behavioral targeting and personalization, but also to some web analytics services. While first-party cookies are unanimously supported, some browsers disable third-party cookies by default\(^3\).

When depth of storage is considered, cookies can be retained in a temporary (cache) browser memory, or persistently archived in the user’s file system for a defined period of time (the latter, for instance, prevents the need for repeated user logins every time a browser window is closed or a session timeout is reached).

Cookies can be replaced by alternative systems that will be considered equal under the law in terms of compliance issues (“non-traditional” cookies). These range from FlashTM: “Local Shared Objects” (available when the multimedia Flash technology is at play), to the HTML 5\(^4\): “local storage” system, which has far greater possibilities in terms of memory and life span\(^5\).

Extreme usage of cookies has come to be known as “supercookies”\(^6\) or “zombie” cookies. These consist of a combination of regular, FlashTM and HTML5 cookies, as well as database systems that allow website operators to keep track of users even after cookies have been expressly removed from the user’s file system. Although “supercookies” have so far only been found\(^7\) in conjunction with the provision of legitimate services (such as MSN.com, Hulu.com or Spotify), they are clear in breach of expected standards of transparency, depriving the end user of clear understanding about the nature of information-retention by the service provider.

Finally, so-called “spyware”\(^8\) cookies are files akin to regular cookies, which differ in that they do not respect the storage specifications determined by browsers. Whereas “spyware” cookies cannot contain programming or carry viruses (they are still flat text files), they are able to retain browser history without the user knowing about it.

---

1. Cookies first appeared in the 1994 release of Netscape browser (Internet Explorer could support cookies in late 1995). Their appearance marked a technical milestone, as it removed the major obstacle preventing the development of electronic commerce applications.

2. Hyper Text Transfer Protocol, a W3C standard which conforms to the “sustaining communications protocol” of the World Wide Web.


4. HTML stands for Hyper Text Markup Language. The various versions of this content description standard (5 being the latest) have accompanied the evolution of the web since its very inception. It is the base and standard for all resources deployed on the web (and available through a standard browser).

5. HTML 5 Local Storage can pile up to 5 MB of information, whereas Flash Local Shared Objects are limited to 100 KB and traditional HTTP cookies cannot exceed 4 KB.

6. See [http://ashikansoltani.org/docs/replay_redue.html](http://ashikansoltani.org/docs/replay_redue.html)


8. [http://tools.ietf.org/html/rfc2109](http://tools.ietf.org/html/rfc2109), determined that they would have to be either not allowed or at least not enabled by default. Although the later scenario is still in place with Safari (Apple) and Opera browsers, the IETF’s latest specification, dating from April 2011 ([http://tools.ietf.org/html/rfc6265#page-28](http://tools.ietf.org/html/rfc6265#page-28)), takes a more flexible approach.

---

5  HTML stands for Hyper Text Markup Language. The various versions of this content description standard (5 being the latest) have accompanied the evolution of the web since its very inception. It is the base and standard for all resources deployed on the web (and available through a standard browser).

5  HTML 5 Local Storage can pile up to 5 MB of information, whereas Flash Local Shared Objects are limited to 100 KB and traditional HTTP cookies cannot exceed 4 KB.

6  See [http://ashikansoltani.org/docs/replay_redue.html](http://ashikansoltani.org/docs/replay_redue.html)


8  [http://tools.ietf.org/html/rfc2109](http://tools.ietf.org/html/rfc2109), determined that they would have to be either not allowed or at least not enabled by default. Although the later scenario is still in place with Safari (Apple) and Opera browsers, the IETF’s latest specification, dating from April 2011 ([http://tools.ietf.org/html/rfc6265#page-28](http://tools.ietf.org/html/rfc6265#page-28)), takes a more flexible approach.
Global compliance of cookie-based web analytics activities

It is only natural that website users rebel against an invasion of privacy that they do not understand nor control. As online content and electronic commerce services have become more sophisticated, users may feel they are irreversibly losing control of their own personal data. Worse, in many cases individuals cannot tell how much behavioral information is being collected about them, and whether this is being tied to personally identifiable information.

Albeit countless business models are built on free services and the exchange of content for a small fraction of personal or even anonymous behavioral data (often collected by third parties in charge of monetizing advertising space), this trade-off is not always stated clearly. Furthermore, as consumers

2. The Social DILEMMA
we have become accustomed (perhaps naïvely) to accessing a large collection of resources at no cost. In this regard, some have compared websites to “private gardens” where a visitor must respect their owners’ rules if he is to enjoy the promenade.

**Websites have been compared to private gardens where a visitor must respect their owners’ rules.**

Of course, if, when entering a new “private garden” (the boundaries between separate gardens not always being so obvious), users were able to clearly understand and accept its privacy rules, they would not feel compromised. They would understand that the information would be used solely in the agreed manner, in both aggregate (anonymous) fashion and where the information identifies the user. This is called “informed consent”.

But informed consent could take many forms: Can a user not simply abandon the website if he or she does not agree with its terms? Must a specific agreement be obtained? Is such agreement the only possible evidence of sufficient prior notice of those terms? Should users bear the burden of informing themselves adequately and adapting their browsers’ preferences prior to adventuring into the unknown? In these questions lie the key differing interpretations of the international legal framework.

Privacy concerns are not contained to a particular region. However, those which have traditionally favored a culture of higher citizen tutelage and public intervention have naturally led the current trend in privacy advocacy. Cookie-related concerns have been no exception.

The World Wide Web Consortium (W3C), hosted by the Massachusetts Institute of Technology, was the cradle of the first ever self-regulatory scheme for cookies and privacy: P3P (“Platform for Privacy Preferences”), officially issued as a W3C standard through a 2002 Recommendation.

With the initial support of Microsoft, Internet Explorer 6 browser’s P3P compliance had the direct effect of preventing the permanent storage of first-party cookies, as well as...
blocking third-party cookies unless a P3P-compliant policy (in itself an XML “machine-readable” file) could be found. The standard did not succeed, and even attracted a good share of criticism from all sides.

P3P was a neither surprising nor inappropriate Internet-born response to a myriad of regional and national initiatives taking off at the very time, threatening the integrity and global appeal of the web. The main source of this concern was, without any doubt, the European Union’s regulatory framework.

The EU had first come up with its first major data protection initiative in 1995. Then, with the advent of the Internet and electronic commerce, a Recommendation “on certain minimum requirements for collecting personal data on-line” was issued by its Data Protection Working Party (“G29”) in 2001. Among other things, it clarified the manner in which the Data Protection Directive had to be applied to online activities, including data collection through online form fields, and the way compulsory information had to be made available to users. More importantly, it specifically imposed an obligation on businesses to disclose the names of companies serving third-party cookies on their website.

In 2001, an EU Recommendation sets forth the need for businesses to disclose the names of companies serving third-party cookies on their websites.

Such legislation would later be complemented by what came to be known as the E-Privacy Directive 2002, establishing legal and technical requirements on the processing of personal data in electronic environments. During the formation and voting period of the Directive an opt-in regime for cookies was discussed, threatening the imposition of a whole new system of information. In the end, it limited itself to requirements for appropriate notification of the usage and purpose of cookies, as well as the consequences of disabling them. Privacy legislation debate is not restricted to the EU but is found worldwide. In cases as recent as China’s, privacy legislation is already addressing Internet-specific concerns. In Australia, and other common law countries, it has proven hard to abandon a traditional approach to privacy and implement any policies beyond the scope of protecting citizens from government bodies.

The simple consequence of such wide coverage is that most countries will impose certain obligations on businesses that store personal data within cookies. These obligations could take the form of registration with a local agency, prior permission, notification, user access, cancellation by user request, minimum data security or ulterior usage obligations. Of course, the limits of “personal data” or “personally identifiable information” vary across countries (eg. a simple IP address would be sufficient to qualify in Germany).

What had never been seen, until the E-Privacy Directive arrived, is a piece of legislation that applied to a particular set of data processing practices, independent of whether those practices involved the storage of personal information. In this regard the E-Privacy Directive was alone, until Do Not Track appeared in the United States.

Canada (as it also follows civil law and boasts the most comprehensive personal data protection legislation in the country).
What had never been seen is a piece of legislation that applies to a particular set of data processing practices, independent of whether those practices involve the storage of personal information.

Run by Stanford University academics in California, the Do Not Track initiative aimed to provide a technical and legal solution which replicated the idea of the “do not call” list, which prevents unsolicited commercial communications over the phone. Once a user has installed a Do Not Track plug-in in his browser, websites that comply with the initiative would be prevented from serving cookies. Of course the problem with self-regulation is that it requires mass adoption if it is to be effective on a large scale.

Do Not Track received a serious boost in December 2010, when the United States Federal Trade Commission decided to endorse24 the initiative. By April 2011, Internet Explorer 9, Firefox 4 and Apple Safari were already supporting it. At that point Google Chrome was singled out by the FTC as the only browser lagging behind25.

On top of this, the United States may be heading for its own piece of legislation on the subject, with current plans by House Representative Cliff Stearns to introduce legal provisions that would be enforced by the FTC along with Do Not Track (based on the existing Consumer Privacy Protection Act26).

25 See http://www.wired.com/epicenter/2011/04/chrome-do-not-track/. Google has released its own technical solution to ensure the implementation of an opt-out approach: Google Chrome’s Keep My Opt-Outs plug-in blocks targeted ads produced by a group of companies and ad networks that have decided to abide by this scheme.

4. The EU Regulatory CHALLENGE

EU amended the E-Privacy Directive in 200927 to address the need for permission when cookies are served or read. Specifically, under article 5 (3)’s new wording, users must be provided with “clear and comprehensive information” about the storage of information, or access to stored information, on their terminal equipment, and users must provide their specific consent.

An exception to this requirement is provided by the article itself- 5(3).


Opt-out vs. Opt-in
Moved by fresh social concerns in light of new technical and business developments (see chapter 1), the
as amended: “permission will not be required when cookies are deemed strictly necessary to the operation of the services.” This concept has proved controversial: Does “operation” mean “service-enablement”? Does it rather encompass “service-optimization”? Whereas the former would only include those cookies used in shopping carts or registered sessions, the latter would be wide enough to include web analytics, commonplace maintenance tasks and non-crucial cookie-based features (such as remembering a language selection or geographical location).

4. The EU regulatory challenge

Office has expressly discarded the UK’s Information Commissioner’s differed across countries. While the interpretation of this exception has as amended: “permission will not be required when cookies are deemed strictly necessary to the operation of the services.” This concept has proved controversial: Does “operation” mean “service-enablement”? Does it rather encompass “service-optimization”? Whereas the former would only include those cookies used in shopping carts or registered sessions, the latter would be wide enough to include web analytics, commonplace maintenance tasks and non-crucial cookie-based features (such as remembering a language selection or geographical location).

While the UK’s competent body has expressly discarded the inclusion of web analytics activities, France’s equivalent body has done the opposite.

Yes I do, Don’t I?

Much has been written about the extent of the consent required. In light of a recent Opinion issued by the EU Data Protection Working Party30 (“G29”): when dealing with online behavioral advertising (built on third party cookies), appropriate consent cannot be assumed to have been given where users are operating within browsers which provide options for disabling cookies (where these have not been disabled). Instead, consent would require a specific “positive” action on the part of the individual.

On the other hand, the EU Commission Communications Committee, which was set up to advise Member States on the Directive’s implementation, has suggested that browser settings or other application settings could be sufficient as a form of consent. For this reason, browser manufacturers have now been dragged into discussions with national authorities.

The former line of thought inspired the initial interpretation of the new rules by the UK’s ICO31. According to it, express permission requests would need to be made every time a new cookie is served. To demonstrate how this solution could be deployed successfully, the ICO applied to its own website. Sharing its impact on the website’s unique visitor count (90% drop)32 has had a very discouraging effect on industry professionals, prompting widespread talk of a complete disconnection between the policy and the reality of business.

Unfortunately, express permission at website level can only be obtained through pop-ups or graphical alerts that prevent the user from making progress on whatever tasks he has chosen to complete online. This goes directly against all usability and user-centered design principles33. As there are no half-way solutions and this seems a high price to pay, making a more precise distinction between different levels of intrusiveness prior to seriously hampering the very purpose of an online service would be sensible. Discussion of this distinction will follow.

Calling a spade a spade: national implementations

Of course, speculation on the Directive’s general terms is useless when the 27 EU members were obliged to implement it into specific national law by June 2011. After much feet dragging, things have started to settle down in the past few months, with the one-year moratory in its application

Permission to read or write cookies will not be required when cookies are deemed strictly necessary for the operation of the services

As was rightly feared, the interpretation of this exception has differed across countries. While the UK’s Information Commissioner’s Office has expressly discarded the inclusion of web analytics activities28, from the outset, France’s equivalent body 29 has done the opposite.

---

29 The Commission Nationale de l’Informatique et des Libertés (“CNIL”)
31 Through its guidance paper on the new framework for cookies (see http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/new_regulations.aspx), even providing as examples the use of specific text displayed to users, either in pop-ups, footers or elsewhere.
32 See The ICO’s response to a public request by our Digital Analytics Association colleague Vicky Brock, referenced IRQ0357602 (“I would like to request information regarding to the recorded levels of traffic to the ICO website before and after the cookie opt in message was placed on the ICO website.”) http://www.ico.gov.uk/about_us/how_we_comply/delivery_log/201106.aspx. A full account can also be found here: http://www.research-live.com/news/analytics/cookie-refusal-leads-to-90-drop-in-measured-unique-visits-to-ico-site/4005538
33 Vid. KRUG, Steve “Don’t make me think”, Que, 2000.
coming to an end in the United Kingdom and the arrival of national implementations in other countries. In particular, the United Kingdom has been rich in developments, with two of them particularly significant: Both ICO’s “Guidelines on the new cookies regulations” and the Government Digital Service’s “Implementer Guide to the Privacy and Electronic Communications Regulations for public sector websites” providing useful frameworks. The following important conclusions can be drawn from a review of both documents:

• A criterion of intrusiveness is gaining ground, allowing websites to classify cookies into separate groups.

• Web Analytics activities and other first-party cookie uses are not considered a priority in the enforcement of prior permission requirements.

• Government websites in the United Kingdom are not expressly requiring permission when analytical cookies are in use.

Spain’s recently enacted law brings another perspective, with an additional element thrown into the mix: According to its newly enacted law, permission can be validly obtained through browser settings, albeit it must involve a positive action on the part of the user (through an initial wizard during installation or upgrade). This throws some hope into the future, although it is not enough to alleviate today’s needs.

At the more lenient end of the spectrum, we can find other countries that have now implemented legal changes: The Czech Republic, Finland, Hungary, Ireland and Sweden are all either expressing a “soft consent” based on appropriate notices (in many ways akin to an “opt-out”) or allowing acceptance through browser settings without further considerations.

**Which law applies to you?**

Unlike other EU legislation, which applies the national law of the end user’s physical location, the legal framework of personal data protection is based instead on the national law where the service provider is established or, if located outside of the EEA (EU plus Norway, Liechtenstein and Iceland), based on the national law of the nation where the service provider hosts its personal data storage hardware (data processing “equipment”). However, since cookies make use of the end user’s personal computer for storage purposes, the Communications committee has interpreted them as data storage facilities operated by the service providers. This interpretation would mean that any EU country could see its national law applied to a website run by a U.S., Australian or Indonesian company (unless access is blocked for residents of said country).

Where applicable laws conflict, we assume that enforcement rationale would determine the action taken against any violation of legislation. Albeit any company could be potentially sued by end users in any other country, a website operator is mainly at risk in the countries where it is headquartered or domiciled due to the difficulty of enforcing compliance and distributing punishments. Of course, for non-EU multinational companies with offices throughout the EU this would mean having to comply with up to 27 different laws.

Non-EU multinational companies with offices throughout the EU would have to comply with up to 27 different laws.
5. TECHNICAL and LEGAL SOLUTIONS for CROSS-BORDER COMPLIANCE of Web Analytics Activities

A proposed approach to the new legal framework
Although the climate remains uncertain, with many national laws pending enactment, and a majority of data protection agencies struggling to cope with the technical implications of the Directive, we will now summarize a website operator's current options for the definition of a minimum common denominator to safeguard against the different national laws involved.

Building a minimum common denominator
A number of sources set precedent and can act as guidelines for the said minimum standard:

- Guidelines issued by those countries which have already implemented the EU Directive into national law
- Recommendations of the EU Communications Committee
- Opinions of the EU Data Protection Working Party (“G29”)
- Recitals to the new ePrivacy Directive
- The United States FTC report on Do Not Track38.

---

It is by looking at these that we can reach the following conclusions:

- A classification of cookies based on their level of intrusiveness would assist in communicating with website users, aiding the explanation of the need for permission in certain cases.

- Both the US FTC and local EU data protection agencies will most likely begin taking action against companies that purposefully disregard the new laws. A second priority would be targeting website operators that do not make any attempt to comply (as recognized by ICO).

- Given the fact that the EU G29’s Opinion on Behavioral Advertising has been a key precedent for the new framework, we must pay special attention to the fact that third-party cookie-based affiliate networks and ad networks represent its most important target. As a consequence, any cookie-based activity that stems from the very same website requested by the end user (and not undertaken behind the scenes and involving third parties) should at the very least attract less scrutiny.

As this differentiation must also be obvious at the technical level (especially if Do Not Track browser plugins become commonplace), an effort to stick to first-party cookies for web analytics activities would undoubtedly help the website operator’s cause. This is further supported by the only recital to the new ePrivacy Directive (recital 66) that expressly goes into detail in the explanation of the intended goal of the new provisions, as only third-party relationships are mentioned.

- Many web analytics vendors offer their own opt-out plugins and options. A link to them can be easily given within the website’s privacy policy disclaimer or legal notice.

- It is easier to prove positive actions towards compliance than to defend an unchanged policy on the basis that everybody else is failing to act.

Technical and practical solutions

With those conclusions in mind, we propose four steps that would ensure compliance with the minimum common denominator defined above. These steps are consistent with existing national guidelines, while remaining essentially practical and aiming at causing only a minimal disruption to the provision of online services:

1. **Cookie audit.** Run an audit of all persistent cookies being used throughout the company’s digital properties, recording basic information about each of them: expiration term (life of the cookie), purpose (e.g.: internal analytics), level of intrusiveness and owner. A sample audit form is provided in the Annex to this document, while a variety of free tools remain available for its fulfillment.

2. **Cookie management policy.** Establish some basic rules for the regular supervision of cookies being used, aiming at reducing their number or, where possible, their expiration term.

3. **Privacy notice update.** Redraft your privacy notice including separate sections for:

   a) Analytical cookies
   b) Other internal usage cookies
   c) Social plugin cookies
   d) Cookies run and used by third parties
   e) A summary table with the results of your cookie audit.

All these sections can be grouped under “Cookies” and precede or follow preexisting notices regarding the collection of personal data (with the new section labeled “Privacy and Cookies”). Also, the link to this policy should gain prominence if not obvious at first sight.

4. **Opt-out compliance:** Make sure that your website can comply with Do Not Track browser plugins and, if possible, include a first-visit only header notice that lets the user choose whether to exclude your own cookies without the need to revert to browser plugin settings.

**NOTE:** These recommendations are by no means intended to replace qualified legal advice.
### 6. ANNEX: Cookie inventory and classification audit form

<table>
<thead>
<tr>
<th>COOKIE</th>
<th>DURATION</th>
<th>PURPOSE</th>
<th>INTRUSIVENESS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About Divisadero

Divisadero is a Digital Analytics and Online Business Advisory Services company. With a 40-strong multidisciplinary team distributed across Europe and Latin America, Divisadero works with multiple Fortune 500 companies, including: Vodafone, Heineken, Mango, Santander, BBVA, ING Direct, Coca-Cola, AXA, NH Hotels, Barclays Bank, Yell, Vueling or Iberdrola.

www.divisadero.eu

About the author

Sergio Maldonado holds an LLM (Merit) in IT and Internet Law from Queen Mary’s University (University of London), and a law degree (JD) from the University of the Basque Country (Spain). He also holds various business, computer programming and web analytics certifications. Initially trained as a lawyer in California and admitted to practice in both England & Wales and Spain, Sergio is co-author of “Internet, key business legal issues” (Spanish language, Thomson-Aranzadi, 2002) and author of “Web Analytics, Measure to triumph” (Spanish language, ESIC University Publishing, 2010). He is also a guest professor at ESIC Business School and a regular speaker at international Digital Marketing events (WSAB London, eMetrics San Francisco, eMetrics Washington D.C., WAW Beijing, OMExpo Madrid, ESEADE Buenos Aires, IMC Barcelona) Sergio is the founder of Divisadero/ MVConsultoria, which he has run since 2006.