ILE MONTHLY REVIEW

Volume I and Issue III of 2023

ISBN - 978-81-961828-8-5

Published by

Institute of Legal Education

https://iledu.in

PRIVACY OF PERSONAL DATA

Author - ADITYA PARASHAR, STUDENT AT ARMY INSTITUTE OF LAW

Best Citation - ADITYA PARASHAR, PRIVACY OF PERSONAL DATA, ILE Monthly Review, 1 (3) of 2023, Pg. 16-20, ISBN - 978-81-961828-8-5

ABSTRACT

With the continuous advancement in the usage of internet and technology, the concept of data privacy has become a debated topic. The internet service providers, various websites that we visits and the applications that we installs in our devices, they all collects user's personal data in order to better provide their services. However there are instances in which the privacy of the user's data is breached and it gets into the hands of unauthorized third parties and hackers due to which, the user's personal data remains no more safe. The main reason for which the user's personal data is stolen is mainly for the fraud and identity theft to steal the information such as date of birth, name, and address and to use it in a fraudulent manner. Nowadays, data theft and privacy has become a major concern of the modern world and all the nations and various international organizations are doing their best to ensure that the personal data of peoples does not goes into the wrong hands.

INTRODUCTION

Today's society, at some extent, is dependent on the internet and technologies for day to day work as in today's world, a life without internet cannot be think of. When we visits any websites or app, then our personal data is collected in order to improve the user interface. . However, there are instances in which the privacy of the user's personal data is breached and it gets into the hands of unauthorized third parties and hackers. Hence, there is a lot of requirement of data privacy of individuals.

Data privacy is an aspect of data protection that addresses the storage, access, retention, protection and security of sensitive data. It is a sub-part of the broader data protection concept. The goal of data protection is to protect the sensitive business and personal data, while maintaining the availability, consistency and immutability of that data.

Government and Various national and international organizations are constantly working for protecting the personal data of its citizen and controlling the cybercrimes in their nation, for example, in India, The Information Technology Act, 2000 is the main act for data protection, as there is not any specific legislation in this matter.

DATA THEFT- WHY, HOW, AND CONSEQUENCES

Data theft is an act of stealing digital information of individuals stored on computers, online servers or in any electronic devices in order to obtain confidential. It is a form of cybercrime that takes place when the hackers and fraudsters gain illegal access to the sensitive and private information of individuals that is not meant to be shared publicly. The data stolen can be anything such as bank account details, online passwords, license numbers, social security numbers, medical records, online subscriptions, and so on. The hackers use these things for the identity theft. Once an unauthorized person has accessed your personal data your financial information, then he can delete, alter, or prevent access to it without the owner's permission, which would automatically results in harm to the person whose privacy has been compromised.

ILE MONTHLY REVIEW

Volume I and Issue III of 2023

ISBN - 978-81-961828-8-5

Published by

Institute of Legal Education

https://iledu.in

The legal definition of data theft is given under section 43(b) of Information Technology Act 2000 as:- If any person without permission of the owner or any other person who is in charge of a computer, computer system of computer network, downloads, copies or extracts any data, or information from computer, computer system or computer network. It is the term used when any information in the form of data is illegally copied or taken from a business or other individual without his knowledge or consent. Data theft is a punishable offence as per Indian laws, according to section 65 of IT Act 2000, if a person conceals, destroy or alters a user's data, then he shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Data theft was once primarily a problem for businesses and organizations but, unfortunately, is now a growing problem for individuals. The reason that why this crime has grown so much over some past years is because of the rapid advancement of technology and availability of internet among the masses. Nowadays, every person has access to internet and people are not much aware of the cybercrimes, due to which it is easy for the hackers to find their prey.

The reasons that how our data is stolen is because of:

- **Weak passwords:** Using a password that is easy to guess, or using the same password for different accounts, can allow attackers to gain access to sensitive data. Hence it is always advised not to repeat the same password for multiple accounts, and to always keep a strong password i.e., using a password which contains abbreviations, numbers, capital words and a long password such as Adjh25@_8*
- **Permissions that we grant**: The websites and the apps that we use asks for various permission in order to better their functioning and to improve user's experience, but in this pretext, these websites and apps collects users sensitive data and use that for their own benefit.
- **Download from unknown sources:** Data theft may also occur due to downloading programs from unknown sources, as these sources may also be malicious and the websites may also be the corrupted websites which can contain malware and viruses and these viruses may access the command of your computer and other devices and can steal some sensitive information and personal data.
- **Human mistakes:** Data breach is not always the result of malicious activities of hackers and fraudsters, sometimes it is by our own mistake. Some of the mistakes that we made are like sharing our password to a wrong person or mistakenly sending some personal information to a wrong mail address or not hiding our atm card details while cash withdrawal, etc.

Consequences of Data Theft

- Ransomware demand by the hackers.
- Potential lawsuits from customers whose data has been exposed.
- Identity theft, like stealing of date of birth, name and address, contact info and other personal data.
- Stealing of financial information, such as card numbers and expiry dates, bank account details, investment details and similar data.
- IT Security Data. This includes lists of user names and passwords, encryption keys, security strategies and network structure.
- Data breach seriously affects the reputation of the person or the organization whose data has been leaked.

ILE MONTHLY REVIEW
Volume I and Issue III of 2023
ISBN - 978-81-961828-8-5
Published by
Institute of Legal Education
https://iledu.in

DATA PRIVACY

As Internet usage has increased day by day, so the importance of data privacy has also increased. Websites, applications, and social media platforms needs to collect and store data of the users in order to provide services, and in this process, the privacy of user's data may be compromised. Hence data privacy is very important in today's world.

Data privacy is an act of protection of personal data, such as one's name, location, contact information card details, intellectual data etc. from the potential threats present on internet, such as fraudsters, malware, viruses, hackers etc.

WHY IS DATA PRIVACY IMPORTANT?

As per Indian law, privacy is considered as a fundamental right of an individual. Data privacy is also important as if a lot of people are engaged online, then there should be a surety that their data would not be manhandled. Organizations also use data protection practices in order to make their customers and users believe that their personal data is not been compromised.

Personal data of the individuals can be misused in a number of ways if it is not handled properly, such as:-

- Fraudster and hackers may use it for money gain.
- Criminals may use our data to fraud or harass.
- The organizations may sell the data of their customers to a third party for their personal benefit.
- It may be used for identity theft.

For individuals, any of these outcomes can be harmful as it could lead to financial loss, reputational lost or identity theft. But for businesses, it could lead to legal sanctions, fines, reputational loss and other legal consequences.

HOW TO KEEP YOUR DATA SAFE

- **Using strong password**
  One of the best way to protect your data is by keeping a strong password. A weal Passwords can be easily cracked by hackers, therefore it is advised to always use a strong password. A strong password should be of at least 12 characters comprising of abbreviations, symbols, capital and small letters and numbers as it would be quite difficult for a hacker to hack these passwords.
- **Two factor Authentication**
  Two factor Authentication is another method of protecting your account and data from hackers, in this method, if someone tries to access your account, then an otp or a code will be send to the number of the person whose account is linked with that account. Two-factor authentication requires two separate, distinct forms of identification to access an account.
- **Anti-virus software**
  Protecting your desktop and laptop with proper antivirus systems is very important when it comes to preventing employee data theft. A good antivirus software would protect your PC whenever a malware or virus tries to attack your PC and in this way, the data would be protected, and hacking a system would not be easy.
- **Beware of free Wi-Fi**
  Nowadays, free Wi-Fi connections are available in various public places. But stealing someone's data from these connections is quite simple. Public Wi-Fi is an easy target for hackers and cybercriminals who can use it to find a new prey. Hence it is advised to only use secured networks in order to protect sensitive and confidential data.
- **Avoid using the same password for multiple accounts**
  Using same password for multiple accounts would be quite dangerous, as if a hacker could crack one of your accounts password, then it would be easy for him to access your other accounts. Hence it is always advised not

ILE MONTHLY REVIEW
Volume I and Issue III of 2023
ISBN - 978-81-961828-8-5
Published by
Institute of Legal Education
https://iledu.in

to use the same password for multiple accounts and to always keep a strong password.

- **Regularly update the systems and programs**
  Always keep your system software and programmes up to date as the older versions are not that much efficient in detecting the viruses and malwares. Hence it is always advised to keep your system up to date as the updated system would also be more compatible in catching the malware and viruses.

LAWS MADE FOR DATA PRIVACY

As the problem of data theft and the need for data privacy is increasing day by day, hence there was a need for some data protection laws in order to make the internet a safer place. For this reason, data protection laws are made both nationally and internationally of which some of them are discussed below:-

- **INFORMATION TECHNOLOGY ACT, 2000**

IT Act 2000 was passed on October 17, 2000. This is the main legislation governing e-commerce, data theft and other cybercrime. There are a total of 94 Sections under this act, which is divided into 13 Chapters and 4 Schedules. This legislation was passed to provide a safer internet surfing and protect individuals from various cybercrimes. This act is applicable all over India and also has extraterritorial jurisdiction, which make it applicable outside the India also.

This act was amended in 2008 by IT Amendment Act, 2008. As a result, all types of communication tools and networks are now included in the scope of the IT act 2000. Data theft is mentioned under section 43(b) of Information Technology Act 2000 as:- If any person without permission of the owner or any other person who is in charge of a computer, computer system of computer network, downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network.

Data theft is a punishable offence as per section 65 of IT Act 2000, this section says that "if a person conceals, destroy or alters a user's data, then he shall be punishable with imprisonment of a period which may extend to three years, or with fine of up to two lakh rupees, or with both."

According to section 66c of IT Act 2000, Whoever make use of the electronic signature, password or any other unique identification feature of any other person, without his or her consent, shall be punished with an imprisonment of either a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

- **PERSONAL DATA PROTECTION BILL, 2018**

A committee was formed by Ministry of Electronics and Information Technology (MeitY), which was headed by retired Supreme Court judge, Justice B. N. Srikrishna, the task of the committee was to draft a data protection legislation for India. Hence the committee drafted the Personal Data Protection Bill, 2018. The bill comes with a maximum fine amount of Rs 250 crore.
This bill was not passed by the parliament and was withdrawn from the Lok Sabha and the Parliament as reported in the Bulletin - Part 1 No. 189 dated August 3, 2022. But it is believed that a more comprehensive version of the Bill may be introduced in the parliament. Some sources believes that the government may introduce a Digital India Act, replacing the Information Technology Act, 2000.

CONCLUSION

Data theft does not seems to completely go away over a period of years as we are living in a society where everything has gone digital. So protecting your data from the hackers won't be an easy task. The only thing we can do is to remain more conscious while using applications and websites. The government is also making efforts in order to stop the cybercrime. Indian government has introduced

Information Technology Act, 2000 in order to stop data theft and to provide punishment to the violators.

References

1. 5 things you need to know about Data Privacy. (2023, 1 10). Retrieved from dataprivacymanager: https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/
2. Data Breaches: Threats and Consequences. (n.d.). Retrieved from cloudmask: https://www.cloudmask.com/blog/data-breaches-threats-and-consequences
3. Data privacy. (n.d.). Retrieved from SNIA: https://www.snia.org/education/what-is-data-privacy
4. data protection laws in india. (2023, february 3). Retrieved from ipleaders: https://blog.ipleaders.in/data-protection-laws-in-india-2/#Conclusion
5. Data protection laws in India. (2023, february 3). Retrieved from ipleaders: https://blog.ipleaders.in/data-protection-laws-in-india-2/#:~:text=The%20Information%20Technology%20Act%2C%202000,legislation%20for%20this%20matter%20yet.
6. Mali, P. (2017, september 21). Data Theft in Organisations and Legal Issues. Retrieved from Moneylife: https://www.moneylife.in/article/data-theft-in-organisations-and-legal-issues/51604.html
7. Personal Data Protection Bill, 2019. (n.d.). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Personal_Data_Protection_Bill,_2019
8. What is data privacy? (n.d.). Retrieved from cloudflare: https://www.cloudflare.com/learning/privacy/what-is-data-privacy/#:~:text=Data%20privacy%20generally%20means%20the,online%20or%20real%2Dworld%20behavior.
9. What is data theft and how to prevent it. (n.d.). Retrieved from Kaspersky: https://www.kaspersky.co.in/resource-center/threats/data-theft