Long Arm of Law Reaches in Cyberspace: Protecting Right to Privacy in Digital Era

By

Dr. G A Solanki
Associate Professor Faculty of Law the Maharaja Sayajirao University of Baroda Vadodara
E: Mail: lawspider2001@yahoo.com

Abstract

The right to privacy is a fundamental human right that has become increasingly important in the digital era. With the rise of technology and the internet, people are generating and sharing more personal information than ever before, and this information can be easily accessed by governments, corporations, and other third parties. The right to privacy is enshrined in International Human Rights Law, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. It includes the right to control how one's personal information is collected, used, and shared, as well as the right to be free from surveillance and unreasonable searches and seizures. In the digital era, the right to privacy is particularly important because of the sheer amount of personal information that is collected and stored by technology, companies and governments. This information can include everything from search histories and location data to emails and social media posts. To protect the right to privacy in the digital era, many countries have passed laws and regulations governing the collection and use of personal information. These laws often require companies to obtain consent from users before collecting their data and to provide them with tools to control how their data is used. They also require governments to obtain a warrant before conducting surveillance on individuals. However, there are still many challenges to protecting the right to privacy in the digital era.

Introduction

The right to privacy is a fundamental human right that refers to an individual's ability to keep their personal information and activities private and free from unwanted intrusion or surveillance by others, including the government, corporations, or other individuals. It is recognized by International Law[1] and protected in many national Constitutions and legal systems around the world[2]. The right to privacy can include a range

[1] The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights which specifically protected territorial and communication privacy. Article 12 states: 'No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks'. Numerous international rights covenants give specific reference to privacy as a right. The International Covenant on Civil and Political Rights (ICCPR), the UN Convention on Migrant Workers and the UN Convention on Protection of the Child adopt the same language. Article 12 of the Universal Declaration of Human Rights states: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.* Article 17 of the International Covenant on Civil and Political Rights states: No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[2] In the United States, the concept of the right to privacy was first articulated by Samuel Warren and Louis Brandeis in their seminal 1890 article "The Right to Privacy," published in the Harvard Law Review. Warren and Brandeis argued that privacy should be recognized as a legal right, and that the law should protect individuals from unwanted intrusions into their private lives by others. Later on, the idea of privacy as a legal right gained further momentum in the mid-twentieth century, particularly in the wake of World War II and the rise of electronic surveillance technologies. In 1965, the US Supreme Court in Griswold v. Connecticut recognized a constitutional right to privacy, which protected a married couple's right to use contraceptives. In subsequent cases, the Supreme Court has expanded the scope of the right to privacy to include a woman's right to have an abortion (Roe v. Wade, 1973), the right to engage in consensual homosexual activity (Lawrence v. Texas, 2003), and the right to refuse medical treatment (Cruzan v. Director, Missouri Department of Health, 1990). Various countries developed specific protection for privacy in the centuries that followed. In 1776, the Swedish Parliament enacted the 'Access to Public Records Act" which required that all government –held information be used for legitimate purposes. In 1792, the Declaration of the Rights of Man and the Citizen declared that private property is inviolable and scared. France prohibited the publication of private facts and set stiff fines in 1858.

of aspects, such as the privacy of personal communications, the right to control one's personal data and information, the right to bodily autonomy and medical privacy, and the right to be free from unreasonable searches and seizures. This right is essential for maintaining individual freedom and autonomy, as well as promoting human dignity and respect for personal choices and beliefs. However, the right to privacy is not an absolute right and may be subject to limitations in certain circumstances, such as national security concerns or criminal investigations. The scope and extent of privacy rights may also vary depending on cultural and societal norms, as well as technological advancements and the changing landscape of information and communication. It is a crucial aspect of individual freedom and autonomy, and is essential for the protection of human dignity, personal autonomy, and personal security.

Over a period of time due to advancement in technology we see that there is new form of committing crime. With the advent of Internet the world has truly became a global village. Apart from several attributes that Internet has viz. easy to use, fastest and cheapest mode of communication, it also offers its dark side. Internet have given rise to new form of crimes which are specific to internet and computer viz hacking, launching virus, child porn, credit card frauds etc. In this era of Internet, privacy has also became a new issue. The explosive growth of hi-tech Computer Science technology and its capacity to gather, store and process copious amounts of personal information has posed grave security threats to vital national infrastructure. This sensitive and seemingly intractable problem of virtually unrestricted internet freedom has compelled to rethink the privacy parameters in the cyberworld. As more and more internet users surf the internet and post their personal information; in the form of educational qualification, marital status, private selfies, videos, family photos, hobbies and interests, online on social media networking websites are easily accessible to the general public. Thus virtual world has left almost no information private. [3]

Historical over view of Right to Privacy

According to ancient Hindu texts, the concept of privacy can be traced back to the Dharmashastras and ancient texts like the “Hitopadesha”, where it is specifically mentioned that certain matters in relation to worship, family, and sex should be protected from disclosure. There is a famous saying articulated by lawmakers at that point in time: “sarvas swe swe grihe raja” (every man is a king in his own house). Thus, essentially inculcating the difference between public and private. It laid emphasis on the personal autonomy of a person (more specifically, a men) within his household and that of being left alone.[4]

During the colonial period the concept of privacy was refurbished from ancient times through the Constitution of India Bill (1895), in one of the first attempts at Constitution-making by Indians. It mentions that every citizen has in his house inviolable asylum. Then came the Commonwealth of India Bill (1925) which advocated for no interference in an individual’s dwelling, without the due process of law being adhered to.[5]

In 1890, American Lawyers Samuel Warren and Louis Brandeis wrote a seminal piece on the right to privacy as a tort action describing privacy as ‘the right to be left alone’.

[3] Dr. Gagandeep Kaur, Privacy Issues in Cyberspace: An Indian Perspective, available at, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3673665, last visited on 14/4/23

[4] Gurpreet Singh, Deep Dive Into The History Of The Right To Privacy In India, available at, https://www.youthkiawaaz.com/2021/10/save-yourself-from-intrusion-know-your-right-to-privacy/, last visited on 12/4/23

[5] Kushi Gupta, Legal protection of right to privacy in Cyberspace, available at, https://thelawcommunicants.com/right-to-privacy-in-cyberspace/, last visited on 12/4/23

Right to Privacy under Indian Constitution

The right to privacy is recognized as a fundamental right under Indian laws. The Indian Constitution does not explicitly mention the right to privacy, but it has been interpreted by the Indian Supreme Court as being inherent in the fundamental right to life and personal liberty guaranteed by Article 21 of the Constitution. In case of P Sharma v. Satish Chandra[6], the court upheld the right of search and seizure; and held that invocation of privacy against search and seizure is not available.[7] In case of Kharaksingh v State of UP[8], the 6-judge bench held that a domiciliary visit at night was unconstitutional. More importantly, the bench held that the right of privacy is not a guaranteed right under the Constitution.[9] In Govind v State of Madhya Pradesh[10], the court in this particular case ruled privacy to be associated with personal liberty and freedom of movement emanating from Article 19 and 21 of the Constitution but also observed that it would be against judicial discipline to declare the right in broad terms that is explicitly not mentioned in the Constitution.[11] In case of R Rajgopala v State of Tamil Nadu[12], the court opined that it would be an infringement of privacy if something is published in relation to an individual's private affairs without their consent.[13] In a landmark case of Justice KS Puttaswamy (retd.) v Union of India[14] the Supreme Court cleared the confusion regarding the status of the right to privacy by ruling that it is a fundamental right emanating from Article 21 of the Constitution. The court expanded the meaning of privacy to include privacy of body, mind, decisions, and information. However, the court laid down that the right is not absolute and it can be intruded upon by the state by passing the test of legality.[15] In case of Jorawer Singh Mundy v Union of India[16] the court invoked the right to be forgotten emanating from the privacy and ordered Google and Indian Kanoon to take down the judgments, as they were causing great harm and prejudice to the petitioner.[17]

There are several laws in India that recognize and protect the right to privacy, including the Information Technology Act, 2000, the Aadhaar Act, 2016, and the Right to Information Act, 2005. The Personal Data Protection Bill, 2019 also seeks to provide comprehensive protection to individuals' personal data, including their right to privacy. In the light of the above discussion, the right to privacy in India has progressed from the ancient period to be elevated as a fundamental right in modern times. With the data protection around the corridors, it has open up avenues for privacy in the information age.

Digital era and Right to Privacy-A changing paradigm

The right to privacy in the digital age is an important and complex issue. With the increasing use of digital technologies such as the internet, social media, and mobile devices,

[6] 1954 AIR 300, 1954 SCR 1077
[7] Privacy Law Library, available at, https://privacylibrary.ccgnlud.org/case/saroj-rani-vs-sudarshan-kumar-chadha, last visited on 10/4/23
[8] 1963 AIR 1295, 1964 SCR (1) 332
[9] Supreme Court Observer, available at, https://www.scobserver.in/journal/right-to-privacy-court-in-review/#:~:text=Kharak%20Singh%20v%20State%20of%20Uttar%20Pradesh&text=Kharak%20Singh%20then%20challenged%20the,of%20life%20and%20personal%20liberty)., last visited on 12/4/23
[10] 1975 AIR 1378, 1975 SCR (3) 946
[11] Chinmoy Patra, A study on Indian Law on Protection of right to privacy, available at, https://www.legalserviceindia.com/legal/article-3763-a-study-of-indian-law-on-protection-of-right-to-privacy-in-the-cyber-world.html, last visited on 12/4/23
[12] 1995 AIR 264, 1994 SCC (6) 632
[13] Deepthi Arivunithi, Cyberspace v Right to Privacy, available at, https://www.tnsja.tn.gov.in/article/Cyber%20space%20vis%20-%20corrected%20new%2012082018.pdf, last visited on 15/4/23
[14] (2017) 10 SCC 1
[15] Ibid 2
[16] W.P. (C) 3918/ 2020
[17] Anujay Shrivastave, Delhi high court order on right to be forgotten: analysis and critique, available at, https://thedailyguardian.com/delhi-high-court-order-on-right-to-be-forgotten-analysis-and-critique/, last visited on, 16/4/23

people are sharing more personal information online than ever before. This has led to concerns about how this information is being collected, stored, and used by governments, corporations, and other entities.

In the digital age, the right to privacy is particularly challenging to protect because of the ease with which personal information can be collected and shared. Social media platforms, for example, routinely collect data on their users' activities, including their location, browsing history, and personal preferences.

In the digital era, privacy has become an increasingly complex issue. Here are some of the main issues pertaining to privacy rights in digital era:

Data collection

Companies and governments collect vast amounts of personal data on individuals, often without their knowledge or consent. This data can include everything from search histories to social media posts to location data, and it can be used to create detailed profiles of individuals.

Data breaches

Cyber attacks and data breaches are becoming increasingly common[18], and they can result in the theft of personal information such as credit card numbers, social security numbers, and other sensitive data. This can lead to identity theft, financial loss, and other forms of harm.

Tracking

Companies often track your online activities[19], such as your browsing history and search queries, in order to target you with personalized advertisements. This is done without your explicit consent, and it can feel invasive.

Surveillance

Governments and companies are increasingly using surveillance technologies[20] such as facial recognition and location tracking to monitor individuals. This can be used for law enforcement purposes, but it can also be used to track people's movements and activities without their knowledge or consent.

[18] There have been several high-profile cyber-attacks in India in recent years that have led to the theft of personal information. Here are some examples: Pegasus Spyware, Aadhaar data breach, Axis Bank data breach, Equifax data breach, and Domino's data breach. These are just a few examples of cyber-attacks in India that have led to the theft of personal information. Cyber security remains a major concern in the country, and individuals and organizations need to take steps to protect their data from such attacks.

[19] Many Indian companies have policies in place that allow them to monitor the online activities of their employees. This is often done to ensure that employees are using company resources appropriately, and to prevent the sharing of sensitive information.

The types of online activities that companies may monitor can include email and chat communications, web browsing, and social media usage. Some companies may also use software to monitor keystrokes or take screenshots of employees' computer screens. However, it's important to note that the legality of monitoring employee online activities can be a contentious issue, and companies must comply with applicable laws and regulations. In India, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 outline guidelines for data protection and security, and companies must adhere to these regulations when monitoring employee activities. Additionally, companies should ensure that their employees are aware of the monitoring policies and have given their consent to be monitored. This can help maintain transparency and trust between the company and its employees.

[20] There have been reports and allegations of the Indian government using surveillance technologies to track individuals. In particular, there have been concerns raised about the use of the Aadhaar system, a national biometric identification program, and the Central Monitoring System (CMS), a government surveillance system. The Aadhaar system was introduced in 2009 and has since been linked to various government services, such as subsidies, pensions, and bank accounts. The system collects biometric data, such as fingerprints and iris scans, and assigns a unique 12-digit identification number to each individual. While the government claims that the Aadhaar system is necessary to improve service delivery and prevent fraud, there have been concerns raised about privacy and security. The CMS is a centralized monitoring system that allows government agencies to intercept and monitor all telecommunications, including phone calls, emails, and internet traffic. The system was introduced in 2013, and its use has been criticized for violating citizens' privacy and freedom of speech. There have also been reports of other surveillance technologies being used by the government, such as facial recognition and social media monitoring. Critics argue that these surveillance technologies give the government too much power and can be abused. They have raised concerns about the potential for misuse, including tracking political opponents and suppressing dissent. The Indian government has defended the use of these technologies, stating that they are necessary for national security and preventing terrorism. However, there have been calls for greater transparency and oversight to ensure that these technologies are not being misused.

Social media monitoring

Social media platforms can collect a wealth of information about their users, including their interests, hobbies, and location. This information can be used to target users with ads and other content.

Lack of transparency

Many companies and governments are not transparent about their data collection and surveillance practices[21]. This makes it difficult for individuals to understand what information is being collected about them and how it is being used.

Third-party data sharing

Many companies share their users' data with third-party partners, such as advertisers or data brokers. This can lead to the creation of even more detailed profiles of individuals, and it can be difficult for individuals to know who has access to their data.

Cyber stalking and online harassment

The internet can be a breeding ground for cyber stalking and online harassment[22], which can have serious consequences for individuals' privacy and mental health. Cyber bullying and online harassment can also violate a person's right to privacy. This can take many forms, including sharing private photos or videos without permission, making threats or sending abusive messages, and spreading rumours or false information.

Revenge porn

Revenge porn refers to the sharing of sexually explicit images or videos without the subject's consent. This can lead to embarrassment, harassment, and even job loss.

Phishing

Phishing refers to the use of fraudulent emails, websites, or other communication to trick people into giving away their personal information. This can include passwords, credit card numbers, and other sensitive data.

These are just a few examples of how the right to privacy can be violated in the cyber world. It's important to be aware of these risks and take steps to protect your personal information online.

[21] In recent years, there have been concerns about the Indian government's data collection and surveillance practices, particularly with regards to the implementation of the Aadhaar biometric identification system and the proposed National Social Registry. Some critics have argued that these initiatives could lead to mass surveillance and privacy violations. There have also been reports of government agencies requesting user data from social media platforms and messaging apps, and of the government using surveillance technologies such as facial recognition and phone tapping without proper oversight. However, it is worth noting that India does have laws in place to regulate surveillance and data collection by the government. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, require government agencies to obtain the consent of individuals before collecting their personal data and to adhere to strict data security standards.

[22] Cyberbullying and online harassment can be a violation of an individual's right to privacy, as they often involve the unauthorized use or dissemination of personal information or private communications. However, despite legal protections, cyberbullying and online harassment remain a significant problem in India. Social media platforms and messaging apps have made it easier for individuals to bully and harass others anonymously or under false identities. This has led to many instances of cyberbullying, particularly against women and members of marginalized communities. Some examples on these lines are: 1). The 2018 Delhi stalking case: In this case, a 29-year-old woman was followed and harassed by two men in their car while she was driving home late at night. The men also posted lewd comments and videos of her on social media. The incident sparked nationwide outrage and led to the arrest of the two men. 2). The 2017 Kerala cyber stalking case: A young actress in Kerala was stalked and harassed by a man who sent her obscene messages and pictures on social media. The man was arrested and charged with several offenses, including cyber stalking and harassment. 3). The 2020 Hyderabad harassment case: A woman in Hyderabad was stalked and harassed by a man who created fake social media profiles in her name and posted derogatory comments and pictures. The man was arrested and charged with several offenses, including cyber stalking and defamation. 4). The 2018 Chennai harassment case: A woman in Chennai was harassed and threatened by a man who created fake social media profiles in her name and posted derogatory comments and pictures. The man was arrested and charged with several offenses, including cyber stalking and defamation. 5). The 2021 Mumbai cyber harassment case: A well-known actress in Mumbai was targeted by a man who sent her threatening messages and videos on social media. The man was arrested and charged with several offenses, including cyber stalking and harassment.

Recent incidences of violation of right to privacy

There have been several incidents of violation of the right to privacy in the digital world in India. Some of the notable incidents include:

*Pegasus spyware controversy*23

In July 2021, it was revealed that the Indian government had allegedly used Pegasus spyware[24] to target over 300 individuals, including journalists, activists, and politicians, for surveillance. The use of spyware like Pegasus is a violation of the right to privacy as it allows unauthorized access to a person's digital communications and activities.

*Aadhaar data leak*25*:*

In 2017, it was discovered that the personal data of over 1 billion Indians, including their Aadhaar[26] numbers (a unique identification number), had been leaked and were freely available online. This data breach raised concerns about the safety and security of personal information in India.

*Cambridge Analytica scandal*27

In 2018, it was revealed that the data of millions of Facebook users had been harvested without their consent by Cambridge Analytica, a political consulting firm. This incident highlighted the need for stronger data protection laws in India.

[23] The Pegasus spyware controversy is a scandal that emerged in July 2021 when a list of 50,000 phone numbers was leaked to the media. The list allegedly contained the phone numbers of potential targets of the Pegasus spyware, a sophisticated surveillance tool developed by the Israeli cyber intelligence firm, NSO Group. Pegasus spyware is designed to infect mobile devices and allow the operator to remotely access and monitor the device's activity, including calls, messages, and emails. It can also turn on the device's camera and microphone, effectively turning the device into a powerful surveillance tool. The leaked list of phone numbers included those of journalists, politicians, human rights activists, and other high-profile individuals from around the world. The controversy sparked widespread concern about the use of spyware by governments and the potential violation of privacy and human rights. NSO Group has denied any wrongdoing and has stated that its software is only sold to governments and law enforcement agencies for the purpose of preventing and investigating crime and terrorism. However, critics argue that the use of Pegasus spyware has gone beyond its intended use and has been used to target innocent individuals for political purposes.

[24] Pegasus spyware is zero-click mobile surveillance software designed to infiltrate iOS and Android devices to secretly collect information. Pegasus has extensive data-collection capabilities — it can read texts and emails, monitor app usage, track location data, and access a device's microphone and camera. Initially, Pegasus spyware spread through phishing attacks, where victims are sent text messages that include links infected with malware. If the target clicked on the link, their phone was infected with Pegasus. Now, Pegasus spyware has zero-click surveillance capabilities, meaning it can spread and infect phones without a victim having to do anything at all.

[25] There have been several instances of Aadhaar data leaks in India. Aadhaar is a unique identification number issued by the Indian government to its citizens, and it contains sensitive personal information such as biometric data, demographic data, and more. The leaks have raised concerns about the security and privacy of Aadhaar holders. In 2018, a report by The Tribune claimed that an anonymous seller on WhatsApp was offering access to the Aadhaar database for just Rs 500 ($6.75). The report alleged that the seller was able to provide access to the Aadhaar database, which included the personal details of over 1 billion Indians, including their names, addresses, phone numbers, and biometric information. The Unique Identification Authority of India (UIDAI), which manages the Aadhaar database, denied the claims, stating that there was no breach of its biometric database. However, it did acknowledge that some unauthorized people may have gained access to demographic information. In another instance, in 2019, it was reported that a government website was displaying the personal information of millions of Aadhaar cardholders. The website, run by the National Social Assistance Programme (NSAP), reportedly exposed the details of over 6.7 million Aadhaar holders, including their names, addresses, bank account numbers, and more. These incidents have sparked concerns about the security and privacy of Aadhaar holders. While the government has taken steps to address the issue, such as imposing fines on those who disclose Aadhaar information and establishing a centralized grievance redressal system, the leaks have highlighted the need for stronger data protection laws and stricter enforcement mechanisms in India.

[26] Zee Media Bureau, New Adhaar date leak exposes 11 crore Indian farmers sensitive information, available at, https://zeenews.india.com/personal-finance/aadhaar-data-breach-over-110-crore-indian-farmers-aadhaar-card-data-compromised-2473666.html, last visited on 14/4/23

[27] The Cambridge Analytica scandal was a major data privacy scandal that erupted in 2018. It involved the unauthorized collection of personal data from millions of Facebook users and its use for political purposes, particularly during the 2016 US presidential election. Cambridge Analytica was a political consulting firm that worked on political campaigns around the world. It was hired by the 2016 Donald Trump campaign, as well as the Brexit campaign in the UK, among others. The scandal began when it was revealed that Cambridge Analytica had obtained the personal data of millions of Facebook users without their consent. This was done through a personality quiz app that was developed by an academic researcher, Aleksandr Kogan, who collected data not only from those who took the quiz but also their Facebook friends. Cambridge Analytica then used this data to create psychological profiles of individuals and target them with political ads and messages. The scandal led to public outrage, calls for greater data privacy regulation, and investigations by governments around the world. Facebook was heavily criticized for its role in the scandal, and CEO Mark Zuckerberg was called to testify before the US Congress. Cambridge Analytica eventually shut down in 2018, and its parent company, SCL Group, filed for bankruptcy. The Cambridge Analytica scandal highlighted the need for better data privacy protections and greater transparency around the collection and use of personal data by companies and political campaigns.

WhatsApp privacy policy update[28]*:*

In 2021, WhatsApp updated its privacy policy, which led to concerns about the privacy of user data. The updated policy allowed WhatsApp to share user data with Facebook, its parent company. However, the policy was challenged in court, and WhatsApp was ordered to put the policy on hold.

Conclusion

These incidents demonstrate the need for stronger data protection laws and greater transparency in the use of digital technologies in India. Protecting the right to privacy in the digital era is becoming increasingly important as more and more personal information is being collected and stored online. Here are some steps that individuals and organizations can take to protect their right to privacy:

Use strong passwords

Passwords are the first line of defense in protecting your personal information online. Use long and complex passwords that include a mix of letters, numbers, and special characters, and avoid using the same password for multiple accounts.

Use two-factor authentication:

Two-factor authentication[29] adds an extra layer of security by requiring a second form of authentication in addition to a password. This could be a fingerprint, a code sent to your phone, or a security key.

Be mindful of what you share online

Be careful about what personal information you share online, especially on social media. Avoid sharing your full name, address, phone number, or other sensitive information.

Use a VPN:

A Virtual Private Network (VPN)[30] encrypts your internet traffic and hides your IP address, making it more difficult for others to track your online activities.

[28] In January 2021, WhatsApp announced an update to its privacy policy that caused widespread concern and confusion among users. The update included changes to how WhatsApp would share user data with Facebook, which had acquired the messaging app in 2014. The new privacy policy stated that WhatsApp would share certain user data with Facebook, including phone numbers, transaction data, and information about how users interact with businesses on the platform. WhatsApp said that the data would be used to improve Facebook's ad targeting and other services. The update also said that users would have to agree to the new terms in order to continue using WhatsApp, and that those who didn't accept the new policy by the deadline of May 15, 2021, would lose access to the app. The announcement led to a backlash from users who were concerned about their privacy and the implications of sharing their data with Facebook. Some users began migrating to alternative messaging apps, such as Signal and Telegram, which have a stronger focus on privacy. In response to the backlash, WhatsApp delayed the implementation of the new privacy policy and clarified that the update would not affect the privacy of personal messages sent between friends and family. However, the company said that the data sharing with Facebook would still apply to business chats and other interactions with business accounts on the platform.

[29] Two-factor authentication (2FA) is a security process that requires two different forms of identification from a user in order to grant access to a secure system, account, or service. It adds an extra layer of security to the traditional username and password login process. The two factors are typically categorized into three types: 1) Something you know, such as a password or PIN code. 2). Something you have, such as a security token, smartphone, or smart card. 3). Something you are, such as biometric data, such as a fingerprint or face recognition. Thus, by requiring users to provide two different types of authentication, 2FA makes it more difficult for unauthorized users to access accounts or systems, even if they have somehow obtained a user's password or login credentials. This type of authentication is widely used in online banking, email services, social media, and other online services that handle sensitive data.

[30] VPN stands for Virtual Private Network, which is a secure and encrypted connection that allows users to access the internet or a private network remotely. It creates a private network over the internet by encrypting all data transmitted between the user's device and the VPN server. This makes it difficult for others to intercept and read the user's data, ensuring their online privacy and security. A VPN can be used for many purposes, such as: 1). Protecting your online privacy: A VPN can help keep your online activities private and anonymous by hiding your IP address and encrypting your internet traffic. 2). Bypassing internet censorship: A VPN can help you bypass internet censorship and access content that may be restricted in your country or region. 3). Accessing geo-restricted content: A VPN can help you access content that may be restricted to certain geographic regions, such as streaming services. 4). Secure remote access: A VPN can allow you to securely access

Use encryption

Use encrypted messaging apps and email services that offer end-to-end encryption to protect your communications from prying eyes.

Keep your software up to date

Software updates often include security patches that fix vulnerabilities that could be exploited by hackers.

Read privacy policies

When signing up for a new service, make sure to read the privacy policy to understand how your data will be used and protected.

Use privacy-focused search engines

There are several privacy-focused search engines available that prioritize user privacy and security. Here are some of the most popular types:

DuckDuckGo: DuckDuckGo is a search engine that does not track user activities, nor does it store user data. It utilizes encryption protocols to ensure that searches and activities are not monitored.

- StartPage: StartPage is a privacy-focused search engine that does not track user activities and offers anonymous searches with Google's search results. It uses proxy servers to ensure that users' searches are kept private.
- Qwant: Qwant is a search engine that prioritizes user privacy and does not collect personal data. It offers encrypted search results, and users have the option to search the web, images, videos, or news.
- Swisscows: Swisscows is a privacy-focused search engine that prioritizes user privacy and does not store user data. It uses semantic data recognition to improve search results while ensuring user privacy.
- Searx: Searx is an open-source, privacy-focused search engine that offers users the ability to customize their search experience. It does not track user activities and offers users the ability to search multiple sources at once.
- Peekier: Peekier is a privacy-focused search engine that offers users a visual search experience. It does not track user activities and encrypts all searches to ensure user privacy.

Overall, these search engines prioritize user privacy and provide a more secure and private search experience compared to traditional search engines.

Use ad-blockers

Ad-blockers can help reduce the amount of tracking that occurs when you browse the web.

Support privacy legislation:

Encourage lawmakers to pass strong privacy legislation that protects individuals' right to privacy in the digital era.

your company's network or remote servers from anywhere in the world. 5). Overall, a VPN is a powerful tool that can help protect your online privacy and security, as well as provide access to content that may be restricted or blocked in your location.

The Indian government has taken some steps towards strengthening data protection laws, including the introduction of the Personal Data Protection Bill, but there is still much work to be done to ensure the right to privacy is protected in the digital world. Overall, protecting the right to privacy in the digital era requires a combination of legal, technical, and social solutions. It is important for all stakeholders to work together to ensure that individuals' privacy rights are respected and protected.