THE CRUX OF COOKIES CONSENT: A LEGAL AND TECHNICAL ANALYSIS OF SHORTCOMMINGS OF COOKIE POLICIES IN THE AGE OF THE GDPR

Gerhard Seuchter / Sabine Proßnegg / Veronika Beimrohr / Dawn Branley-Bell

Senior Lecturer, FH JOANNEUM University of Applied Sciences, Department of Applied Computer Sciences, Werk-VI-Straße 46, 8605 Kapfenberg, Gerhard.Seuchter@fh-joanneum.at

Senior Lecturer, FH JOANNEUM University of Applied Sciences, Department of Applied Computer Sciences, Werk-VI-Straße 46, 8605 Kapfenberg, Sabine.Prossnegg@fh-joanneum.at

Legal Advisor, FH JOANNEUM University of Applied Sciences, Personnel and Legal Services, Alte Poststraße 147, 8020 Graz, Veronika.Beimrohr@fh-joanneum.at

Research Associate, Northumbria University, Department of Psychology, Northumbria University, Newcastle upon Tyne, NE1 8ST, UK, dawn.branley-bell@northumbria.ac.u

Keywords: ***Cookies, Data Privacy, Profiling, Dark Patterns, GDPR***

Abstract: *EU legislation such as the ePrivacy Regulation and the GDPR impose a variety of obligations on how browser cookies need to be implemented on web pages. While almost all website operators adhere to the letter of the law, many websites fail to uphold the spirit of the law. Website operators may nudge visitors into accepting superfluous cookies by carefully crafting cookie popups; thus impinging on visitors' right to self-determination of their data. The authors propose to define a machine-readable representation for cookie policies. This representation can then be used to present the cookie policy to website visitors in a standardized manner, thus reducing the potential for deceptive cookie policies.*

1. Introduction

Cookies are an essential part of modern websites. However, the average user often has limited understanding about what cookies really are; including why some cookies are needed and others are not, and the privacy implications. The following section will cover the technical groundwork on how cookies work and their necessity for the modern web. After that some legal issues will be addressed.

1.1. Cookies

In the early 90s when the world wide web was envisioned it was primarily designed as a document retrieval system with a novel approach of so-called hyperlinks, allowing the user to navigate between documents. An end-user would retrieve a document from a server, the document would then be rendered by a program running on the user's computer called a «browser». The protocol to request and transmit the document is called the HTTP (Hyper Text Transfer Protocol). However, this simple approach for serving interlinked documents was soon found to be lacking during the commercialization of the world wide web in the late 90's. The problem with the HTTP protocol is that the web server cannot correlate requests from the same client or more technical: HTTP is a stateless protocol. For example, a web browser cannot determine if the user has already visited the page before. Without such correlation (of individual visits to the webpage), it is difficult to implement use cases for e-commerce such as shopping carts, in which the server must be able to distinguish between different users and serve different functions and/or present different contexts dependent upon the user.

Further examples are personalised website recommendations, where the site suggests additional items to the user based upon previously purchased or viewed items. In order to implement this functionality (without the need for a user account) the website needs to know which article i.e. webpages the user has visited previously.

A cookie itself is nothing more than a short text fragment (identifier) which is initially sent from the server to the browser (or client). The browser will repeat the text fragment on each subsequent call to the server. Since the identifier was generated by the server, the browser will include the text fragment in each subsequent call to the server enabling the server to correlate requests, i.e., visits.

Cookies were first implemented as a proprietary browser extension in 1995[1] and formality standardized in 1996 as RFC2109[2] by the Internet Engineering Taskforce. Ever since their inception cookies have been a divisive issue in regard to data privacy versus e-commerce. The first ever public discourse about the potential danger of cookies has been sparked by the article «This bug in your PC is a smart Cookie»[3] by the Financial Times in 1996.

1.2. Anatomy of Cookies

The cookie standard has gone through major revisions over time; however, the basic principles and structure have stayed the same. In its most basic form, a cookie is a simple key value pair, consisting out of a name and a value (e.g., **SessionID=a5EOokRDjSlknbn35EOZ**).

However, the following optional values are also often set for cookies:

1. **Expiration Date**: Date after which the cookie should be deleted by the browser. The browser can also delete cookies before their specified expiration time for privacy reasons or due to memory restrictions/ limitations.
2. **Domain**: The browser sends cookie data only to the server which originally set the cookie. However, the domain property enables the server to also share the cookie with subdomains within its own server.

The followings snippets show an excerpt of the communication between the client (browser) and the web server.

```
HTTP/1.0 200 OK
Set-Cookie: SessionID=a5EOokRDjSlknbn35EOZ; expires=Thu, 27-Feb-2020
9:00:42 GMT;domain=example.com
```

Figure 1: Response from the server to the client to store Cookie with the name «SessionID»

The first line indicates the beginning of a HTTP response from the server to client, the response code 200 indicates that the server could successfully fulfill the request from the client. Before the server sends the actual content of the web pages, several HTTP headers are transmitted to the client first. HTTP header contain meta information about the content such as size content type and also which cookie data should be included in the subsequent calls. The HTTP header[4] Set-Cookie defines a new cookie with name SessionId, an expiration date and also specifies that the cookie is valid for all subdomains of example.com.

In each following request to the domain example.com (and all its subdomains) the following cookie data will be included:

[1] Montulli, Persistent client state in a hypertext transfer protocol based client-server system, US Patent 5774670, 1996.
[2] Kristol/Montulli, HTTP State Management Mechanism, RFC Editor, 1997.
[3] T. Jackson, «This bug in your PC is a smart Cookie», Financial Times (Feb. 12. 1996).
[4] HTTP headers are essentially simple key values pairs delimited by a colon, e.g., *«Content-Language: en-US»*.

```
GET /shopping-cart.html HTTP/1.1
Host: www.example.org
Cookie: SessionID=a5EOokRDjSlknbn35EOZ
```

Figure 2: Cookie data included by each request to the server after the cookie was set

Each HTTP request starts with a verb i.e. the action the browser wants to perform. The verb *GET* indicates that the browser wants to retrieve a document from the server, in this case a document with the name shopping-cart.html. When a browser performs HTTP requests, it also includes HTTP headers as a way to send requests for meta data to the server. Since the cookie has been previously accepted, all requests to the server will now include the cookie *SessionID*. In our example the value of the cookie is just a random string which the web server can now use to correlate requests from the same user.

1.3. First and third party cookies

The technical introduction has shown that cookie data are only sent to the domain, or subdomain(s), from which they originated from. Generally, it is reasonable to assume that the domain and subdomain(s), e.g., *example.com* and *shop.example.com* are controlled by the same entity. This is known as a first party cookie. These cookies are generally used for remembering user preferences (e.g. language settings) and helping to deliver a «better» (i.e., user-specific) experience by keeping consistency between multiple visits to the same website by an individual user. However, through various technological workarounds it has become possible to create cookies which are not only valid for the original domain but also for a third-party domain. For example, if a user visits *example.com*, a cookie for a completely different domain would be set such as *analytics.third-party.com*. In order for third party cookies to work, the operator of the original website must add a special code to their website. If a third party convinces many site operators to include its cookies, it becomes possible for that party to track the activity of users over different sites. This is possible because many website operators include small code fragments from tracking companies into their webpage. With the aid of third-party cookies these tracking companies can create a profile of when a user visits a web page, since each time the code fragment is loaded the cookie is also sent to the tracking company

There are many business cases which require third party cookies, the following is a non-exhaustive list of the most common ones:[5]

– **Targeted Advertisements**: There are a multitude of different advertisement business cases, which involve cookies. Nevertheless, the basic premise is that advertisers want to know about their target audience in order to show more effective ads. This practice of targeted advertisement needs to track the websites a user visits over a certain period of time in order to make an assessment about the target demographic. The ability to track user activity across multiple sites, allows businesses and websites to retarget customers by showing adverts more suited to the sites that they know the user has been visiting.[6]
– **Analytics**: Third party analytics services allow the operator of a website to gain better insights into how visitors use their site. Strictly speaking analytics services do not require a third-party cookie, however it is often easier for a website provider to outsource the analytics to a third party. The amount of data collection performed by third party analytics depends on the business model of the company. Free analytics solution often tracks the same user over different websites while paid analytics services only collect simple telemetry of user behavior on a single website.

5 Cf. Mayer/Mitchel, Third-Party Web Tracking: Policy and Technology, IEEE Symposium on Security and Privacy, 2012, P 419.
6 Cf. Sharp, Retargeting vs. Remarketing – What's the Difference?, Awin, https://www.awin.com/gb/affiliate-marketing/retargeting-vs-remarketing (accessed 29th Oct 2019).

– **Social Media Integration**: In order to increase customer engagement many site operators embed functionalities from social networks such as Facebook and Twitter into their page. By embedding these functionalities operators of social networks place third party cookies on the site for authentication and also analytics purposes. Also social media companies use this approach to track people which are not even part of their social media platform for advertisement purposes.

Third party cookies (sometimes referred to as «tracking cookies»[7]) have been at the core of many privacy debates, as it is often not clear to the user that they are accepting third party cookies and/or how these cookies are being used. For example, many Facebook users do not realize that the social networking site uses third party cookies to track their use of other websites. For example, if a user clicks on a link or advert on Facebook that subsequently directs them to an external website, Facebook can subsequently track their activity on that site via a third-party cookie.[8] Controversies over privacy have led to software and browsers allowing users to block third party cookies. However, there are workarounds starting to appear by marketing and businesses, for example Facebook has recently introduced an expansion to its current system of third-party cookies which uses first party cookies for «third-party reasons», i.e., advertising and marketing.[9]

2. Legal aspects

Cookies first came into the focus of Union legislation in 2002, when the ePrivacy Directive[10] was introduced. Article 5 (3) ePrivacy Directive which is the provision concerning the usage of cookies was subsequently amended in 2009.[11]

The ePrivacy Directive does not define cookies or the underlying technology and thus its Article 5(3) is not limited in scope to this particular technology: The provision governs two actions: **the storing of information** and the gaining of **access to information** already stored in the terminal user's equipment via the use of electronic communications networks. This technical storage or access shall be permitted provided that the user consented in accordance with Directive 95/46/EC[12] which the user can only do after having received clear and comprehensive information as to the purposes of the data processing. However, this consent requirement shall not prevent storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by that user.

Directive 2009/136/EC which replaced the users negative right to refuse with the consent requirement laid down today, notes in Recital 66 that this storage and/or access may happen «*for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses)*», referring to the danger cookies may pose to users' right to privacy and the right to confidentiality.

---

7 Cf. Wlosik/Sweeny, What's the Difference Between First-Party and Third-Party Cookies?, Clearcode S.A., https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/ (accessed 29th Oct 2019).

8 Cf. Doucette, First Party Versus Third Party Cookies for Facebook Advertising, Ethoseo, LLC., https://www.ethoseo.com/blog/first-party-versus-third-party-cookies-for-facebook-advertising (accessed 29th Oct 2019).

9 Flynn, WTF are Facebook's first-party cookies for pixel?, Digiday, https://digiday.com/marketing/wtf-what-are-facebooks-first-party-cookies-pixel/ (accessed 29th Oct 2019).

10 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 2002/201, 37.

11 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, OJ L 2009/337, 11.

12 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data – OJ L 1995/281 p 31.

Even though this consent requirement is more than ten years old it has come into renewed focus due to the GDPR and the very recent ECJ case «Verbraucherzentrale Bundesverband eV»[13]. The German Federal Court of Justice raised the question to the ECJ, whether pre-checked checkboxes represent a valid method to obtain consent under Union law.[14] The ECJ first ruled that along with the Data Protection Directive, the GDPR was also applicable in determining the validity of the consent.[15] The ECJ formulated three requirements for a valid consent, namely that the consent needs to be active[16], that the requirements of consent are the same for the processing of personal and non-personal data[17] and finally, that the information requirements laid down in Article 13 GDPR are applicable[18].

This ECJ decision means that the already cumbersome nature of cookie consent has just become more cumbersome: even more information needs to be provided, not only on the purposes for the processing, but also all the information required by Article 13 GDPR.[19] Recital 60 of the GDPR offers a possible solution, namely that information may be provided *in combination* with standardized icons that are machine-readable. The use of the terms «*in combination*» is crucial; solely providing information *or* standardized icons are not sufficient, both must be present.

2.1. Current implementation

If a website operator uses cookies which are not strictly needed for the functionality of a website then consent from the user is required. The operator is only allowed to send the cookies after consent has been given by the visitor of the webpage.

The current technical implementation of this legal requirement manifests itself in so called «Popups» which block access to the site until the user reviews and accepts the cookie policy. Depending on the implementation by the website operator the user can, in some cases, control which cookies he or she wants to accept prior to consenting to the policy. This is usually implemented as a set of checkboxes allowing the user to select which cookies to accept and reject.

2.2. Implementation Issues

According to Article 7 para. 1 of the GDPR[20] it is required that if data is processed based on consent a stored record of said consent should be kept. Article 7 para. 3 further stipulates that given consent can also be withdrawn by the data subject at any time. These legal requirements raise some interesting technical issues when implementing GDPR cookie handling.

Browsers are not aware of legal requirements and generally store cookies without user intervention. As a consequence, the whole process of only sending cookies to clients (meaning user) after obtaining consent is solely controlled by the website operator. It is the responsibility of the data controller to adhere to the obligation.[21] However, even if a website operator acts in good faith there is potential for accidentally sending cookie data before obtaining the user's consent. Simple changes to the website like adding a new component e.g. social network integration could lead to the premature transmission of cookies to the user. As was previously

13 ECJ 1.10.2019 C-673/17.
14 Ibid, para. 37.
15 Ibid, para. 43.
16 Ibid., para 62.
17 Ibid., para 71.
18 Ibid., para 76 ff.
19 Depending on the nature of the processing and counting method up to 27 information fields.
20 The applicability of this provision is a given when personal data is processed, as was the case in Verbraucherzentrale Bundesverband eV (see para. 45; 67). The following discussion of this issue presupposes that the cookie processing involves personal data.
21 See Art. 24 GDPR, data controller and website operator might not be the same entity but it is assumed in this case.

discussed, cookies are primarily managed by the browser. Although web standards like RFC 6265[22] define the general behavior to which the browser needs to adhere to, it is the browser's discretion to reject cookies.

The requirement that consent can be withdrawn at any time also makes a strong case to support the browser implementing cookie consent handling. Since the lifetime of cookies, i.e. their expiration, is also managed by the browser, it should be the browser that removes the cookies after withdrawal of consent. The usage of third-party cookies further complicates the issue, since site operators cannot delete third-party cookies themselves.[23] This implies that even if consent is withdrawn the cookies still remain on the user's computer. It is then the responsibility of the third party and the website operator to stop the processing of such cookie data, although the data is still present and also still gets sent to third parties.

Again, we can make a case that cookies should be managed by the browser and not the website itself. Removing cookies upon the withdrawal of consent would also remove the technical means by which cookie data can be used to track people. Of course, this would not delete already collected information by third parties, however, at least further collection of data could be prevented.

2.3. Coercing users into giving consent

Article 4 para. 11 GDPR defines consent that the consent is given freely, informed and unambiguously by a clear affirmative action. The GDPR is designed to give the user a high degree of self-determination in regard to how their data is collected and stored. However, said freedom directly conflicts with the business interests of certain website operators, who sell analytics and advertisement data in order to increase revenue.[24] Therefore, companies are often heavily invested in obtaining consent from the user for third party cookies.

The term «dark pattern» was first coined by the user experience (UX) researcher Harry Brignull and describes user interfaces that are designed to manipulate users into actions, which are not necessarily in their best interests.[25] The psychological and behavioural economics literature demonstrates how subtle design changes and «nudges» can be used to influence users' behaviour. There are many ways in which behavioural nudges can be implemented to increase the likelihood of users accepting cookies[26], e.g.:

- Making the option to decline cookies difficult to locate compared to a very accessible, highly visible «accept» button. Research shows that users will often choose the quickest, most convenient option (in this instance deliberately designed to be the «accept cookies» option).
- Asking users to log in to access a website, e.g., «login using your Google account», «login via Facebook» – this allows the domains to use third party cookies to track the users activity on the site but again the option to «skip» the option to «log in» is hidden. Again, these options are made appealing to the user through their convenience (i.e. the user just has to click the «login button» and not complete a form). These login options often include sharing the user's personal information such as their e-mail address, friends list, and location (etc.) obtained from the social media site, with the website that they are attempting to access.
- Making cookie and privacy information complex and lengthy, to discourage users from reading this information. Even usually privacy-conscious users may opt not to read due to various reasons including fatigue from information on every single site they visit, time constraints, lack of understanding or, again, convenience.

[22] Request for Comment.

[23] Cf. Barth, RFC6265: HTTP State Management Mechanism, RFC Editor, 2011.

[24] Cf. Mayer/Mitchel, Third-Party Web Tracking: Policy and Technology, IEEE Symposium on Security and Privacy, 2012, P 419.

[25] Birgnull, Dark Patterns – Definition, https://www.darkpatterns.org/ (accessed at 28. Oct 2019).

[26] Cf. Bösch/Erb/Kargl/Kopp, Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Pattern, Proceedings on Privacy Enhancing Technologies, Volume 2016/Issue 4, P. 237–254.

Unless security information is made accessible and as easy as possible, users will fall foul to poor security decisions. Often, security is seen as an obstacle to productivity, the cookie «popup» just preventing them from simply accessing a website or information they require. Removing the burden is essential to improve user adoption of secure behaviours, including reviewing cookies prior to acceptance.

3. The need for machine-readable cookie polices

Currently, cookie policies are a part of the website and thus the website owner has full control of the rendering and structure of the respective cookie policy. This creative control, however, allows for dark patterns to take root. Furthermore, we have seen that the management of consent and/or withdrawal of cookies should be managed by the browser instead of the website operator. The authors therefore propose to define a machine-readable representation for cookie policies.

The advantages of this approach over regular cookie polices are numerous. For one the representation can then be used by the browser to display the cookie policy in a standardized manner. Since the browser itself is not controlled by the website operator the potential for dark patterns is reduced. Additionally, a machine-readable cookie policy would allow the browser to effectively manage the consent and also withdrawal of consent.

The approach also offers advantages to website operators. Most websites are already built on extensible Content Management Systems (CMS) such as WordPress, therefore most parts of the cookie policy could be also auto-generated by the CMS. Therefore, changes to websites like adding new functionality in the form of a WordPress plugin would also automatically update the cookie policy.

3.1. Requirements for a machine-readable cookie policy

A machine-readable format needs to support at least the following use cases:

1. **Presentation:** The presentation of the cookie policy will be performed by a browser. The machine-readable format still needs to support user-friendly text in various languages.
2. **Consent/Withdrawal:** The machine-readable format requires a detailed description of the purpose of each cookie to facilitate the blocking of specific cookie types. This would give the end-user fine grained control over which cookies to accept or to ignore.
3. **Versioning:** Cookie polices are not static and evolve over time. To guarantee transparency, the system should allow old versions to be archived in order to make it easy to track changes to the cookie policy over time.

3.2. The need for a multiple discipline effort

The viability of machine-readable cookies policies is not only determined by a technical implementation. For such an endeavor to gain traction a multi-discipline team is needed. The presentation of the cookie policies by the browser is a decisive factor for the acceptance of such a solution. The polices should be presented to the user in an easily understandable manner while still conveying all of the essential information. This can however be challenging since Article 13 of the GDPR stipulates a comprehensive list of information that is required to be accessible to the user. In order to achieve this goal competence in the fields of (visual) law and human computer interaction is of uttermost importance.

4. Conclusion

An implementation of cookies policies needs to be in compliance with legal requirements as stated in the GDPR and the ePrivacy directive. However, the way cookie policies are currently implemented leave much to be desired both on a technical level and from a usability perspective. The manner in which cookie consent is currently realized gives too much power to the website operators. Consent and its withdrawal is almost entirely implemented on the server side, giving the website visitor little choice but to trust the operator.

The same holds true from a usability perspective. It is the website operator who decides on the content and the overall user experience of the cookie policy. This approach sometimes leads to questionable practices ranging from simply «nudging» the users to just skim over the cookie policy up to complex dark patterns which outright discourage the user to opt out from privacy invasive tracking. These practices call into question whether the consent was truly freely given within the meaning of Article 4 (11) GDPR.

The aforementioned technical, usability and legal issues can be mitigated by introducing a machine-readable format for cookies polices. This approach allows for cookies polices to be enforced for the most part by the browser, giving the end user the final say about cookies. Also, the overall user experience can be improved if the browser is in control of the visual representation of the cookie polices, leaving little room for deceiving practices and empowering users to exercise their rights free from manipulation.