

## Cookies and Trackers: Inventorying and Analyzing Your Cookie Practices

The European Union continues to change the face of privacy rights and thereby the obligations of organizations that process personal information and otherwise interact with people. In 2009, the European Union updated its directive related to privacy and electronic communications, mandating that website operators not only to provide notice to website users when cookies are used, but also to seek consent unless the cookies are “strictly necessary” to provide the service. For example, cookies for shopping carts, authentication, and fraud protection are generally deemed necessary, whereas those for advertising and analytics are not.

The so-called “Cookie Directive” requires the member nations of the European Union to enact and enforce laws to meet this requirement, and we began seeing rules and guidance being established at the national level in 2011. By the end of 2011, however, not all countries had enacted rules and those that did lacked harmony in the associated guidance. In addition, the data protection authorities, granting grace periods for implementation, have not yet begun to enforce the rules.

The Cookie Directive certainly significantly changes the online privacy rules, but organizations had already been losing control and accountability over their use of cookies and other tracking techniques on their websites. Increasingly complex websites, lack of central management of online analytics, and new breeds of tools (e.g., active content such as scripts, ETags, local storage objects) often result in a rather chaotic environment across an organization’s web properties. With the enforcement of the Cookie Directive looming, and other general online privacy rules already in effect, it is a good time to understand the use of cookies and trackers and to bring order to the chaos.

### Tools

There is no single tool that fully automates the task of inventorying and analyzing cookies and other tracking techniques used on a website. Rather, a combination of tools is needed to identify, catalog, and inspect those objects. Some organizations may employ website compliance monitoring services, but most do not have suitable capabilities in place.

Athena uses a combination of add-ons to standard browsers to support the discovery and cataloging of these objects. We rely primarily on the Mozilla Firefox browser with cookie management and export add-ons to help us view cookies and to extract them from the browser into reports. We also use an HTTP header viewer add-on so that we can review the exchange of HTTP headers between the browser and website, including where cookies are set and read and where ETags are used. We also use the iPerceptions Web Analytics Solution Profiler to catalog the use of third party scripts and other active content encountered. Ghostery is used as a further check by which we can validate the completeness of our identification of the analytics and tracking scripts and other active content. Finally, we set the permissions on Adobe Flash Player to inform us of attempts to write Flash-oriented local stored objects to our devices.

#### **Our Standard-issue Toolset**

- Mozilla’s Firefox with the following add-ons:
  - Cookies Manager+
  - Cookie Exporter
  - LiveHTTPheaders
  - Ghostery
  - Collusion (beta)
  - Web Analytics Solution Profiler

## Approach

Although it is not uncommon for websites to have thousands, if not millions of pages, we prefer to manually interact with the websites for much of the discovery and analysis of cookies and trackers. Our goal is to interact with the website as a human user would, and to understand how the different interactions may result in various encounters with the cookies and trackers. For example, we would browse, subscribe, register, login, logout, manage accounts, shop, and otherwise use the website to encounter cookies and trackers as a human user would. In general it is sufficient to identify the primary set of cookies and trackers encountered, but in some cases we will create a checkpoint after key actions, such as identify cookies after login or after logout.

We simultaneously capture HTTP headers so that we can further correlate the headers with the set cookie and read cookie events. This enables us to have visibility into the use of other HTTP techniques such as ETags.

We also browse with the Web Analytics Solution Profiler enabled to identify and catalog third party scripts and other active content, some of which may be associated with cookies already detected, but others may not be directly associated with any cookies.

## Cookie Analysis

In general, we catalog cookies according to the following parameters.

<b>Name</b>	The name assigned to the cookie.
<b>Domain and Path</b>	The web domain, website, and path within the website in which the cookie is used.
<b>Sample Contents</b>	Representative content in the data field.
<b>Secure</b>	Whether the cookie is set as "Secure". A secure cookie will be sent by the browser to the website only during secure HTTP sessions.
<b>Expiration</b>	The expiration date and time assigned to the cookie if it persists, or an indication that the cookie is a session cookie.

We further analyze the cookies regarding the following characteristics:

<b>Purpose</b>	Identify the purpose or purposes of the cookie. Determine if the cookie otherwise has an appropriate and non-obsolete purpose. Understanding the purpose is a key step to dealing with the Cookie Directive when working through methods of achieving consent for cookie use. We might recommend renaming cookies to be more aligned to their intended purpose.
<b>Strictly Necessary</b>	Determine if the cookie is strictly necessary for the service requested by the user. This is a strong standard; being an important cookie is not the same as being strictly necessary. If the cookie is not strictly necessary, then consent of the user will be required for operations involving European Union users.
<b>Responsible Party</b>	Determine whether the cookie is a first party cookie (i.e., set in the domain of the website) or a third party cookie (i.e., set in another domain). It is important, however, to identify the legal entity responsible for the cookie at this stage.
<b>Excessive Path</b>	Determine if the domain, website, and path appropriate for the intended use of the cookie. Cookies can be constrained so that they are set and read only where needed.
<b>Inappropriate Contents</b>	Determine if the contents includes plaintext personal or otherwise confidential information, such as a user name, email address, IP address, or other user specific codes. In general, plaintext confidential information should not be in the data field, and the data that is contained should be specifically protected to thwart replay and cookie poisoning, among other forms of cookie-based attacks.
<b>Secure</b>	Determine if the cookie should be set as secure. A cookie could be set as secure if it is intended to only be used through secure sessions with the website.
<b>Appropriate Lifetime</b>	Determine if the cookie expiration represents an appropriate lifetime related to its purpose. Session cookies will expire at the end of the session or when the browser closes. Persistent cookies may not expire for hours, months, years, or decades depending on the setting.

Using the Web Analytics Solution Profiler add-on to Firefox, we also identify the following characteristics of the third party scripts and other active content that it detects:

<b>Location</b>	The URL on which the object was located on the website.
<b>Page Name</b>	The natural language name given to the page where the object was located.
<b>Service Provider</b>	The name of the service provider and when known the specific service involved with the object.
<b>Tracking Object</b>	The URL to which the object refers.

Normally, a list of the third parties whose scripts and trackers used, including some representative entries, is sufficient for the purposes of cataloging and analyzing the use of these services on a website. Although some of the services encountered may operate without cookies, their presence will affect the overall privacy approach a website operator takes.

## Next Steps

The inventory and analysis of cookies is just the first step. Next steps to be considered include the following:

- ❑ **Cleaning up the cookies in use.** The inventory and analysis can be used to identify cookies no longer needed and cookies whose contents or use warrant tailoring.
- ❑ **Establishing a suitable consent mechanism.** For websites that must comply with European national data protection law, the means to solicit and receive consent of the user will need to be established. Although none of the methods shown in the guidance are directly appealing to website operators, an approach or set of approaches will be needed to comply.
- ❑ **Revising the privacy statement.** Although the revision to the cookies is the first step, a review of the privacy statement for the website is also warranted. The privacy statement should be revised as needed to precisely characterize the use of first and third party cookies, and to describe the consent mechanisms available. This revision may also affect information previously collected through cookies; if the changes are significant, notification to users may be warranted.

Although the Cookie Directive is a good reason to inventory and analyze the cookies used on your website, organizations without European operations will also benefit from increasing their understanding of cookies and improving their practices related to cookie use across their websites.

## References

In addition to the references indicated in the text, the following provide guidance related to cookies and the Cookie Directive.

- ❑ **European Parliament and Council**, “Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws” <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF>, November 2009.
- ❑ **European Commission, Article 29 Working Party**, “Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising”, [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf), December 2011.

- ❑ **République Française Commission Nationale de l'Informatique et des Libertés (CNIL)**, “Ce que le "Paquet Télécom" change pour les cookies”, <http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/>, October 2011.
- ❑ **United Kingdom Information Commissioner's Office (ICO)**, “Guidance on the rules on use of cookies and similar technologies”, [http://www.ico.gov.uk/news/latest\\_news/2011/~media/documents/library/Privacy\\_and\\_electronic/Practical\\_application/guidance\\_on\\_the\\_new\\_cookies\\_regulations.ashx](http://www.ico.gov.uk/news/latest_news/2011/~media/documents/library/Privacy_and_electronic/Practical_application/guidance_on_the_new_cookies_regulations.ashx), December 2011.
- ❑ **European National and Information Security Agency (ENISA)**, “Bittersweet cookies. Some security and privacy considerations”, [http://www.enisa.europa.eu/act/it/library/pp/cookies/at\\_download/fullReport](http://www.enisa.europa.eu/act/it/library/pp/cookies/at_download/fullReport), February 2011.