LSEP ISSUES AND CONSIDERATIONS AND IMPLICATIONS THAT MAY ARISE IN THE WEB DEVELOPMENT THAT USES COOKIES.

Web cookie is a modern-day term that we came across almost every day while using internet. A cookie is basically a storage of data sent from the website when an internet user browses through his web browsers. The function of these cookies is to allow the website to record the stateful information of the user. The primary intended purpose is to use this information to adapt to the user’s preferences and provide him relevant information regarding his browsing activity. The cookies are designed to remember the contents of the online shopping trolleys, some arbitrary information in online forms e.g. the name of the users, their passwords, credit card numbers and their addresses. They are also used to authenticate whether the user is logged in to the website. However, all the access to the user’s personal information has given rise to the privacy concerns.

Anthony D. Miyazaki (2008) discusses the covert nature of the cookies. Third party cookies are placed with the help of ‘clear GIFs’ which are invisible to the users. Although modern browsers allow the users to accept or reject a particular cookie, but the studies show that most of the times the users are unable to use this capability. The FTC (2000) describes cookies as a “nonobvious” means of information collection and their usage can be the violation of user’s privacy. Often Web sites discloses the general use of cookies but the lack of explicit disclosure of any cookies placed by third parties is still considered a privacy violation (Antón, He, and Baumer 2004)

In view of the possibility of privacy violation of internet consumers using cookies has resulted in legislation. The EU and U.S Law makers took steps to ensure the preservation of consumers privacy. EU cookie law is the common name of e-privacy directive. this law was passed in 2002 by EU and further amended in 2009. It aims to secure EU citizen’s online privacy. EU Charter of Fundamental Rights (Article 8) states that

‘’Everyone has the right to the protection of the personal data, such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned’’.

According to the New York Times, [Europe is now the leading tech watchdog in the world](https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html). This is undoubtedly a result of both the EU cookie law in place, and the newer and broader General Data Protection Regulation (GDPR). EU cookie law sets a boundary for websites, service providers and companies for what they can do with consumers personal digital data and what they cannot do without their consent. It also deals with the use of personal data for marketing purposes and how they must handle it as anonymous and protected unless consensual. It also encompasses how it is used and for what purpose they might share it. (cookiebot.com)

The ePrivacy Directive states that **no cookies and trackers must be placed before prior consent from the user, besides those strictly necessary for the basic function of a website**, i.e. that a website has to hold back all cookies, regardless of whether they contain personal data or not, until a user consents.

E.U law requires that the web developers from all the EU countries take informed consent from the users for storing the cookies on their device. World wide web consortium developed the platform for for privacy preferences (P3P). It aims to provide a standard format for privacy policies. Basically, the P3P project was designed to enable the development of tools for making informed decisions about when and if the personal information should be revealed.

EU legislations about cookie privacy is done via regulations and directives. Regulations are automatically and uniformly applied to all the countries without the need for interpretation on a national level. However, directives are the legal actions that every country must adopt and implement in their own ways on a national level. All the EU countries are abided by the law to make legislations regarding privacy of data. However, it must be noted that although there is legislation on the legal issues of cookies and personal data is present, but it is old. The advancement in the field of information technology demands that cookie consent provision be updated. concerns have been raised that the national implementations have created an unlevel playing field with overlapping and fragmented legal realities. In other words: to update, clarify and modernize the 2002 directive into a version that would, like the GDPR, be binding, uniform law in all EU countries.

Despite the legislations on the matter of privacy matters, there are still legal concerns that internet users are dealing with. Primarily it has to do with the law language that a website uses while showing the cookie consent window. Even if a user tries to read it, the law language is beyond the understanding capability of a common internet users. There is also a lack of trust at the part of users as they may never know where their personal data might end up.

Apart from the legal issues related to the web development concerning the use of cookies, many social and ethical issues are surfacing which are completely alien to the aged old social concepts of morality, ethics and privacy. The technology has provided new platforms for socialization and along came the dilemmas as to what and how the social norms of privacy should be standardized. The privacy violation through the cookie has given rise to serious social uneasiness. There is a variety of cookies in nature as well in their purpose of operation. For example Third party cookies who have access to the first party site can potentially be cookies belonging to a social media websites, which track and monitor users’ behaviour on a website. They gain access by “share button” or a “commentary” on the first-party website. In other words, if you have a Facebook share-button on your website, Facebook will also have cookies on your website. What complicates privacy matters here, is the fact that a website owner is legally responsible for what happens on their website, including the protection of all user data from its potential harvest by third-parties for the non-consensual use in profiling and targeted advertisement. (cookiebot.com)

(omar tene and jules Polonetsky in theory of creepy\_) suggests that a shared understanding of social values according to the latest technological capabilities hasn’t yet been established. Consequently, the word “creepy” has become a term of art where social values of privacy do not conform with the web technology. Moreover, the paper suggests that ambient social apps, social listening, personalized analytics and data driven marketing are the modern social tools considered creepy owing to their privacy breaching nature. In February, 2012 the new year magazine ran a cover story revealing the data-driven marketing strategies of a retail giant Target who went a step way further in their advertising campaigns. The New York Times discovered that Target assigns customers a pregnancy prediction score, which is based on their purchase habits, in order to beat its competitors in identifying a precious moment when shopping habits are most amenable to change-the birth of a baby. According to the New York Times, Target employed statisticians to sift through buying records of women who had signed up for baby registries. This along with some other personal data of the consumers Target could accurately predict a customer’s pregnancy and even her due date. Public opinion condemned Target’s covert marketing operation although upon later investigation it was found out that nothing illegal was carried out but still too much intrusion into people’s personal lives made them uneasy.

(Andrew Mc Stay, I consent: an analysis of the cookie directive……..) discusses that behavioural advertisers have been using the informed consent but it might lead to concerns about ethical practices. Behavioural advertising tracks users’ browsing activities to understand the user’s interests and provide this data to the networks which are the third party in the form of advertising networks. In order to deliver targeted advertising, they gather the user’s personal information from the websites the user visited. The paper explains that these third-party cookies is a technological loophole which allows the owners of third-party components of a web page to insert their own cookies. This helped the flourishing of behavioural advertising industry which is perceived as a privacy threat as they sometimes generate ethical concerns

In the web development the use of cookies can create ethical issues as the behavioural advertisers, discussed earlier, could prey upon the user’s weaknesses. For example if a user who is addicted to gambling or gaming is trying to get rid of his habits, and uses internet the behavioural advertising websites knowing the interests of the user can use his weakness and provide him recommendations about gambling or gaming etc and the user might get trapped in the cycles of temptations. The debate arises that the user could have easily overcome his habits if the temptations in the form of recommendation never appeared on his computer screen. Another ethical concern regarding the use of cookies in the web development is that the users do not necessarily understand where their data is being processed and used. The debate arises that users click ‘I consent’ when the cookie message pops up, so the privacy is not breeched but in many cases we as participants are partly blameworthy in our own scrutiny, as we offer up personal details for services and rewards although, as Lanier and Saini (2008) highlight, such incentives can only be truly ethical and voluntary when consumers fully understand the nature of the bargain. Most of the times the user’s choice about cookie consent is conditioned as they do not understand the full implications of their consent as to what and how their data is processed. Turow’s (2003) empirical investigation of privacy seems to suggest this. His participants were unclear on both the nature of data processing and how to protect their personal information. When the techniques employed by online organizations were revealed to them, participants were unhappy (also see LaRose and Rifon, 2006).

The breach of privacy via third part cookies could be a serious concern professionally. Adopting to the technological advancement of the modern day, every professional is somehow connected to the world of web. The professional information stored on various professional websites is used for finding better prospective jobs. Third party cookies might help the companies looking for the employees looking for relevant jobs. However, it might create a leakage of personal information that the user might not like to share with his employers.

The issue of breach of privacy in the web development has been raised at various national and international political forums. It is because of these political voices that legislations on the subject matter of privacy has been done.

In order to understand all aspects of the matters of privacy, it is essential that we understand the philosophical concept of consent which the web uses to store their cookies. (I consent:……..)The notion of consent flows from liberal conceptions of freedom. Freedom is the belief in free choice, voluntariness, autonomy and privacy. Privacy serves to guarantee autonomy and the right to personal choices. In accordance with Kant’s universalizing principle we should not restrict the autonomy of others. The right to privacy is in fact the extension of the right to autonomy. Therefore, philosophically the preservation of one’s privacy be it in the virtual realm is essential to the basic human rights.

The web development using cookies has economic issues concerning privacy. (Jonathan R. Mayer and John C Mitchell, third party web tracking :policy and technology) discusses that webpages are increasingly composed of content from third party websites in various businesses like social networking, advertising, analytics and many more. Although these third party have a huge value as they support free content and facilitate we innovation but these services come at the cost of privacy. (feng Xu , Factors affecting privacy disclosure on social network sites) shows concern about the exploitation of personal web data that has a negatively impacted on online business transactions and online social activities. Previous studies estimate that that the decreasing levels of user’ trust caused by privacy concerns have led to heavy losses in business-to consumer online business. It can be deduced that a trustworthy online relationship with consumers could lead to the flourishment of internet economy all over the world. The protection against fraud and the leakage of one’s personal data e.g. the protection of users’ credit card numbers, bank details and passwords will ensure a convenient internet usage. The dispelling of scepticism about one’s privacy breach will provide peace of mind to the users.