ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 8.4
IJAR 2022; 8(8): 175-178
www.allresearchjournal.com
Received: 29-04-2022
Accepted: 11-07-2022

Himanshi Singh
Institute of Legal Studies and Research, GLA University, Mathura, Uttar Pradesh, India

Rohit Solanki
Institute of Legal Studies and Research, GLA University, Mathura, Uttar Pradesh, India

Corresponding Author:
Himanshi Singh
Institute of Legal Studies and Research, GLA University, Mathura, Uttar Pradesh, India

Web cookies: A potential threat to users' privacy

Himanshi Singh and Rohit Solanki

Abstract
In this modern world, people are mostly concerned about their privacy but most of the time people do not really know about the things which they encounter in the cyber space yet they enter into it.
Web cookies are used over the internet to collect users' personal data and the basic task of the cookies is to enhance the experience of the user on the website and to show user centric content, but this data is also accessed by the third parties, hence making the user vulnerable to be the victim of breach of privacy.
This paper discusses the Concept of cookies on the internet and how it poses a potential threat to users' privacy. This paper raises an issue regarding the confidentiality of the data provided by the users. It also mentions India's position in protecting the privacy of users over internet space. A brief study of the international legal system relating to data privacy has been done in this research paper.

Keywords: Web cookies, potential threat, legal system

1. Introduction
In everyday life when a person accesses any website while surfing the internet, there appears a certain pop up messages on the screen. Usually people ignore the content of the pop up and directly accept and proceed to the website. These pop ups are generally called cookie policies of that website.
Cookies are essential tools on websites to gather the information from the users. A text box pops up on the web page while using that page. Either user can accept or decline the content of the pop up. The content of the pop up contains the information regarding the cookie policies of the website. It contains the information about how the website is going to use the data provided by the user. When accepted, the website cookies start tracking the activities of the users on that web page. It collects information about how the user interacts with the website, their preferences and their personal information provided by them. The website uses cookies to enhance the experience of a user.
Most Internet users do not know about these policies and they accept it without considering them and proceed with the website. These cookies used by the websites have potential to violate the privacy of users, as it stores the personal data of users, they track their login activities. No person can feel comfortable knowing that someone is keeping an eye on him. This is an infringement of their privacy which should not be taken lightly. Privacy has always been subject of concern among people in the society.
The term Privacy can be defined as the state of being alone and not watched or interrupted by other people. Privacy enables an individual to manage boundaries and create barriers to protect himself/herself from unwanted interference. Privacy helps us establish boundaries to limit who has access to our bodies, places and things and also includes communication and information. (Bitdefender.com, n.d.)
Privacy is one of the qualified Fundamental Human Rights. The provision of privacy as a human right is articulated in almost all of the major international as well as regional human rights instruments. (Privacy international, 2017)
Privacy of an individual has become a major concern in this digital era. When an individual is scrolling through his/her phone he/she might be physically alone. However, one can also be watched or interrupted by other people 'digitally', hence, acting as a data point someone is following. One may consider this situation as private but it is not the case.
The definition of online privacy covers the natural expectations of an individual to have his/her personal data protected and to prevent tracking of behavior with any explicit consent

while connected to the Internet. (Bitdefender, n.d.)

2. What are cookies?

When an individual visits a website, his browser saves little text files called cookies. The website provider can then save information on the users' computers, such as their username and password that can be accessed next time the user visits the website. It can be said that cookies are advantageous to the website's users, allowing them to utilize specific features. Cookies can be used by website providers to collect information about the user and his behavior on the website. This information can be used to create user profiles in order to customize the advertisements that are displayed to users on the website.

Cookies are also helpful in session management. A user remains logged in over the course of a single user session. It also provides the option to the user to remember the user's profile through the login credential. It helps in multiple- tab browsing.

The cookies are distinguished mainly into three types

I. Session cookies
II. Persistent cookies
III. Third-party cookies

Session cookies that remember a user's online actions are also known as temporary cookies. Without these cookies, the user's site browsing history would always be blank because websites have no sense of memory. In fact, the website would treat the user as if he were a brand-new visitor with each click. Online purchasing is a good example of how session cookies may be useful. When shopping online, a customer can check out at any moment. This is due to the fact that session cookies keep track of his movements. If he didn't have these cookies, his cart would be empty every time he went to check out. Session cookies, in the end, assist a user navigate the internet by remembering his actions, and they expire when he closes a web page.

Persistent cookies (sometimes referred to as first party cookies) track your online preferences. When a user first visits the website, it is set to its default settings. Persistent cookies will remember and implement users' preferences the next time they visit the site if it is customized to their interest. This is how computers remember and store the information such as login credentials, language choices, settings etc. Persistent, permanent and stored cookies are all phrases that refer to cookies that are saved on a computer's hard drive for a long time and duration is determined by the expiration date. Once that date has passed, the cookie, along with everything the user has modified, will be destroyed.

Third party cookies, often known as tracking cookies, collect information about a user's online activities. These cookies collect various types of data when a user visits a website, which is subsequently passed on or sold to advertisers by the website that created the cookie. It collects information about interest, age, location, and search pattern so that the advertiser can show customized advertisements to the user. These advertisements that appear on the websites a user visits are relevant to his/her interest. Third party cookies serve a crucial role for advertisers by analyzing the behavior and providing customized advertisements, but they can appear troublesome and invasive to user's internet privacy. (Dutko & Gehring, 2018) [2].

3. How do cookies violate the privacy of users?

Though cookies were intended to improve online experience by remembering information about the users, the possibility of malicious actus using cookies to comply with persons unique profiles on individuals has been identified as a danger to the user's privacy. (Getterms, n.d.)

3.2 User's perceptions and reaction to the internet cookies

There was a survey conducted by Karlsruhe institute of technology, Germany about the user's perception and their reactions to the cookies. The survey is based on the questions regarding how a user reacts towards the cookie's disclaimers and about their perceptions regarding the same.

It was found that, out of 150 people surveyed, a majority of people considered cookie disclaimer as a disturbance in their web surfing, because the disclaimer covers a significant portion of the screen and hides the content of the website. Another portion of participants were concerned about their privacy and they felt being observed while using the website.

Many participants have become used to the cookie's disclaimers on the website because they frequently face such disclaimers while surfing the internet. It does bother them and they act in a neutral manner. It was also found that most of the participants were not aware of the consequences of cookies to their privacy. They are unaware of the facts about what information is collected and how it is to be used by the website. It makes them nervous as they do not know what it means to allow cookies and what may be the consequences of it. (Kulyk *et al*., n.d., #) [5].

A user must only be aware of third-party cookies. This is the type of cookie that irritates users' privacy. These cookies are also known as marketing cookies, tracking cookies as well.

3.4 When an advertiser who has paid to display his ad at a particular website on a per-view basis, he and the site both want to know how many times that ad has been viewed. This concept is very straightforward. The advertisement includes code that places a cookie on the computer of the user when he uses third party cookies. The advertiser, the website and the user are all identified by the cookie. The advertiser can not read the identity of the user because it is encoded. However, it does give a distinct identity to the user.

When any user encounters the same ad on a different website, the browser cookie is updated to reflect that he has seen that ad before. The site is then edited to the list of sites where the user has seen the advertisement. The advertiser now has knowledge about the website a user visits, The advertiser is unaware of his identity. Although personally identifiable information is encrypted, a list of websites is linked to an encrypted value that identifies him.

The power of tracking cookies can be estimated by the fact that a user browses for a particular product at any online store then the ads for similar products start following him around the internet. Cookies do not contain any information that identifies the user. However, in the event of a data breach, the encrypted user identity could be linked to his online username or even the real name. Even the browsing history of the user may become a matter of a public record.

4. Legal Frameworks in India

Presently, India has no specific Act or law for protection of Data. There is no legislation regarding the infringement of

data and information but some provisions of (IT) Information technology Act of 2000, and (SPDI) Sensitive Personal Data and Information Act of 2011 are functional in this regard. In the case of K.S. Puttaswamy v. Union of India, the Supreme Court ('SC') ruled that the right to privacy is a fundamental right guaranteed by Part III of the Constitution. Furthermore, it stated that the user's personal information could not be used without the user's consent. Cookies, on the other hand, are not considered personal information in India. This allows websites to issue many sorts of cookies, both essential and superfluous cookies, to users' devices without their consent.

As there is no cookie law, Indian companies can use personal data to their benefit according to their wish. Many claim that using cookies without the user's consent falls under the definition of "computer virus" in the IT Act and is thus unlawful. However, in the lack of clear legislation or legal precedence governing cookies, businesses may be able to bend the law by identifying technical flaws in the definition. Websites, for example, may argue that cookies are not dangerous or malevolent. As a result, cookies cannot be definitively included in the concept of "computer virus." (Kumar, 2021) [6].

Websites are governed by legally binding agreements regulated by the Indian Contract Act, 1872, which require users to agree to the terms and conditions as displayed to them when the terms and conditions of a privacy policy are indicated. The Consumer Protection Act, 2019, governs such websites and contains important provisions related to consumer data privacy. According to Section 2(46) of the Consumer Protection Act, any unreasonable imposition of a condition on consumers that certainly puts them in jeopardy would be treated as an unfair contract under unfair trade practices. (Rai, 2021) [8].

There is a need for specific legislation or Act for the protection of individual's privacy as there is an increase in the cases related to data protection. As we all know everything is online nowadays so there are chances of more risk in the internet space or internet world. People are more into internet space; they use the internet in a day-to-day life then there are strong chances of infringement.

Despite the fact that the new Personal Data Protection Bill of 2019 has not yet been passed, it should be amended. Personal data is defined in this law as any information about a natural person that may be used to identify that person directly or indirectly. This clearly refers to the identification of data on a natural person. Cookies, on the other hand, do not often have the capability of identifying an actual person, therefore this is beyond their scope. Personal data cannot be irreversibly anonymized, according to experts, and organizations that utilize browser history to identify individual users risk being de-anonymized. (Rai, 2021) [8].

5. International frameworks regarding regulation of cookies

5.1 The ePrivacy Directives

The eprivacy directive, often known as the European cookie law, is a piece of European law that mandates the websites to obtain users' agreements before storing, processing or retrieving their information. The e- privacy directives was the first legislation to demand that sites acquire prior consent from EU based users before using trackers and cookies to process their data. E-privacy directives, when combined with the general data protection regulation (GDPR), creates one of the strictest privacy regimes in the world. (Komnenic, 2022) [4]

5.2 General data protection regulation (GDPR)

Companies which collect data on citizens in EU countries must adhere to know data protection regulations. The GDPR establishes a new standard for customer data rights. The GDPR is world's toughest privacy and security law. Despite the fact it was drafted and passed by the EU, it imposes duties on organizations anywhere that targets or gathered data about EU citizens. On 25 may, 2018, the regulation went into effect, though it was adopted by European parliament in April 2016. GDPR replaced the outdated e-privacy directives from 1995. It contains regulation requiring companies to respect EU citizens' personal data and privacy for transaction that takes place within EU member states.

GDPR defines personal data as any information that can be used to identify an individual, either directly and indirectly. It includes names, email addresses, location, ethnicity, biometric data etc. The person whose data is processed is known as a data subject. The person who decides for what purpose the data would be use and how it would be processed is called a data controller, and any third party that processes data on behalf of a data controller is known as a data processor.

GDPR mentions several data principles in order to process data. These outline in article 5.1-2

- Lawfulness, fairness and transparency.
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

The GDPR takes a wide view of what constitutes personal identification information. Companies will require the same level of security for IP addresses and cookies data as they do for a user's names, address and social security number. GDPR requires the organizations to ensure the data subject that collected data would be stored safely and they will be held liable in case of any data breach. GDPR also provides fines and penalties to be imposed on the non-complying organization and companies.

5.3 Case Study (Planet 49 Case)

In 2013, a German website known as Planet49 GmbH, held an online promotional lottery. Users had to input their postal code to enter the lottery, after which they were required to provide their names and addresses. This website sought to consent from users beneath this request for names and addresses. The first consent was allowing third parties to contact users with promotional offers. The second consent was for cookies to be dropped on users' browsers in connection with online lottery participation. Planet49 used an unticked box to obtain consent for third party promotional offers, and a pre-ticked box to obtain consent for the use of cookies.

In order to take consent from the users the Planet49 should have used unticked boxes for the both consents. In this case, use of a pre-ticked box implies that the condition has been already imposed on the users without taking their consent. According to The Court of Justice of the European Union

(CJEU), a pre-ticked box does not provide legitimate consent or the use of cookies or similar technology. The court began by looking at the e-Privacy directive which clearly requires consent for the storage or excess to information contained in a user's computer system. However, the ePrivacy directive does not specify how consent must be given. The court used literal interpretation for the phrase 'provided his/her consent' and held that the user must give an indication of their preferences. The user must take action which must be active and not passive. (Kurth, 2019) [7]

6. Conclusion

Cookies enhance the performance of the website while surfing and also the experience of the user. There are various types of cookies which are used by the website. Only certain types of cookies pose a threat to users' privacy.

The third-party cookies - the tracking cookies used by marketers - are the ones that pose a privacy concern. By using an ad blocker or setting the browser to reject third-party internet cookies, or changing the preferences of the cookie's disclaimer on the website to only utilize first party cookies, users can eliminate the danger.

According to Recital 30 of the General Data Protection Regulation (GDPR), the collection of cookies by websites and other non-specific data may result in the profiling of an anonymous user. As a result, in order to safeguard people' privacy, it is critical to develop a cookie law or complete personal data privacy legislation that includes measures controlling cookie usage.

The user can also keep him safe by clearing cookies and cache on a regular basis. India, currently does not have any dedicated legislation regarding data privacy and regulation of internet cookies but there exist several different acts which contain certain provisions regarding data privacy. The Indian parliament has also proposed a PDP (personal data protection) bill in 2019 which is pending approval by the legislature.

The EU (European Union) has a dedicated law that regulates data privacy of the citizens of the member countries. Initially the EU had e-Privacy directives for this purpose which was later replaced GDPR (general data protection regulation) in 2016. The GDPR is considered to be the toughest privacy and security law in the world and it imposes obligations onto organizations anywhere in the world if they target or collect data of people in the EU.

The solution to all ambiguities in various privacy legislations is a complete cookie policy law that is jurisdiction-based, which would be advantageous in addressing interpretational issues and ensuring effective enforcement. Enforcing a cookie legislation will also safeguard firms' economic interests while eliminating privacy problems by implementing penal requirements under such laws.

7. Acknowledgement

We are very grateful to Ms. Ankita Sharma, Assistant Professor, Institute of Legal Studies and Research, GLA University, Mathura, for her valuable inputs and her guidance.

We are thankful to Dr. Abhishek Trivedi, Assistant Professor, Institute of Legal Studies and Research, GLA University, Mathura, for allowing us to write this Article and inspiring us for this present research.

8. References

1. Bitdefender.com. (n.d.). What is Online Privacy? Bitdefender. Retrieved May 12, 2022, from https://www.bitdefender.com/cyberpedia/what-is-online-privacy/
2. Dutko J, Gehring J. How Computer Cookies Affect Your Online Privacy. CRU Solutions, 2018. Retrieved May 23, 2022, from https://crusolutions.com/blog/how-types-of-computer-cookies-affect-your-online-privacy/
3. Getterms. (n.d.). How cookies impact online privacy. GetTerms.io. Retrieved May 13, 2022, from https://getterms.io/blog/how-cookies-impact-online-privacy/
4. Komnenic M. Cookie Law Guide for Businesses: EU, US, and the UK. Termly, 2022. Retrieved June 09, 2022, from https://termly.io/resources/articles/cookie-law/#what-is-the-eu-cookie-law
5. Kulyk O, Hilt A, Gerber N. (n.d.). This website uses cookies: Users' Perception and Reaction to the Cookies Disclaimer.
6. Kumar A. Cookies Crumbling: India Needs a Cookie Law – Law School Policy Review & Kautilya Society. Law School Policy Review & Kautilya Society, 2021. Retrieved May 21, 2022, from https://lawschoolpolicyreview.com/2021/07/13/cookies-crumbling-india-needs-a-cookie-law/
7. Kurth HA. CJEU Reaches Decision in Case Involving Cookie Consent under EU Data Protection Law. Privacy & Information Security Law Blog, 2019. Retrieved June 05, 2022, from https://www.huntonprivacyblog.com/2019/10/03/cjeu-reaches-decision-in-case-involving-cookie-consent-under-eu-data-protection-law/
8. Rai D. Enforcement of Cookie Policies. iPleaders, 2021. Retrieved May 21, 2022, from https://blog.ipleaders.in/enforcement-of-cookie-policies/#Position_of_Cookie_Policy_in_India