

GUARDING PRIVACY IN ELECTRONIC AGE: WEB COOKIES ARE THREAT TO FUNDAMENTAL RIGHT TO PRIVACY

Nancy Dhillon

Research Scholar, Department of Laws, Bhagat Phool Singh Mahila Vishwavidyalaya,
Khanpur Kalan, Sonipat, Haryana.

Dr.Parmod Malik

Assistant Professor, Department of Laws, Bhagat Phool Singh Mahila Vishwavidyalaya,
Khanpur Kalan, Sonipat, Haryana.

Abstract---PRIVACY is one of the grave issue in present time. Today, internet availability is arguably the cheapest and fastest it has ever been. Anyone with easy internet access and basic computer knowledge can enter the digitized world in the blink of an eye. This research paper aims to explore the rights to PRIVACY of individuals and the necessity of protecting those rights in the face of advancing cyber technologies. Individual privacy, particularly in cyberspace, is at greater risk than ever before. The researchers assume that the violation of the fundamental right to PRIVACY necessitates providing essential protection as a guardian under Constitution of India. This research paper aims to understand the threats posed by e-surveillance and Web cookies tracking upon PRIVACY in India and to examine the existing laws on the data protection of an individual.

Keywords---Dark web, E-surveillance, India, PRIVACY, Web cookies.

I. INTRODUCTION

IN the era of internet and technology, online surfing has become an integral part of daily life, leading to an increasing concern about data privacy and security among users. Monitoring and tracking of online activities of users is a serious threat to PRIVACY of an individual. From websites to applications installed on smart devices, to smart watches and to cameras in public places – all are monitoring and storing information of an individual with or without their consent. People are unaware that their privacy has been infringed by such online activities.

Due to continuous evolution of technology, the concern of privacy and security is growing among internet users. Most of the population in India are having little understanding about web cookies and e-surveillance. A proper insight in the behaviour and uses of web cookie is also very important. Protection of data stored by web cookies is also very important because users don't feel safe while surfing the internet. Although web cookies are unable to identify the true identity of a user but it can become a serious threat to PRIVACY of a user through Cookie Hijacking and Cookie Tossing.

E-surveillance is used by government agencies to control the crimes like terrorism, to protect the sovereignty and integrity of India and to maintain good foreign relations with other countries. However, there is always a threat to the individual right to PRIVACY. In *KHARAK SINGH V. STATE OF UTTAR PRADESH (AIR 1963 SC 1295)*, Justice K. Subba Rao has held that broad surveillance powers are threat to right to privacy of innocent citizens.

India being a rapidly growing digital market, faces significant challenges regarding PRIVACY and data security. Recently on 11th August, 2023 new Act has been assented by the president. This Act is called "The Digital Personal Data Protection Act, 2023". This Act enables the processing of digital personal data in a way that acknowledges both the right of an individual to have their personal information protected and the necessity to use that information for authorised purposes. The rights, responsibilities, and obligations of the data principal and data fiduciary are laid down in this legislation. The Data Protection Board of India, a legitimate regulatory body, is to be established in accordance with its rules.

The researchers aim to identify the awareness among internet users and to examine the existing laws on the protection of PRIVACY of an individual in India.

II. DEFINING WEB COOKIES AND E-SURVEILLANCE:

Web browser programmer LOU MONTULLI is credited with creating the term "Web cookies". Web cookies are the small text files saved on users devices by websites. When a user visits a website, a hypertext transfer protocol cookie is created, and the website uses this cookie to track the user's activity. When a user accesses a website, the browser sends the cookie value to the server to let it know what the user has previously done. Not every cookie is threat to privacy, there are only some of them like third party web cookie. As part of the web cookie information, web cookies typically hold the following information: name, web address, authorised cookie path, expiration date, and security information. Web cookies has play an important role in tracking user behaviour and collecting personal information.¹

The French words "sur" and "veiller," which translate as "to watch over," are the origin of the English word "surveillance". E-surveillance is the new form of surveillance which store and monitor the online activities of individuals with or without their consent. E-surveillance has been conducted by various

¹ Shehu Mohammed Ahmed, Song Shombot Emmanuel, and Avong Emmanuel John, 'Security and Privacy Concern of Web Cookies, with User's Understanding and Management of their Web Cookie' (2020) 9(3) International Journal of Computer Science and Network.

government agencies and business entities. Monitoring and storing of personal information of people amount to infringement of their right to PRIVACY.²

III. RELATIONSHIP BETWEEN WEB COOKIES AND E-SURVEILLANCE

There are basically two categories of web cookies. First one are those web cookies which are stored on the web browser of your device and second one are those which collect data from your browser and send it to website server. Web cookies are necessary for the websites. They are not in itself violating PRIVACY, rather the purpose or usage of web cookies decide whether they are good or bad. Web cookies were made to improve the online experience of the internet users by remembering their data but some malicious acts and usages by third party has been caused breach to their PRIVACY.³

Third party web cookies are used for mass surveillance. Monitoring and storing of data can be done through various ways such as websites, CCTV cameras, social media, various applications on smart devices etc. In digital age, web cookies and e-surveillance are used for monitoring and storing the activities of internet users. Web cookies and e-surveillance are used as a tool for cybercrimes and to infringe PRIVACY of individuals.

A. BREACH OF PRIVACY

In 2023, India has 1.2 billion internet users across the country. COVID-19 has been responsible for such an increase in number of internet users. Due to covid-19, people became totally dependent upon internet facilities. Pandemic has changed the way of life of people. At the start of the lockdown period, the Telecommunication Department of India consumed 307,963 TB (Terabyte) or 308 PB (Tera Bytes) of internet data daily. According to Openvult's Broadband Insight Report, the average broadband consumption of data has increased to 402.5GB from 273.5GB, which was roughly 47 percent in 2019. Lockdown caused the bandwidth use to rise from 190.7GB in the fourth quarter of 2019 to 233.6GB in the first three months of 2020. This data indicates a dynamic growth of internet users in India.⁴

² J Lakshmi Charan, 'E-Surveillance On Telecommunications And Privacy Issues In India' (2019) 6(1) International Journal of Legal Research
<https://www.academia.edu/96639491/E_SURVEILLANCE_ON_TELECOMMUNICATIONS_AND_PRIVACY_ISSUES_IN_INDIA> accessed 20 September 2024.

³ Himanshi Singh and Rohit Solanki, 'Web Cookies: A Potential Threat to Users' Privacy' (2022) 8(8) International Journal of Applied Research 175-178.

⁴ Rabi Narayan Subudhi and Debajani Palai, 'Impact Of Internet Use During Covid Lockdown' (2020) Horizon <<https://horizon-jhssr.com/view-issue.php?id=64>> accessed 20 September 2024.

In 2022, India was ranked as second largest online market in world.⁵ Such a growth in internet users has raised concern about PRIVACY. Some internet users are aware about their online activities and understand their right to privacy but some users are unaware about their PRIVACY. Breach of their PRIVACY does not seems important to them and they just use internet blindly and does not pay any heed towards their right to PRIVACY. Such kind of internet users share or disseminate their Personal data even on unencrypted websites that result in breach of their PRIVACY.

"Digital personal data" refers to personal information that is stored digitally. Personal data breaches include any illegal processing of personal data as well as unintentional acquisition, sharing, use, alteration, destruction or loss of access to personal data that jeopardises their confidentiality, integrity, or availability of personal data.⁶ There is a relationship between internet literacy, social awareness and PRIVACY. For example, personal data protection of an individual depends upon how effectively an individual has used internet platforms. Internet users should be aware about, how their personal data has been used without their consent.

In 2022, personal data of 6 lakh Indians has been sold on dark web with the help of bots. Stolen personal data includes user logins, web cookies, fingerprints, passwords, and credit or debit card information etc. Digital bots were used to do shopping, booking tickets and accessing government and private services but they were also used for stealing data. Once these malware bots were installed in user's device, they started to sniff in user's device and detected valuable personal data. It becomes very difficult to stop sharing or dissemination of personal data from dark web network. Internet users should be aware before using unauthorised applications and websites and should not access unencrypted data.⁷

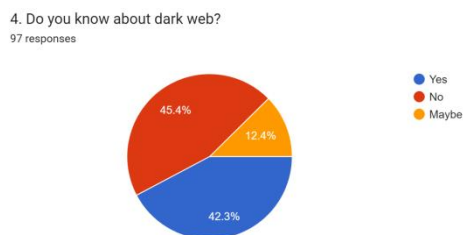


Fig. 1 Awareness about dark web among internet users

⁵ 'Data of 600,000 Internet Users in India Being Sold on Dark Web via Bots: What Are They and How They Operate' The Times of India (8 December 2022) <<https://timesofindia.indiatimes.com/gadgets-news/data-of-600000-internet-users-in-india-being-sold-on-dark-web-via-bots-what-are-they-and-how-they-operate/articleshow/96084441.cms>> accessed 20 September 2024.

⁶ The Digital Personal Data Protection Act 2023 (No 22 of 2023).

⁷ 'Data of 600,000 Internet Users in India Being Sold on Dark Web via Bots: What Are They and How They Operate' The Times of India (8 December 2022) <<https://timesofindia.indiatimes.com/gadgets-news/data-of-600000-internet-users-in-india-being-sold-on-dark-web-via-bots-what-are-they-and-how-they-operate/articleshow/96084441.cms>> accessed 20 September 2024.

5. Do you know your personal information may sold on dark web?
 97 responses

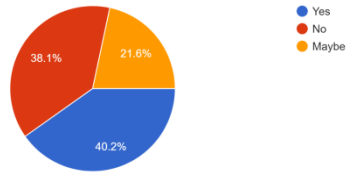


Fig. 2 Awareness among internet users that personal information may sold on dark web

Researchers have conducted a survey on approximately 100 internet users and had found that almost 50 percent internet users were not aware about darkweb and even have no idea that stolen information may be sold on dark web and uses for illegal purposes.

B. GLOBAL ISSUE.

Individual's right to privacy has not only become a concern in India, rather it is a global issue. Web cookie tracking and e-surveillance has no boundaries, a person sitting in America can easily access the information of an Indian citizen with the help of website tracking. The issue of PRIVACY spread cross borders because internet has no limits. Globally around five million people have been facing the problem of breach of their PRIVACY. Without their consent, their personal information is being sold online.

General data protection regulation was passed by European Union and it is the world's toughest privacy law. This regulation is applicable on any organisation which targets or collects personal data of EU citizens. It imposes an obligation on to respect the privacy of EU citizens. It describes personal data as any information that can be used to directly or indirectly identify a specific person. For example- name of internet users, their email addresses, location, fingerprints etc. It defines the individual whose data is processed as the data subject, the one who elects how the data will be used as the data controller, and any third party who processes personal data on behalf of the data controller as the data processor. In accordance with GDPR, business entities are required to preserve data subjects' information securely and are accountable if their PRIVACY is violated. The GDPR has also imposed fines and penalties on organisations and companies that violate its provisions, including Art. 83(4) GDPR up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the prior fiscal year, whichever is higher and Art. 83(5) GDPR up to 20 million euros, or, in the case of an undertaking, up to 4% of its entire global turnover of the prior fiscal year, whichever is higher.⁸

⁸ Michael Iheanyichukwu Godwin Onugha, 'Internet Privacy In 2020' (2020) ResearchGate
 <https://www.researchgate.net/publication/347362107_INTERNET_PRIVACY_IN_2020> accessed 20 September 2024.

C. RECENT TRENDS IN INDIA

The DIGITAL PERSONAL DATA PROTECTION ACT, 2023 is a new law that the Indian government has passed to protect personal data. On August 11, 2023, the President of India gave his approval to this Act. It intends to make provisions for processing of digital personal data in a way that acknowledges both the necessity to handle such data for authorised purposes and the rights of individuals to have their personal data protected. This Act maintains an acceptable balance between the right to privacy of the individual and national security of India. The Act applies to all organisations or companies whether they are public or private. Any third party that processes personal data on behalf of a data fiduciary is referred to as a data processor. It describes the individual whose data is processed as a "data principal" and the person who decides how the data will be used as a "data fiduciary".

The Act states that only in legitimate purposes and in accordance with its rules, principal's personal information may be used to process a data. Such data cannot be used without the data principle's permission, which must be obtained in writing and includes a notice. Such notice informs data principle:

1. For which purpose the data will be used
2. Data principal's right to withdrew consent
3. Complaint procedure in case of (any) breach.

On the grounds of national security and to stop the commission of any crimes that are punishable by law, the central government has the authority to exclude its agencies from the provisions of this Act. The central government is given enormous power by Section 7 of the Act, which raises the possibility of data misuse.⁹

TABLE I
PENALTIES¹⁰

Sr. no.	Breach of provisions under THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023	Penalty

⁹The Digital Personal Data Protection Act 2023 (No 22 of 2023).

¹⁰ The Digital Personal Data Protection Act 2023 (No 22 of 2023).

1	Breach of the Data Fiduciary's duty to follow Section 8(5)'s requirement that it take adequate security precautions to avoid the loss of personal data	May increase to 250 billion rupees.
2	Breach of the requirement to notify the Board or the affected Data Principal of a personal data breach as required by section 8's subsection (6).	May increase to 200 crore rupees.
3	Violation of section 9's special responsibility in relation to minors.	May increase to 200 crore rupees
4	Breach of the Significant Data Fiduciary's additional section 10 duties.	May increase to 150 crore rupees.
5	Violation of the obligations outlined in section 15.	May increase to 10 thousand rupees
6	Any violation of a term of a voluntary undertaking that the Board has accepted under section 32.	Up to the extent applicable for the violation for which the section 28 proceedings were commenced.

7	Any other violation of this Act's or its implementing provisions.	May increase to 50 crore rupees.
---	---	----------------------------------

TABLE I lists severe consequences in the event that this Act's rules are broken. It demonstrates the legislature's plans to create robust legislation to safeguard the personal information of internet users.

TABLE II

COMPERATIVE CHART

SR . no.	Subject	INDIA	USA	UK
	Number of internet users	759 million Over 50 percent	297.3 million Approximately 90 percent	66.1million Approximately 97 percent
	Data protection law	The Digital Personal Protection Act,2023, and Information Technology Act,2000	Privacy Act of 1974, Children's PRIVACY Protection Act,1998 (COPPA), and	The Data Protection Act, 2018

			Californ ia consume r Privacy Act, 2018	
	Maximu m Penalty for breach	250 crores	40,000 USD under COPPA	17.5 million euro or 4% of its entire global turnover of the prior fiscal year, whichev er is higher

IV. CONSTITUTIONAL RIGHT TO PRIVACY

In India, the constitution doesn't define privacy. The concept of privacy has been brought in India by judicial precedents. In the world of technology people process more data through online platform, this arose a need for the protection of right to PRIVACY. The fundamental right to privacy of a person is defined and protected by numerous judicial decisions in India.

The supreme court of India ruled in the first case involving the right to privacy, *M.P. Sharma and Ors. v. Satish Chandra, District Magistrate, Delhi and Ors. (1954 AIR 300)*, that the right to search and seize property under sections 94 and 96(1) of the Criminal Procedure Code, 1973, does not contravene any provisions of the Indian Constitution. Therefore, the right to privacy is not recognised as a basic right in the Indian Constitution.

The Supreme Court ruled in the case of *Kharak Singh v. State of Uttar Pradesh and Ors* (AIR 1963 SC 1295) that nighttime home surveillance of the accused was against Article 21 of the Indian Constitution. The majority of judges have ruled that Article 21 does not encompass the right to privacy, however Justice K.Subba Rao has held, in a minority opinion, that such powers pose a threat to the right to privacy of law abiding citizens.

The Supreme Court ruled in *Govind v. State of Madhya Pradesh* (1975 4 SCC 373) that the right to privacy is a basic freedom and should be exercised in accordance with each case's facts and circumstances.

The Supreme Court has expanded the scope of Article 21 and determined that the right to privacy is an essential component of the right to life under Article 21 in the case of *Maneka Gandhi v. Union of India* (1978 AIR 597).

R. Rajagopal and Anr. v. State of Tamil Nadu (1994 SCC (6) 632) (*Auto-Shanker Case*) was the first case to analyse the range and development of the right to privacy. The Supreme Court ruled in this case that even if the right to privacy is not expressly mentioned in Article 21, it is nonetheless a crucial component of that article.

The Supreme Court has decided in the case of *People's Union for Civil Liberties (PUCL) v. Union of Indians* (AIR 1997 SC 568) whether telephone tapping infringes one's right to privacy or not. The court ruled that telephone conversations are an individual's personal records. Thus, telephone tapping infringes a person's right to privacy.

In the famous ruling of *K.S. Puttaswamy (Retd. Justice) and Anr. v. Union of India and Ors* ((2017) 10 SCC 1), the court unanimously ruled that Articles 14, 19, and 21 of the Indian Constitution include the right to privacy. Additionally, it was decided that the state has a responsibility to safeguard its people's privacy and that individuals have the right to legal redress in the event that their data privacy has been violated. This judgment has brought a wave of awareness among Indian citizens for their data privacy.

V. CONCLUSION AND SUGGESTIONS

Web cookies are proven tool to intrude in the PRIVACY of Data Principal without their consent. Consent is well protected in India via The Digital Personal Data Protection Act. This Act has retrospective effect with respect to consent of Data Principle. It protects the consent of internet users who has given her consent before commencement of this Act.

No doubt this Act is competent to make a balance between individual privacy and national security but there are some other factors which affects the competency of this Act. For Example--- there is a huge gap

between number of active internet users and literacy rate in India. Without being aware about their rights, people cannot protect them. This Act alone is not sufficient to protect the right to PRIVACY of individuals.