THE COOKIE NOTICE

[By reading this paper you accept our use of cookies]

WORD COUNT: 72.365

Abstract

This paper takes point in the implementation of the cookie notification post EU legislation from 2011 and the use of cookies on websites in general. The paper discusses the views on cookies and the notification from the perspective of danish internet users and compares these views to findings of existing research in this field. The paper revolves around the theory of contextual integrity, as presented by Helen Nissenbaum, which analyses the maintenance of privacy in these digital environments. The paper concludes that the notification mostly does not work as intended and can therefore seem unnecessary or indifferent to the user. Moreover, further research on EU citizens' perspective on cookies and the notification have to be conducted, as its impact on users after 2011 is not known. The research is important as maintaining online privacy will continuously be a challenge due to the growing industry of data collection, which can possibly endanger the EU citizens right to privacy not only now, but also in the future.

Table of contents

Chapter 1 · Introduction

1.1 Introduction

Since the introduction of information technologies, such as stand-alone systems, large government or corporate databases or linked information technologies over the Internet, as well as the *World Wide Web,* social issues of privacy have been a large concern (Hildebrandt 2013). One of many concerns of privacy is the conservation of *intellectual privacy* as Richards (2013) describes: *"Intellectual surveillance is especially dangerous […] to protect our intellectual freedom to think without state oversight or interference, we need [...] intellectual privacy".* Intellectual privacy is important as it, according to Richards, allows people to develop as people, become the person they are and altogether has a huge influence on society. One way to protect privacy is by maintaining *contextual integrity* as a benchmark of privacy. It is defined by norms of appropriateness, and norms of flow or distribution, and can only be maintained if both norms are upheld (Nissenbaum, 2004). Contextual integrity as a theory is based on privacy, which is constantly evolving. Privacy should always be seen not as abstract but in a context. As information technology is evolving, so is privacy, and that radical transformation of technology brings further concerns of privacy protection.

In the European Union (EU) there is a citizen's right to privacy, which is a sub-directive to the EU Citizens' Rights Directive, making it a fundamental right. This directive is quite unique to the world and means that the EU has to be aware of privacy concerns. Privacy is protected in the EU by making directives on privacy that the individual members of EU then have to adapt as legislations. One of these directories is the EU directive on Privacy and Electronic Communications (e-Privacy Directive), which is also known as *the Cookie Directive*, as it concerns data protection and privacy in the digital age, which is commonly known to the user because of cookies. The e-Privacy Directive has resulted in several legislations concerning privacy, such as the right to be forgotten and a number of legislations addressing protection of processing data, such as the e-Privacy extension of the EU directive on Data Protection (European Commission, 2015). One of the latest attempts to protect the right to privacy is by expanding the EU e-Privacy Directive with the EU Cookie Legislation which concerns the use of cookies. The EU Cookie legislation states that: *"The EU e-Privacy Directive* [...] *requires prior informed consent for storage of/or access to information stored on a user's terminal equipment"* (European Commission, 2015). The legislation resulted in a notification based solution (the Cookie Notification), which has already been implemented and has had a large impact on the everyday web experience for internet users throughout Europe (ibid.).

This paper focuses on the EU Cookie Legislation as its rather small size makes it advantageous to study within a small timeframe and because of the large impact the legislation has had on EU citizens. Furthermore, no research of the affected users' perception of the cookie notification currently exists. Realising the importance of the study on the cookie legislation, has led us to the following research question.

1.2 Research Question

How do danish internet users perceive cookies and cookie notifications after the EU wide cookie legislation of 2011?

1.3 Paper Structure

The paper consists of six chapters. The first chapter, which you have just read, is an introduction that presents the reader with a basic overview of the topic and its historical evolution. Chapter 2 is a background literature review, which presents the framework for this paper and its relevance, as well as existing research. This is followed by Chapter 3, which describes the methods used to conduct the study, and the methods applied for analysing the extracted findings. Chapter 4 contains an analysis of the findings followed by Chapter 5, which discusses the overall findings of our research in relation to the applied theories and existing research. Chapter 6 presents the conclusion of the paper. After the last chapter, references and appendices containing method tools and the raw data referred to in the study follow.

Chapter 2 · Background Literature Review

2.1 What Are Cookies?

A growing number of consumers actively use the internet and as a result, more companies are being represented online, which also increases the competition between them (Manyika & Roxburgh, 2011). The expanding competition makes the importance of good user experience on the websites critical to the companies, and one of the most used ways to analyse user experience is by using *cookies*. A cookie is a term covering basic information that a website can place on a visitor's computer and then recall later on, when the same visitor revisits the website. It offers the possibility for the website to identify the user and customize the shown content on the website accordingly. It is typically used for improving user experience, increasing conversion rate or gathering of information about the user's behavior on the website, making the use of cookies almost unavoidable.

Cookies themselves are small text strings that websites can choose to place in the visitor's browser. These strings contain nothing but text, an indication of which website it is from and the cookie's expiration date. A user can at all times view the complete 'content' of the cookie and delete it. Most browsers also give the user the ability to disallow the storage of cookies in the browser. A website can only access the cookies they have set themselves, not cookies set by other websites (Kristol, 2001).

Cookies were first introduced to the general public in 1995 and its technology has stayed the same ever since. They have always been used for the same, which is for a website for store information on the user's computer in order for the information to be used by the website when the visitors return. One of the most commonly use of cookies by websites is the implementation of *Google Analytics,* which is an open source tool for analysing visitors behavior. The use of Google Analytics expands the presence of cookies, by combining the information gathered from the website with information from Google, making information of searches etc. available to the website (Google, 2015). About a year after cookies were first implemented in Internet Explorer, the public became concerned with their use after *Financial Times* published an related article on February 12th, 1996. Afterwards, cookies received much media attention, especially due to potential privacy implications.

There are a variety of different cookie types, which each serve different purposes. The most basic cookie, and the one with the shortest lifespan, is the session cookie, which stores information for the user until the browser session is terminated by closing the browser tab or window. This automatically deletes the cookie. As these cookies' function does not interfere with privacy in any way, there is usually no concern with the use of those, as they are simply a way of developing websites. Furthermore, they do not contribute with information about the user that is not already available to the domain. Then there is the persistent cookie, which among other things stores user information for a certain domain in the browser of the user. The persistent cookie however, is not deleted upon terminating the session with a domain. It remains saved in the browser until it expires. The expiration date is either set by the domain itself or by the user through the browser settings. The cookie is automatically deleted when the set expiration date is met. Information that is collected through the cookie serves the user and aims to improve the user experience within the domain, as it can be used to identify the user and his or hers settings. However, this also offers the option of surveilling, which might interfere with a user’s wish of privacy. Both of these types of cookies are first-party cookies, which means that they only serve the domain they were placed by. Contrary to that there is the third-party cookie. This type of cookie is placed through a website but from a third-party domain. This cookie also collects user data based on the user’s behavior on a website, but sends the data back to it’s own domain. Third-party persistent cookies are the cookies which are the most concerning in terms of privacy, as they provide personal data to a third-party, letting the user remain unaware of where the gathered information is distributed to. The possibility of combining data in such way also provides the option of gaining much larger insight in a single user, possibly contributing to even larger interference with privacy and possible large-scale surveillance.

2.2 How Has the Concern of Cookies Been Addressed Before?

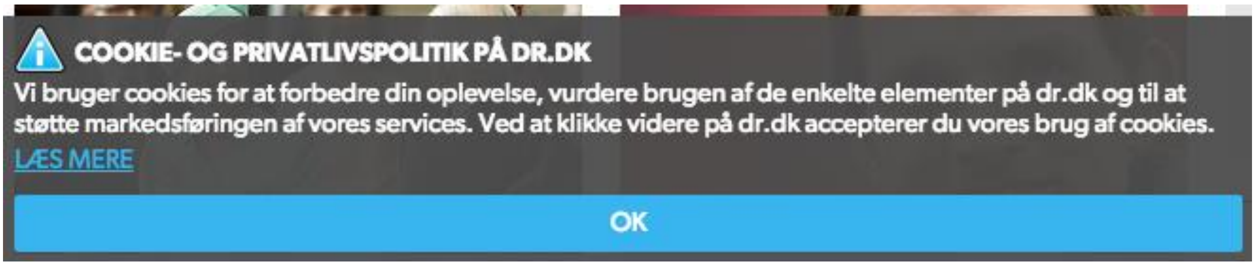
The concerns of potential privacy implications by the use of cookies has led to earlier studies on cookies. Several studies have been conducted, confirming that people find the use of cookies alarming and that the use of cookies is often in violation with their personal privacy. Notable studies are the ones by Yue, Xie and Wang in 2010 and by Ha, Inkpen, Shaar and Hdeib in 2006. Both studies include this concern and underline the importance of this issue. One of their main arguments is that many misconceptions of cookies exists, which brings uncertainty to the user's possibility of protecting their privacy. The studies conclude that there is a need for a tool to improve transparency of cookies that at the same time makes users able to manage the use of cookies. Current tools result in misconceptions and only improves transparency on data usage slightly. The studies conclusion is also backed by a study by McDonald (2010) which again underlines the importance of understanding how the users perceive cookies, how websites use them and for what they use them for. One of the ways that EU addresses the concern of cookies affecting privacy is through the EU Cookie

Legislation. A paper criticizing the way the legislation implements its solution, as well as the lack to protect the user's right to privacy, was written by Luzak (2014). Even with the critique of its implementation, and its major effect on internet users in Europe, no studies have been made on how the users experience the implementation of the legislation and what it means to their privacy online.

2.3 The EU Cookie Legislation of 2011

As mentioned in the introduction, the EU Cookie Legislation is unique to the world. Iit is a result of the fundamental right to privacy, which all EU citizens have. The European Union Agency for Fundamental Rights (FRA) expresses the reason for the need of the cookie legislation as: *“Safeguarding fundamental rights in today’s information society is a key issue for the EU and increasingly for FRA as more and more people use information and communications technologies (ICT) in their daily lives at work and at home.”* (European Union Agency for Fundamental Rights, 2015). Specific for EU is that the fundamental rights include the right to privacy, which pose as a possible threat to the development of information and communication technologies. One of these threats to ICT is the use of cookies, which allow large-scale surveillance and misuse of personal data. FRA mentions: *“[...] growing use of ICT is creating fundamental rights challenges. These range from concerns about privacy and the potential misuse of personal data online to the threats posed by cybercrime or large-scale surveillance operations.”* (ibid.). As a result, internet users in the EU may at some point face violations of their fundamental rights as citizens of EU. To fight these evolving concerns the EU legislation was passed in 2011. The EU legislation should contribute to applying the same general legal frameworks online as offline. As Hildebrand (2013) writes: *“According to the Bonn Ministerial Conference Declaration of 1997, whereby the Ministers of the European Member States (MSs) had the mission to agree on key principles to handle and regulate the fast developing Global Information Networks, ‘the general legal frameworks should be applied online as they are offline”* (Hildebrandt, 2013)

The EU Cookie Legislation states that: “*EUROPA websites must follow the Commission's guidelines on privacy and data protection and inform users that cookies are not being used to gather information unnecessarily*” (European Commission, 2015). According to the EU e-Privacy Directive, this more specifically means that all EU websites require informed consent from the visitor to be able to use cookies. Only then are they allowed to place them on the user's computer. The legislation includes all types of cookies, with the exception of first- party session cookies, which do not require informed consent. For the users, this means that on every website affected by the cookie legislation, they will meet a notification upon entering the site, which informs them that the website uses cookies. The notifications comes in various different designs, as it is up to the website how the notification is implemented. A typical example of a cookie notification is shown in *Figure 1*. The approach of these notification is informing the user that by using the website they automatically give their consent to the use of cookies.



COOKIE- OG PRIVATLIVSPOLITIK PÅ DR.DK

Vi bruger cookies for at forbedre din oplevelse, vurdere brugen af de enkelte elementer på dr.dk og til at støtte markedsføringen af vores services. Ved at klikke videre på dr.dk accepterer du vores brug af cookies.

Figure 1 - Screenshot taken from the danish website http://dr.dk/ (april 19th, 2015).

As mentioned before, criticism of this way of implementation has been made. The main argument is that the current form, where ignoring of the notification counts as giving consent, should not be seen as the informed consent that the EU directive requires. However, this still is the most common and accepted solution today.

The notification itself is designed to make cookie use easily viewable for the user. However, studies have shown that user simply chose to ignore notifications for a variety of reasons. Leon et al. (2012) talk about the layout of such notifications. They state that that text based notifications are often discarded, as user simply do not like this form of information. *“Studies have indicated that people do not read these policies, do not understand them, and do not like them. McDonald and Cranor estimated that if Americans actually read privacy policies, it would take 244 hours per year per person, corresponding to a national opportunity cost of $781 billion dollars.”* (ibid.) The amount of time users would actually have to spend to read all the information they are presented with leads to what Shklovski et al. (2014) refer to as *warning fatigue,* which happens when the user is exposed to seemingly unmanageable amounts of information. As a result the user then has to prioritize the time he spends online, divided into time spent reading end-user license agreements (EULAs), disclaimers etc. and the time he uses to complete the actions he intended to do on the internet in the first place. Therefore it can be debated whether or not the text based cookie notification as it exists today works as intended, as it too often is ignored for different reasons, which will be presented later in this paper.

As the cookie notification is a solution to improving current issues on privacy and surveillance, it becomes interesting to know why an informed consent is improving privacy, as the use of cookies remain the same, possibly opposing the same threats. One way to look at the solution and how privacy is maintained is by analysing the context and thereby finding out if contextual integrity exists.

2.4 Contextual Integrity

Contextual integrity is a theory coined by Helen Nissenbaum (2004) that defines how privacy in the modern electronic world can be analysed, even as the circumstances of privacy constantly change alongside information and communication technologies. The theory states that contextual integrity exists when both norms of appropriateness and norms of flow or distribution are upheld. Nissenbaum (2004) describes it as: "*Among the norms present in most contexts are ones that govern information, and, most relevant to our discussion, information about the people involved in the contexts. I posit two types of informational norms: norms of appropriateness, and norms of flow or distribution. Contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated."* Contextual integrity is important to the concern of cookies interfering with privacy, as privacy is hard to define with the constantly evolving technology. Therefore, technology changes the context and with it the boundaries of privacy. Looking at contextual integrity makes us able to see how privacy is affected by the cookie legislation, when analysing how the users perceive the cookie notification and its context. This allows using contextual integrity as a measure of whether privacy is maintained. *"The benchmark of privacy is contextual integrity; that in any given situation, a complaint that privacy has been violated is sound in the event that one or the other types of the informational norms has been transgressed*" (ibid.).

To maintain contextual integrity norms of appropriateness need to not be crossed. *"[...] norms of appropriateness dictate what information about persons is appropriate, or fitting, to reveal in a particular context"* (ibid.). When it comes to the use of cookies, this is very relevant as it means that the implementation of the cookie notification should have contributed to maintaining appropriateness, even though the legislation does not dictate what cookies can be used for, but rather when the user should be informed of its use. Therefore, it is very interesting whether the cookie notification enhances the appropriateness or stops it from getting less appropriate. One thing is the appropriateness of the information, another is how it is distributed. Nissenbaum describes how *complex equality,* which is Walzer's mark of justice when distributing social goods according to the norms of distribution in different spheres, contributes to norms of distribution or flow to be upheld for contextual integrity to exist. *“Complex equality adds the idea of distributive principles or distributive criteria to the notion of contextual integrity. What matters is not only whether information is appropriate or inappropriate for a given context, but whether its distribution, or flow, respects contextual norms of information flow.”* (ibid.). Again this is interesting as it means that in order for the cookie notice to contribute towards maintaining privacy, and therefore also contextual integrity, it should protect how the information is distributed according to the existing norms.

To further explore how the cookie notice improves privacy, we therefore need to research how internet users perceive cookies and cookie notification in everyday life, what the effect of its is on them and what it means to their perception of the informations appropriateness and its distribution or flow.

Chapter 3 · Method

The research study that was conducted for this paper, is made up of two parts, a broader survey study and a series of smaller follow-up interviews. The survey study allowed for an overview of the general understanding of cookies and the users' perception of the cookie notice. The follow-up interviews allow for a more detailed picture of the individual user's' interaction with cookies, while browsing the internet, as well as the possibility for us to discuss the findings from our survey with the users. This chapter furthermore highlights the research methods' strengths and explains the reasoning behind the choice of methods.

3.1 Survey

Under most circumstances, a survey is conducted in order to get representative data in forms of numbers, which tell researchers the opinion of a given population. A survey is therefore viewed as a quantitative research method. The first part of the research conducted in the context of this paper also called for a general overview of danish internet users' experience with cookies and the cookie notice. However, the goal of the survey was not to obtain representative data, but to give insight in the respondents thoughts about cookies. Furthermore, the data from the survey was obtained to provide a good basis for follow-up interviews, as it contained several subjective textbox responses and therefore detailed qualitative data. With this in mind, the survey acts more in the manner of qualitative research (Bryman, A. 2012).

The survey was conducted in the form of a convenience sample, which means that the sampling was rather opportunistic (ibid.). We distributed the survey through a Facebook link and via mails in the form of a snowball sampling. This means that we let our peers distribute the link within their own network and thereby spreading it further out than we could normally have reached. The result was that we gained many responses from active internet users, since we distributed the survey via a social media network. Most of our respondents are people that have average to excellent computer knowledge to begin with. This also means that we have to keep in mind that these respondents possibly have a strong opinion about cookies and tracking to begin with, which might not represent the average internet user in Denmark. Furthermore, given that Facebook is a social media network, this means that most of the respondents are fairly young of age. We therefore chose our parents and friends of the family to distribute the survey link via mail, resulting in responses from an older group of people. As stated, a majority of the responses came from Facebook and the average age of the respondent ended up being 29. Both the utilized platform and the young age of the respondents should be kept in mind, as the outcome is based on a generation of people, who are familiar with both social media networks as well as browsing the internet and some of the associated privacy debates. The outcome would have been different if another method had been chosen instead.

We chose a survey to extract the general opinion on cookies among our respondents, how they are perceived and how they interact with them. In addition, the survey answered our question in regards to whether or not the mandatory cookie notice has had any effect on the respondents knowledge on the topic. Lastly, we were interested in seeing if the cookie notice changed the perception of cookies and whether it legitimized its existence in the eyes of the respondents. The survey gave us some interesting findings, which will be presented later in the findings chapter. These findings also made for a fundament on which the interviews were build upon.

3.2 Interviews

For the follow-up interviews, four respondents were chosen. We selected the respondents based on diversity and availability. Only one third of the respondents, who completed the survey, agreed to be contacted in case of further questions. Therefore, we analysed our findings and proceeded to calculate how many respondents we would need to ask further questions that would cover the entirety of our findings. We selected four respondents from the survey for the follow-up interview out of the 33% of total respondents, which each covered a section of our findings.

The individual interview guides were tailored to the individual respondent, but contained a couple of basic, overlapping questions. Generally speaking we wanted to know if cookies are something positive or something negative in the respondent's perception. Furthermore, we wanted to know why they delete cookies, why they did not read the cookie notifications and if they could relate to the cookie notification after they were told what exactly cookies are and the reason why the notification is displayed. The interview process was varying, two of the interviews were phone conversations, which were recorded on a personal computer, one was a audio-only Skype conversation recording and the last was a regular face-to-face interview, which was also recorded on a pc. The follow-up interviews provided us with a variety of statements, which we have collected as separate findings. For our analysis we then proceeded to hold the two sets of findings against each other to deduct a conclusion to our research question. The parts of the interviews that were important to the writing of this paper have been summarized in Appendix 4.

3.3 Sampling / Target Group

Our target group is as stated all danish internet users. However, due to the way the population was self-selected through Facebook, there is a sampling bias in our method. The survey excludes all non-Facebook-users, except for the respondents that obtained the link to the survey via email. A sampling bias occurs, when a distortion in the representativeness of the sample arises, when some members of the sampling frame or population stand little or no chance for being selected for inclusion in the sample (Bryman 2012). The conducted sampling method is also known as a convenience sample. This means that researchers rely on an already established network, which is easily accessible. A convenience sample is a form of nonprobability sampling, which is an umbrella term for all the sampling methods that are not based on probability calculations (ibid.) However, the main focus of this study is the qualitative data we get from both survey and interviews, as the representativeness of the survey was secondary to the study. With this in mind, the sampling bias is not as severe, as we are still able to discuss the respondent's subjective view on cookies, based on our findings.

3.4 Analysis Method

The data, which was collected from the survey was sorted according to themes and patterns that we found through coding. These extracted themes or findings are presented in the fourth chapter of this paper. Whenever the respondents had made the similar arguments or a relevant statement repeated itself, it was noted. The interviews are, as stated earlier, based on the findings from the survey. The questions were build around our findings and were formed to let us confirm or invalidate the tendencies behind the findings.

The most important findings, combined from the survey and the interviews, are gathered in the next chapter. We selected the four most important findings based upon answering our research question in relation to contextual integrity.

We see the study as a whole as a thematic analysis, as we examine data and extract core themes through coding. Moreover, the study is conducted in the manner of an inductive research method, as we find coherent patterns and draw a conclusion (Bryman, 2012) that builds upon the theoretical framework of contextual integrity.

Chapter 4 · Findings

4.1 Cookies Are Still a Concern to the Users

In the survey we find that there is a tendency among the respondents to describe cookies as something negative. Only 21% of our respondents mention improved user experience or other positive outcomes, when talking about what cookies can be used for. Most talk about topics like surveillance, tracking, advertising and marketing (Appx. 2). This says something about how the respondents perceive the different uses of cookies, which in most cases are based on issues of privacy and a negative attitude towards cookies and its use in general. This finding is interesting, as cookies are often used to make better user experience, from which we assume no negative perception would come from. Earlier studies, before the EU legislation and the implementation of the cookies, show the same concern. McDonald (2010) cites that Anton et al. studied privacy concerns in 2008, and found that *"individuals have become more concerned about personalization with regard to customized browsing experiences, monitored purchasing patterns, and targeted marketing and research"* (McDonald, 2010)

A tendency among our respondents is to perceive the use of cookies as negative, where a concern of cookies obviously exists both before and after the EU legislation. The same concern of the possible misuse exists after the EU legislation, even though 73% of the respondents often or always accept the use of cookies (Appx. 2). One could argue that the norm of appropriate use of cookies has changed for the current use of cookies to be acceptable. Even though their use i perceived as negative and concerning to privacy, the user often accepts the terms and conditions. The findings also show that even though it can be argued for the use to be within the norms of what is appropriate, it is very clear that the respondents are concerned about the distribution and flow of the data provided by cookies.

An example of the concern among our respondents is the perception of cookies being a concern to privacy, deleting them is protecting oneself. Respondent B states: *"I have a software that deletes them (the cookies) automatically"* (Interview 2, Appx. 4). When respondent B is asked if she actively would chose to delete them, if not done automatically, she answers that *"Yes i would, neither do I save passwords and such on the internet"* (Interview 2, Appx. 4) When asked why, she explains her concern that others might gain access to her private information. And she is not the only one, in fact almost all users know how to delete cookies. Only 12% of our respondents state that they do not know how to delete their cookies from their browser. The fact that the users know how to delete cookies tells us that there must be a reason for it, and more importantly why they want to delete them in the first place. It is essential to the discussion how the respondents perceive cookies according to privacy, as this seems to argue against the use of cookies being within the norm of what is appropriate, unlike our earlier finding. It is of interest to know why the respondents accept the terms and conditions, but then still concerns themselves with deleting them later on. One could argue that this finding indicates a tendency of accepting the terms of cookie use, not because its contextual integrity is maintained, but because it is worth the risk, and therefore the cookies are deleted later on after accepting them. When asked why the respondents deletes cookies amongst the answers were: *"To avoid commercials where i can see it is about something i have looked at before*", *"Because of SPAM [...]"*, *"Because i did not want to have them"*, *"A naive try to get rid of advertisement and malware"* and *"I did not want to be tracked more than necessary"* (Appx. 2). Another argument could be that deleting cookies does not always rely on the concern of privacy but rather on misconceptions of cookies.

4.2 Misconceptions of Cookies Still Exist

The findings show us that some misconceptions of cookies still exist. Some of the misconceptions among our respondents are that *cookies are used for something bad*, that *clearing cookies can improve computer performance*, that *cookies can infect your computer* and that *ignoring the notification declines the use of cookies altogether, while closing it deletes the cookies*. These findings are very relevant as the purpose of the notification is to protect privacy and therefore maintaining contextual integrity by ensuring that the norms of appropriateness and distribution or flow are followed throughout the process. These misconceptions do not contribute to the use of cookies being more appropriate or distributed according to the norm, they are rather an example of doing the opposite. We can say that as the findings show a relatively clear tendency of transparency when it comes to the use of cookies. They are being defined as making the user's perception on the use of cookies as appropriate. Within the answers of the respondents is a very strong opinion on the use of cookies being more appropriate if the user is informed beforehand, even though the use of cookies remains the same. The occurring misconceptions can therefore be seen as a critique of the implementation of the notification itself. However, in order to be able to say something about this matter, we need to look at why these misconceptions exist.

Misconceptions might be caused by some users not knowing what cookies are at all and they therefore just ignore the cookie notification. 7% of our respondents from the survey state that they do not know what an internet cookie is precisely, nor do they know its use. All of these respondents are women in the age 18-54 and all of them state that they have average computer knowledge. They furthermore state that they do not use the cookie notification for anything other than closing it, and that they do not know why websites have cookies. This finding is interesting since it says something about the respondents view on cookies, but also about the effect of the cookie notification and the respondent's perception of privacy. To these users the notification does not provide any improvement of maintaining contextual integrity, as the main function of the notification is to inform the user and obtain a given consent before use. However, these users do not seem to concern themselves with reading the notification at all, to them it's the same as any other annoying popup. This finding seems to have some aspects of the notification not working for those users, as they experience warning fatigue. As our survey shows this tendency, we can only say that these perceptions or missing perceptions of cookies exists. At the same time the survey shows a tendency among our respondents that only very few have never heard about cookies. One could argue that the notification is not to blame, but rather that no matter the circumstances there will always be some people, to whom online privacy just is not that important. This lack of taking responsibility and reading notifications and the like, will always present a concern to privacy.

But misconceptions also exist within those who know what cookies are, or at least those who think they do. The findings show that almost all users think they know what cookies are, but many of them fail to describe them adequately, or sometimes even describe them wrongfully. 93% of our respondents state that they know, or at least partly know, what an internet cookie is. However 22% of those respondents’ answers show that they have a wrong perception on the subject. A large part of the respondents fail to describe the whole spectre of what a cookie does adequately and only describe some parts. This finding is important as the users have a perception of informed use of cookies being a key aspect to constraining the use to within the norms of appropriateness. However, the same users might not know entirely what cookies are or what they can be used for, making their perception somehow unreliable.

Another misconception is that clearing cookies can improve computer performance, which simply put is not the case. When the interviewer states that respondent A has answered in the survey that he has deleted cookies, and asks him why, he answers that: *“I just remember that i have done it, probably just to clean the computer.”* (Interview 1, Appx. 4). It might have been true in the first years of the cookies in the mid nineties where computers had very limited hardware storage, but today the impact on computer performance by cookies is comparable to a drop of water in an ocean. This is interesting because the respondent does not clean the cookies in terms of privacy, as one could have expected, but rather as a way of freeing disk space on the computer. He therefore is expected to bring the concern of his computer performance into consideration when accepting cookies. Even though he has this misconception, the respondent always accepts cookies and has never read the notification.

A further misconception is that cookies can infect your computer. When asked if respondent A has any concerns on websites using cookies he answers: “Well, then it should be about getting virus or something like that [...].” (Interview 1, Appx. 4) This answer is interesting as its is similar to misconceptions found in earlier studies of cookies before the notification was introduced. An example of that is the findings from McDonald’s interviews in 2010 showing that: *”Most people believed something that was not correct about cookies. [...] participants believed cookies are malware.”* (McDonald, 2010). The misconceptions of cookies enabling malware is a clear example of how the notification have not had impact on the respondent's knowledge of cookies, other than informing him that cookies were being used. Seeing that the respondent does not seem concerned with his privacy and at all times accepts the notification, one could argue that the notification has not contributed to protecting his privacy, as the EU e-Privacy directive intended. Neither the use of cookies have been made more appropriate in his opinion, nor have its norm of distribution or flow been more clarified. On the other side, this finding also indicates that the respondent does not perceive the use of cookies as a concern to his privacy.

Something that contributes to this tendency among the respondents is the misconception that cookies are for “bad” use. When respondent B is asked if she thinks cookies could be used for other than marketing she answers: “They show something about where my interests lie. If you have bad intentions you could probably also track me online, so they could probably be used for surveillance.” (Interview 2, Appx. 4) This is not a directly misconception as it is true, but when asked further about the use of cookies, respondent C says that: “Actually, I don’t know what a cookie is, but it is a way to track your activity on the internet. Or remember which websites you have visited and through that track what kind of person you are and which preferences you have.” (Interview 3, Appx. 4). We see this as a misconception, since cookies in many cases are used for enhancing the user experience and not only for “bad” use. This tendency is not new, as it is also found in earlier studies by McDonald in 2010. *“Participants have a vague notion that too many cookies are bad but do not know why. For all that they do not understand how cookies work, they do understand some of the benefits of cookies, such as not needing to log back in every time they visit a website.”* (McDonald, 2010).

What makes it interesting and contributing to the tendency is that even though most of the respondents describes cookies as being for “bad” use, almost all of the respondents always accept the use of cookies without reading the notification. The cookies are therefore accepted without the respondents knowing what cookies are used for. Therefore it could be argued that the finding indicates a norm of appropriateness within our respondents when it comes to use of cookies, though clearly stating that the distribution or flow of cookies is not within their norm. Still the respondents do not leave the site, rejecting the cookies, or read the notification to inform themselves of the cookies, they just accept them. None of the users read the conditions of cookie use every time, in fact 88% state that they have never read them. None of our respondents chose ‘always’ when asked how often they read the terms and conditions of cookie use.

It is up for discussion whether the use of cookies actually is not within the norms of being appropriate in the eyes of the respondents, and our findings show a tendency of accepting the cookies, because it is inconvenient not to. As it is not within the norms, and therefore without contextual integrity, privacy may not be protected. Some of the misconceptions are so grave, that it results in a distortion of the user’s perception of how the experience of cookies is within their norms. An example of that is the misconception of closing the notification deletes the cookies. When asked about if respondent D deletes cookies once in awhile, she replies that: *“Yes, sometimes. I do understand that it's improving the service I’m entering (refers to a webpage). Sometimes i just think: Oh well, cookies just improves the possibilities of the service I’m using, but sometimes it just annoys me and then i close it.”* (Interview 4, Appx. 4). Here the respondent believes that by closing the cookie notification she deletes or rejects the cookies, which is not the case. In fact when closing the notification the exact opposite happens, she accepts the terms and conditions of their use of cookies.

These findings of misconceptions are important, as they confirm that such perceptions exists. This shows that the norm for when, where and for what the use of cookies is appropriate are different from what was first expected. If a number of users believe that by ignoring or closing the notification they decline or delete the cookies, then it breaks the norm of distribution or flow of the data. At the same time this may result in the norm of appropriateness being crossed, as our findings showed that transparency in the use of cookies is key to maintaining appropriateness. Even though the user in reality is acting in ignorance. Furthermore, it makes it interesting to see why these misconceptions persist, when the information and transparency the user needs is presented to them in the notifications every time they enter a website with cookies. Moreover it is interesting to know why they do not read the notifications.

4.3 Convenience Over Privacy

The EU legislation on cookies was implemented ensure that users know what their personal data is being used for when visiting websites on the internet. Therefore, it would be easy to assume that the cookie notification serves this purpose of informing the user and works as intended, as people in most cases tend to value their online privacy highly. Our study confirms that our respondents are interested in knowing what happens to this information as well. When asked what he thinks of the EU legislation in regards to it ensuring that websites have a cookie notification, respondent A answers: *“I think it is fine (to have notifications) if a website keeps information about you, that you haven't agreed to and they haven't told you. Because it (the information) can be quite personal to some people. So it is okay that the legislation says that they have to inform people.”* (Interview 1, Appx. 4) Other respondents add to this by giving similar statements. Several of our respondents from the follow-up interviews give the impression that they in general feel like their personal data should be theirs to control and that they should decide which information about them is shared and which is not. Our respondents were also highly interested in having the option to check what kind of cookies were used and what they were doing to their privacy. This does not mean that they all effectively inform themselves, they just like to have the option.

As already mentioned earlier this speaks for appropriateness of the notification in terms of contextual integrity, as it gives the user more insight into what is happening with their personal data. At the same time the EU legislation on cookie use fails to address the underlying problem of whether or not the collection of said data through cookies is necessary in the first place. Cookies, especially the third-party type of cookie, collect more data than they in fact need in terms of providing a good user experience throughout the domain. This over-sharing of personal information would according to Nissenbaum represent a breach in both the norms of flow and distribution and the norm of appropriateness. This means that the presence of contextual integrity is nullified and that privacy therefore is not able to be maintained.

Going back to looking at the results of our research, only 8% of our respondents state that they read the cookie notification frequently, even though they know that they could read more about cookies by clicking on the notification. As part of our procedure in the follow-up interviews, we thoroughly explained to our respondents what cookies are and what they are used for. Respondent A was asked whether she would start reading the conditions in the cookie notification based on the new information she had just received. The respondent’s answer is “No” (Interview 1, Appx. 4). Again, this is a tendency found in all of our interviews.

The respondents were interested in understanding what cookies are and what they mean to them in terms of privacy online, however none of the respondents intended to read the notification frequently in the future, nor did they intend to change their browsing habits. When asked why they did not intend to read the notification in the future, the respondents often emphasize the annoyance that these notification represented for them. An example is Respondent C, who says: "*No (she does not read the cookie notification), but that only comes to underline my perception of how annoying I think they are. If I do something about them, I mostly click them away (close them), otherwise I just let them be."* Respondent D elaborates why she is annoyed with the notification by saying: *"I'm not interested in reading them. I'm in the middle of something else. Something that is interesting to me, that is why I'm in this spot on the internet in the first place. So therefore I do not want to read about cookies or anything else."* (Interview 4, Appx. 4)

By now we know that our respondents want to value their privacy highly, but at the same time they do not intend to change anything about their online habits or spend time on informing them about cookies, which ultimately is a paradox. This particular paradox, where intentions and and behaviour around information disclosure differ radically, is called the privacy paradox (Shklovski et al. 2014). The problem with this paradox is that the difference between what people say and what people actually do is big. A possible reason is that people know that the 'right' thing to do would be to inform themselves and adjust their behaviour and thus they would like to give their peers the impression that they are doing just that. In reality they have a variety of reasons for why they cannot and do not want to spend time on reading more about cookies.

When asked about the cookie notification and the EU legislation respondent D answers that: *"I think it's fine that they (websites) are required to inform about the presence of cookies. I think that's a very good idea. And now that we talk about it, I remember thinking to myself that I should read more about the individual cookie (notification), but that is where my laziness got the best of me...I never got around to it."* (Interview 4, Appx 4). This is one of many statement from our study that makes it clear, that there are a lot of reasons for people not to inform themselves about cookies. However, they know that it would be the right thing to do, so they often tend to make up excuses to justify their disinterest. These excuses range from respondents who think they know everything there is to know, despite them having misconceptions, to respondents who think they reject cookies by closing the notifications. The result however is the same, only very few of our respondents know what the purpose of cookies is and even less respondents inform themselves, despite having all the tools available.

According to Leon et al. (2012), researchers have studied different options when informing users online, as e.g. using icons to help informing the user. Text-based notifications that we know from EULAs in software or smartphone apps, tend to have little impact on the user's interest. That is why alternative methods have considered, among other icon-based notifications. The idea is to display symbols or icons instead of writing text, which should make it easier for the user to identify a website's privacy configuration in a quick glance. This was partially experimented with to ease the load of information that online users are exposed to everyday, which is what was described earlier as *warning fatigue* (Shklovski et al., 2014). Shklovski et al.'s study explained how their participants had to download an application on their smartphones and where afterwards questioned whether they had paid attention to the EULA or noticed what they allowed the application to do in terms of data collection and given access. They found that the participants have had their worries about privacy, but discarded it later on due to two facts: they had never experienced any negative consequences by just accepting and secondly the desire to install the app won over the worries about privacy. The reason this is interesting, is because it supports the trend that we have seen in our study. People generally care about their privacy, however only when it is convenient for them. As soon as the task of maintaining privacy becomes inconvenient, e.g. having to read text or adjust the setting of the browser, most of our respondents lose motivation. This is arguably also a question of convenience, where the desire to continue with what you are doing online trumps over the privacy aspect as e.g. respondent D described. Another interesting aspect of Shklovski et al.'s study is the following citation from one of the participants of the study. When asked about why he never read the EULA he responded: *"I will never waste my time reading privacy policies, my time is simply too valuable. To some extent I just have to accept this."* (ibid.) This shows that there generally speaking is knowledge about privacy issues when installing apps, however the respondent had come to accept it, since he did not really have a choice when it comes to enjoying an app without it being inconvenient for him or her to install it. We can see the same in the EU legislation, where the trend is to discuss how the user is informed about cookies using their data, instead of discussing whether it should be morally and legally acceptable to collect and sell data, because at the moment it is simply the norm.

The notification therefore protects privacy as it improves transparency of when cookies are used, by ensuring that the users know when the cookies are used. According to the respondents perception, this makes the use of cookies more appropriate and therefore it contributes to maintaining contextual integrity. However the distribution or flow of the data that the cookies provides seems unchanged, and even though the notification provides further information of this, almost none of the respondents seem to take advantage of it. The notification's design and implementation is currently based on being an informed consent, but this aspect of the notification does not seem to improve protection of privacy in the eyes of the respondents. It can be discussed whether a notification designed in a different manner could simplify the informing of cookie use and thereby making it more informative. A redesign could also try to improve how the user perceives the distribution or flow, so it is ensured to be within the norms, and therefore maintaining contextual integrity.

4.4 Knowing If a Website Uses Cookies Is Enough to Maintain Contextual Integrity

Seeing that it is necessary to maintain contextual integrity when working with technology, it is interesting to know what it would take to accomplish that in regard to cookies. When asked about what she thought about the implementation of the cookie notice, respondent B stated that the notification did not tell her anything she did not already know. When the interviewer asks respondent B if the cookie notification has contributed to her knowledge in any way, she answers: *"Erhm, I don't think so. I cannot reject that completely, but I have never used or read them. It was more (of concern) when the debate was ongoing."* (Interview 2, Appx. 4). This is interesting, as the respondent states that the notification has not contributed to her knowledge on the subject. Earlier in the interview she stated that she thought visitors should be informed of the use of cookies, not by having to close a popup as of now, but rather just as accessible information on the page. Due to the lack of newness, the same respondent therefore thought that the notification was rather unnecessary and elaborates by saying that: *"I think it is a little bit redundant to be honest. If you keep yourself up to date just a little bit, you know that no matter where you go (online), a cookie is stored on your PC, so they can see where you are going and recognize your machine."* (Interview 2, Appx. 4) It is interesting that the respondent finds it to be common knowledge what cookies are used for, as well as the fact that almost every website uses them. This therefore makes the legislation unnecessary for the respondent and at the same time provides the respondents with a sense of annoyance to their browsing. The general sense of annoyance is mentioned by various respondents from our survey study. In fact the majority of our respondents mention that they are disruptive to their use of the internet.

Respondent B feels that the notification is redundant for herself, however at the same time thinks that the information about cookie use generally is appropriate to have access to. In terms of contextual integrity this translates to the norm of appropriateness in this example is upheld, whereas the norm of flow or distribution on cookie use still are not. Furthermore, we see this trend present in all types of respondents, whether they are well aware what cookies are or know nothing about them. None of our respondents thought that the information within the cookie notification was inappropriate knowledge, while almost all of our respondents thought that the nature of the constant notification was intrusive.

Ha et al. (2006) describe in their article the following: *“Most cookie management software utilise alerts to indicate the presence of an incoming cookie while a user is browsing the Web. Although this feature provides users with a heightened awareness of cookie interactions, users generally find this form of immediate feedback frustrating and overly intrusive. However, this approach provides excellent control over the information being sent out.” (*Ha, Inkpen, Shaar & Hdeib, 2006) This shows that researchers are aware of the fact that this kind of notification has a tradeoff between being informative and being annoying or intrusive, which can be applied to the way the cookie notification informs the user according to the EU legislation. Here the information is presented constantly in the form of a pop-up notification upon entering a majority of websites. In contrast to other forms of agreements, e.g. EULAs, where the user is typically prompted once to agree, cookie notifications have to be accepted individually on different websites or manually closed each time you visit a website.

Cookies are useful, but can at the same time fail to maintain privacy for the user, as there is a distinct tradeoff between privacy and convenience of their use. The efficiency of maintaining privacy depends very much on the individual user’s knowledge on online privacy, which leads to varying views on the cookie debate. In the following chapter the findings of our research will be discussed based on our respondents’ views and in relation to the mentioned related theories.

Chapter 5 · Discussion

The findings show that the concern with online privacy still exists, but that the perception of cookies influence on online privacy has changed when compared to earlier research. In our findings we see a tendency where respondents describe that the norms of the appropriateness of use of cookies have changed for them to lie within the norm, as long as the user is informed that cookies are being used. This norm contributes to maintaining contextual integrity and the belief that our privacy is protected. That being said, it seems that the norm of distribution within the use of cookies is unchanged among our respondents. Though the appropriateness seems to be within the norms, the distribution is perceived as debatable and offensive in many ways. Still the respondents seems to accept the distribution, as it is the norm to accept that the distribution stays in conflict with the norms, because of its convenience to the user, who sees no alternative. Seen in a more general perspective, the prioritizing of convenience over privacy is a huge concern to privacy, as the users set aside the very concerns of privacy that they have expressed themselves.

Existing research showed that the users privacy was violated by cookies because of missing information about the use of cookies. The findings showed that among our respondents, the understanding is that everyone knows that cookies are being used on almost every website. The perception is that the knowledge of cookies being used everywhere has become common knowledge. The cookie notification itself therefore could seem obsolete, as the findings also show that no users found the notification to present them with new information.

Our findings show us that misconceptions of cookies still exists among our respondents. The misconceptions concern the technology itself, but also its distribution. For these misconceptions to still exist to such an extent, raises questions of the design of the cookie notification. The current design seems to contribute to warning fatigue among our respondents, as the legislation requires for the notification to be shown on every new website, as mentioned in our findings. The result is that almost none of our respondents have ever read the notification. There is a possibility that if the respondents read the notification, the number of misconceptions might be reduced. We can not say whether a better design of the notification would increase the number of users that read the notification, but we can say that the current design counteracts the notification’s purpose. People are not going to start caring more simply because they get an onscreen notification all the time.

Another question to the design is the way the notification is designed for the user to give their consent to the website's use of cookies. The current implementation means for the consent to be passive, as ignoring the notification also results in giving consent. Its design encourages users to give their consent no matter what the user does. The only way to get rid of the notification, as one would naturally want to, is to close it, which also acts as a consent to cookie use. Our respondents perceive the notification as contributing to maintaining contextual integrity because of its information about cookies being used, but none of the respondents see the consent as contributing to be within the norms of appropriateness and distribution or flow, which otherwise would help to protect privacy. The notification therefore should focus its design on informing the users instead of giving passive consent. If a consent could improve privacy, an active consent might be required instead.

The current legislation on cookies argues that if you do not wish to accept cookies as a user of the internet, then you should not enter the sites that uses cookies. Furthermore, the legislation provides you with the information that gives you the possibility to do so. As argued earlier in this paper, that option seems to be an illusion, as the modern society does not provide the possibility to avoid going online. This also means one cannot be part of the community without accepting the use of cookies in modern society. One could argue that the legislation should concern the actual use of cookies to protect the EU citizens right to privacy rather than the informing of its use, as it seems to have become obsolete. It also seems that the EU legislation is made to secure the consumer's right to information rather than the right to privacy. There is no argument that the legislation is wrong, but rather that it might already have become insufficient in protecting the user's right to privacy. If the legislation should be able to cover the actual use of cookies and all the possible uses to which cookies contribute, it would be rather complex. It might not even be possible to enforce the legislation, due to the complexity of controlling the use of cookies. This only tells us how potentially dangerous the use of gathered, personal information could be to privacy.

How badly do we even need data protection when it comes to use of cookies? They are not the only method that can be used to violate the users privacy. As mentioned, it seems that the EU legislation is very concerned with cookies, as it is a more approachable technology to legislate. However many other methods and technologies provides the same options and possibilities as using cookies (McDonald, 2010). An example of such a technology is *fingerprinting*, which is a way of identifying users through the combination of many different technologies, in the same way that cookies do. One could argue that fingerprinting is an even more extensive technology than the use of cookies (Tanner, 2013). To legislate the use of all these technologies seems impossible, as the only way to enforce it would seem to be for the EU to establish mass surveillance. This however is of course a contradiction, as surveillance is what the EU legislation is trying to prevent in the first place when protecting the user's right to privacy. The legislation on only one of these technologies therefore seems to be insignificant when it comes to protecting the user's privacy, though it affects all users of the internet within EU.

Privacy continues to be an important subject. As technologies keep evolving the challenge to maintain the protection of privacy continues alongside. The latest example of an EU legislation on data protection is the legislation against a dark pattern design phenomenon called *Sneak into basket*. Sneak into basket is a method where a webshop adds things to a user's shopping cart or basket without their consent. This forces the user to deselect the items at checkout, if they do not want to pay for them. These items are however commonly overlooked, as the price of the added items is low enough to slip past the attention of the user. The EU legislation against this is made to ensure that online users have the same circumstances as offline. If someone at your local store added groceries into your cart while being unaware, it would be perceived as wrong. In the same matter it seems debatable that cookies and technologies alike are even legal, as tracking of our offline behaviour by strangers would not be accepted. The definition of privacy will continue to change as society and technology changes, and the only way for EU to protect the user's right to privacy is to keep trying to maintain contextual integrity in a way that balances the distribution of information with the appropriateness of data collection.

Chapter 6 · Conclusion

The definition of privacy is constantly changing, both online and offline. New technologies allow for an easier way of living, however these technologies also collect vast amounts of personal data, which can reveal and trace the movements of its users. In this paper we have taken a closer look at the implementation of the cookie notice and the related EU legislation on the use of cookies, and researched the impact these new laws have had on a selection of danish internet users. The research allows for an insight in the perception that our respondents have voiced and furthermore acts as a stepping stone to possible further research in the future. A tendency we can see from our research is the fact that the majority of our respondents have heard of cookies, however at the same time they are misinformed about the exact purpose of cookies. Whether this is due to misinformation through media or social peers or simply the personal lack of interest, is hard to tell from our data. Our data does however tell that close to none of our respondents take the time to read more about cookie usage by utilizing the cookie notification on various websites. This also means that for the majority of our respondents the cookie notification fails to act as an informant on online privacy, and therefore does not work as intended in all situations. In our example, the implementation of the cookie notice has had little impact on the user and related research tells us that *warning fatigue,* as well as the text based nature of the cookie notification, are possible implications in that matter.

We have utilized Helen Nissenbaum's theory of *contextual integrity* to analyse whether it is present and maintained in the case of cookies and the notification. By looking at contextual integrity we found that two norms have to be maintained in order to uphold it; the norm of appropriateness and the norm of flow and distribution. These two norms act as a substitute for the term privacy, as the term is hard to define precisely, however contextual integrity can give an indication to whether privacy is present or absent. We found that contextual integrity in relation to cookies and the cookie notification is debatable; in our case our respondents tend to have a negative view on cookies and the majority seems to think that the negative aspects of using cookies outweigh the positive. This being said, we have to understand that the outcome of our research cannot be seen as representative and should therefore rather be seen as a trend or a tendency of beliefs among danish internet users.

As far as we can see based on our research, the optional, text-based approach of delivering critical privacy information to the user could use rethinking. Further research would undoubtedly benefit, as shaping the nature of this different approach relies on it. Moreover, a broader study in the EU on the effects of cookies, the cookie notification and the related EU legislation after 2011 could help gather the opinions of internet users of all the different countries. Thereby, the bias of data gathered through surveys conducted in one country would be eliminated. Lastly, we see that the profitable business that lies in selling collected user data further implicates the establishment of true privacy online. As long as it is lucrative and legal to sell user data, measurements that enable privacy online seem unlikely to be implemented successfully.

References

BRYMAN, A. (2012) Social Research Methods. Fourth Edition. New York, USA: Oxford University Press.

EUROPEAN COMISSION. (2015) *The EU Internet Handbook - EU Legislation on Cookies.* [Online] Available from: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm#section_2 [Accessed: 6. April 2015]

EUROPEAN UNION AGENCY FOR FUNDEMENTAL RIGHTS. (2015) *Information Society, Privacy and Data Protection*. [Online] Available from: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection [Accessed: 6. April 2015]

GOOGLE (2015). Google Analytics website. Available from: https://www.google.com/intl/da_Dk/analytics/ [Accessed: 6. April 2015]

HA, V., INKPEN, K., SHAAR, F. A. & HDEIB, L. (2006) An Examination of User Perception and Misconception of Internet Cookies. *CHI '06 Extended Abstracts on Human Factors in Computing Systems*. [Online] ACM Digital Library. pp. 833-838.
Available from: http://dl.acm.org [Accessed: 6. April 2015]

HILDEBRANDT, M. & TIELEMANS, L. (2013) Data Protection by Design and Technology Neutral Law. *Computer Law & Security Review (29).* Elsevier Ltd. pp. 509-521.

LEON, P., G. et al. (2012) What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users? WPES '12 Proceedings of the 2012 ACM workshop on Privacy in the electronic society. [Online] ACM Digital Library pp. 19-30. Available from: http://dl.acm.org/citation.cfm?id=2381970 [Accessed: 6. April 2015]

KRISTOL, D. M. (2001) HTTP Cookies: Standards, Privacy, and Politics. *ACM Transactions on Internet Technology.* 1 (2). [Online] Cornell University Library.
Available from http://arxiv.org/pdf/cs/0105018.pdf [Accessed: 6. April 2015]

LUZAK, J. A. (2014) Privacy Notice for Dummies? Towards European Guidelines on How to Give “Clear and Comprehensive Information” on the Cookies’ Use in Order to Protect the Internet Users’ Right to Online Privacy. *Journal of Consumer Policy*. 37. pp. 547-559.

MANYIKA, J. & ROXBURGH, C. (2011) The great transformer: The impact of the internet on economic growth and prosperity. McKinsey Global Institute [Online]. Available from: https://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/The%20great%20transformer/MGI_Impact_of_Internet_on_economic_growth.ashx [Accessed: 6. April 2015]

MCDONALD, A., M. (2010) Cookie confusion: Do browser interfaces undermine understanding? CHI '10 Extended Abstracts on Human Factors in Computing Systems. [Online] ACM Digital Library. pp. 4393-4398.
Available from: http://dl.acm.org [Accessed: 6. April 2015]

NISSENBAUM, H. (2004) Privacy as Contextual Integrity. *Washington Law Review 79(1)*. New York: Basic Books.

RICHARDS, N. M. (2013) The Dangers of Surveillance. *Harvard Law Review 2013*. [Online] SSRN. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412 [Accessed: 6. April 2015]

SHKLOVSKI, I. et al. (2014) Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. *Proceeding CHI ‘14 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. [Online] ACM Digital Library. pp. 2347-2356.
Available from: http://dl.acm.org [Accessed: 6. April 2015]

SILVERMAN, D. (ed.) (2013) *Doing Qualitative Research: A Practical Handbook.* Fourth edition. London, England: SAGE Publications Ltd.

TANNER, A. (2013) The Web Cookie Is Dying. Here's The Creepier Technology That Comes Next. Forbes [Online]. Available from: http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/ [Accessed: 6. April 2015]

YUE, C., XIE, M. & WANG, H. (2010) An automatic HTTP cookie management system. *Computer Networks*. [Online] ACM Digital Library. 54 (13) pp. 2182-2198.
Available from: http://dl.acm.org [Accessed: 6. April 2014