IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Review of Data Privacy Laws and Case Study

Parisha Bhatia, Saloni Jaitly, Soham Sharangpani, Arth Akhouri, Ami Munshi,
SVKMs' NMIMS, Mumbai.

Abstract: Data consists of information ranging from text documents, images, voice memos, and videos that are considered the oil of the 21st century. With the exponential rise in the amount of data generated, analysed, stored, and transferred, the issues about data privacy and security issues are also increasing at an alarming rate which could be a precursor to cybercrimes. Data thefts pose a threat to the privacy rights of individuals as well as organizations. The organizations use different DLP techniques to avoid data breaches but since no system is invincible, data laws exist to regulate the handling of data in ethical ways. The laws need to evolve with the speed of technological advancements to reduce potential privacy threats and risks. Many countries have similar laws that are tailored to different industries like Finance, Health, IT, Commerce, etc. Laws framed by the Indian constitution attempt to protect the data of government organizations and other public bodies with the personal data protection bill of 2019. Information Technology Amendment Act 2008, different sections of the Indian Penal Code (Example: Section 403, Section 378), Securities and Exchange Board of India, and Credit Information Regulations Act 2005 form laws for various organizations. In this paper, we have comprehensively reviewed the topic of the data leak, its causes and consequences, prevention measures, and data privacy laws. This paper also looks at case studies of Target Incorporation and Unacademy relating to the data breach.

Index Terms **- Data privacy, Data Leak, Indian Data Loss Prevention.**

I. INTRODUCTION

Data Privacy is the dependency between the gathering and distribution of data, information, and technology with the public keeping in mind the general laws and rules and following standard ethics. It relates to how a piece of information should be handled based on its relative importance in a way that the data is used for its intended purpose only. The ways and process in which we protect data from corruption and unauthorized access through its lifecycle is called Data Security. It includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms.

Data leakage is the unauthorized movement of data from within an organization to an external destination or recipient. The advancements in technology have made the data more vulnerable to leaks, what was initially created to give a safe space for individuals and organizations to discuss revolutionary ideas has become an unethical source of income for others. The dark web is the go-to place for unethical hackers to sell the stolen data from big corporations to their competitors or the highest bidder. The laws to protect the privacy of individuals and organizations have not evolved as swiftly as technology. The lack of clear expression of the content of these laws has contributed to difficulties in its application and enforcement. This makes it difficult for the law protectors and law enforcement officers to implement and interpret the laws related to privacy protection. The right to privacy is qualified, its interpretation raises challenges concerning what organizes the private sphere and in establishing notions of what constitutes public interest.

Each country has a different law to protect the rights of its people. The review paper aims to discuss different laws that protect individuals and organizations from intentional or unintentional data privacy breaches. The review paper also discusses different case studies where the laws were unable to protect the privacy of individuals/organizations.

II. DATA PRIVACY AND LEAK

In today's dynamic world, the amount of data generated every second is huge, thus there is an increasing need to better protect this data and make sure that it is not misused in any manner. A lot of data is owned by huge corporations who use it to gain an edge on their competitors. Since these corporations are majorly interested in profits, there is always a big ethical question about other ways in which personal data of customers is being used by the organizations.

To monitor this, several organizations have privacy programs under the laws of their country. But because certain laws can be interpreted in an open-ended way, organizations exploit it and misuse the data. We believe that these existing privacy programs can be better protected against breaches if a certain level of ethical reasoning can be applied to them. They will also better help the organizations to overcome the sometimes-difficult challenges to comply with the legal requirements of the country.

We can divide data privacy into two wide categories: Data reuse and unauthorized access to data. If a company uses the client data in its custody for some other use under legal boundaries, it is referred to as data reuse. On the other hand, if a person or an organization accesses the data in violation of the ethical or corporate laws, we call that unauthorized access of the data. In unauthorized access, a person can either just browse through the data they are not supposed to see, or they can download the data illegally, actions we call as data breaches [1].

The unauthorized distribution of data from an organization to an external entity carried out by internal or external personnel is called a data leak. It occurs mostly via web and email services or offline data storage devices like USBs, hard drives, and laptops. The advancements in technology have made the data more vulnerable to leaks, what was initially created to give a safe space for individuals and organizations to discuss revolutionary ideas has become an unethical source of income for others. A lot of times what happens is that the intentionally leaked data is sold on the Dark Web which can have dangerous implications.

Data can be accidentally breached, distributed, or shared by an ill-intentioned employee, can be a host to a malicious attack, etc. Here are some common causes of data loss [2].

1. Natural Causes: Your data stored in a hard drive can be damaged due to fire, floods, or any other natural disasters, or in case the hard drive is mishandled or accidentally dropped, this may result in data loss.
2. Accidental Deletion or Formatting of Data: Sometimes a user or employee can accidentally format an entire hard drive or delete the information stored in it. Administrative errors also fall here.
3. Intentional Deletion of data or Leaking of Data: An intentional attack from inside the organization can threaten the working of the whole organization, by corrupting the data, it may get deleted in the future or be redundant to work upon. Leaking sensitive information may hamper the reputation and can hamper the organization.
4. Virus and Malicious Attacks: External attacks by hackers, which invade through security programs and enter the system and steal valuable data.

III. DATA LEAK CONSEQUENCES AND PREVENTION

Data leak prevention is a set of tools and processes or software which ensures that sensitive data is not lost, misused, or accessed by unauthorized users while the data is stored or transmitted from owner to client. A DLP system detects potential data breaches/unknown data transmissions. Breaches are prevented by monitoring, detecting, and blocking sensitive data. A data leak prevention system analyses the content and the surrounding context of the data to detect any threats. A data leak prevention system that uses content analysis mostly depends on data fingerprinting, statistical analysis, and various algorithms.[2]

The immediate consequences of a data breach are unknown, but at the very least are damaging to the consumer and the user. Let us look at some consequences of data breach [3]:

1. Fines and Fees: Payment industries and security councils may impose heavy fines and fees over improper handling of data.
2. Further Investigations: Once a data breach occurs, an investigation is carried out to determine the cause of the data breach. It may help in getting significant information and preventing further breaches. But investigations often take a long time and are costly. It also hampers the working of employees in an organization.
3. Increasing Security: Once a data breach has occurred it should be the aim of businesses to check their security layers and make proper changes if required.
4. Loss of Reputation: The biggest consequence of a data breach is the loss of reputation and confidence between the company and the user. This results in the loss of trust which was built over years. It becomes difficult for the company to get on its feet at times.

Knowing the consequences of a data breach is the initial step in safeguarding the business. The next step is planning and taking an action and implementing better security methods.

IV. DATA PRIVACY LAWS

4.1 General Laws

All countries have various laws to be followed by organizations in each sector. The laws may vary from country to country on the extent of their implementations, but all of them have the same basic standards. Listed below are the overall requirements for data privacy in some certain sectors with regards to the Fair Information Practices guidelines followed worldwide [4][5][6] :-

1. Financial Institutions: - They have to ensure security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or the integrity of the records, and protect against unauthorized access to or use of such records or information which could result in inconvenience to any customer.
2. Health Organizations: - All the covered entities must implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements include implementing a comprehensive risk management program, workforce security, information access management, security awareness, and training.
3. Commercial Organizations: - There should be no unfair or deceptive acts or practices. Failure to implement reasonable security may constitute unfair trade practice if a breach results in harm to consumers that could not reasonably be avoided by the consumer and could have been avoided by the firm. Firms can also be prosecuted for making a false statement in their privacy policy.
4. Organizations Accepting Payment via Cards: - These organizations need to implement an information security policy, build, and maintain a secure network, maintain a vulnerability management program, implement strong access control measures, and regularly monitor and test networks.

4.2 Indian Laws

The right to privacy makes up an integral part of the right to liberty and the right to freedom of speech expression [7]. The right to privacy was introduced to provide a personal domain that is free from unjustified interference or surveillance by state or other actors. The issue arises when the laws cannot clearly define the line between the private sphere and public interest information. The increasing potential of computers to survey other systems has created a need for rules that govern the methods of collection and handling of personal information.

1. Data Protection and Right to Information Act 2005 (information held by public bodies) [8]
   - 1.1. Strict check on the limit of collection of personal data should be obtained by lawful and fair means with the consent of the individual.
   - 1.2. Information should be accurate and relevant and used for the stated purpose specified at the time of collection of data without any ambiguity
   - 1.3. Information should be secured and protected, and the collector must ensure the safety of the same
   - 1.4. In the case of abuse of data, the organization will be held liable.
   - 1.5. The individual has a right to access, edit, or ask info to be deleted.
   - 1.6. The Data Protection Bill states that there shall be no obligation to give out any citizen's personal information unless it has a relationship to any public activity or interest since the data could cause an unwarranted invasion of privacy. The State Public Information Officer or a higher authority should justify the disclosure of such information.
2. Data Protection and Information Technology Amendment Act 2008 [9]
   - 2.1. Prevention of unlawful use of computers, computer systems, and data stored
   - 2.2. Internet Service Providers face imprisonment for disclosure of personal information and may need to pay the damage.
3. Data Protection and Indian Penal Code [10]
   - 3.1. Under the Indian Penal Code, liability for breaches of data privacy must be inferred from related crimes. Example: Section 403 of the IPC imposes criminal penalties for dishonest misappropriation.
   - 3.2. In another Section 378, no one can dishonestly take any movable property out of the possession of any person without that person's consent, if he does so then he is said to commit theft and is punished but there is not any particular act regarding electronic data protection to till date.
4. Data Protection and National Security
   - 4.1. Data Collection and its use for national security and law enforcement – no standards set
   - 4.2. Location detection like GPS done by police, some extent this encroachment is genuine if for national security reasons or other valid reasons but the personal privacy issue.
5. Data Protection and Corporate Affairs [11]
   - 5.1. SEBI undertakes inspection of corporate organizations belonging to the securities market if they believe a company has been indulging in insider or fraudulent trading practices, transactions in securities are being dealt with in a manner detrimental to the investor, or any provisions in the act are being contravened by any intermediary or person belonging to the securities market.
   - 5.2. The Credit Information Companies (Regulation) Act, 2005 specifies the privacy principles that every credit institution needs to adopt. The principles ensure that the data relating to the credit information maintained by them is accurate, complete, duly protected against any loss or unauthorized access or use or unauthorized disclosure thereof.

V. CHALLENGES OF IMPLEMENTING LAWS

The courts only in recent times have been realizing that the protection of personal information of clients is the company's responsibility and has been enforcing basic data ethic laws on companies in compliance with the government. This is generally a difficult task because the data privacy systems are judged on "basic requirements" but there is no proper definition of what these basic requirements should include. This will vary from organization to organization depending on their size and the scale of the data they handle.

The status of data protection and privacy law remains unclear to this date in India. According to one commentator, "most of the rules and regulations of data security, as they exist in the American and European countries' Data Protection Acts (based on Fair Information Practices), have been incorporated in the revamped Information Technology Act of 2008." But Indian attorney Shojan Jacob, upon reviewing the new 2008 amendments, concludes that its provisions are still "not adequate to meet the needs of corporate in India."

VI. CASE STUDIES

6.1 Target Incorporation

The systems and networks of Target Corp. were breached in November and December 2013, which resulted in 40 million card numbers (i.e., credit, debit, and ATM cards) and 70 million personal records i.e., (PII) stolen. On November 12, 2013, the malware later found to be BlackPOS attacked Target's computer system and it was designed to steal information of every credit card used at the company's 1,797 US stores [12].

BlackPOS is a memory scraping malware that scrapes systems memory and adds filters to extract the target information. According to Krebson Security, an HVAC firm was attacked by a malware phishing virus, this firm did business with Target. Via the HVAC company's vendor portal, the criminals were able to access Target systems. Once they were able to do so, they installed malware on the point of sale (POS) systems to steal information from customers. The security division of Target attempted to protect their systems and networks against such cyber threats and Six months before the breach, they even deployed a well-known intrusion and malware detection service named FireEye. There were several malware alerts but were ignored and the prevention functionalities were turned off by the admins who were not well versed with the system. On 12 December DOJ informed Target about suspicious activities involving payment cards that had been used at the company's stores.

Target officially announced this breach on December 19. According to the Data Protection Report, the data breach resulted in over 100 lawsuits across the country, which were handled by the United States District Court for the District of Minnesota [13]. Target agreed to pay as much as $20.25 million to banks and credit unions, $19.11 million to reimburse MasterCard Inc card issuers and Visa Inc card issuers about $67 million over the breach and reached a $10 million settlement with customers, under which they will be paid up to $10,000 in damages by the company if they can provide documentary proof of loss [14].

6.2 Unacademy

Unacademy is one of India's biggest online EdTech providing preparation material for several professional and educational entrance exams. These lessons are in the form of Live lessons both free and via subscription. On 3 May 2020, US-based cybersecurity firm Cyble disclosed the data breach where the Unacademy database was available on the dark web for $2000 containing 20 million accounts [15].

The last user account created present in this database was from 26 January, which indicates that the hacker was able to breach into the systems, towards the end of January 2020. According to the reports, the hacker alleged to have access to the database of the whole company. They, however, decided only to leak users' accounts at that point in time. Usernames, SHA – 256 hashed passwords, last login date, date joined, names, email addresses, account activity status, and level of the user were among the information leaked. Cyble also informed that several accounts that were made using corporate emails exist in this database as well. Because of the scale of the breach, it is anticipated that if these account holders use the same passwords at their workplace then it poses a threat to the workplace as well. Accounts of domain names from Infosys, TCS, Cognizant, Reliance Industries, TCS, Accenture, ICICI, HDFC, SBI, several other large organizations were recorded [16].

Around 11 million was the official number of users affected as cited by the CTO of the company and he denied any knowledge of exposure of passwords of users. He also assured that no sensitive information such as financial data or location had been breached, stringent encryption methods were used, PBKDF2 algorithm with a SHA256 hash, making it highly implausible for anyone to access the learner passwords[17]. All the Unacademy learners were still suggested to change their passwords for Unacademy and other portals with similar password patterns and closely track their financial transactions by the cybersecurity firms.

VII. CONCLUSION

Whether a data leak occurs by an imposter among the system or by an external party, its effects can be seen over a wide variety of platforms. The horror of losing personal information and identity creates uncertainty while going online. If such attacks and data leaks are increasing in today's world, it reflects how society is growing to be unethical and immoral. It is an arguable topic if information should be stored in the first place and the virtues and vices of information stored. Data is growing daily and the debate over how much and what information should be made accessible is also increasing rapidly.

In today's world, the question is who should have the responsibility to prevent data leak: The Organization or the government. While organizations are implementing various data leak prevention techniques, hackers are becoming even more proficient than ever. A country's constitution can also implement strict laws and regulations to account for the data leaks that occur. Ultimately, it is important to educate and create awareness among people to keep their information safe and have a regular tab on the accounts they have.

REFERENCES

[1] Mary J. Culnan & Cynthia Clark Wilson 2009 - How Ethics Can Enhance Organizational Privacy: Lessons from the Checkpoint and TJX Data Breaches.
[2] Jadhav, P. and Chawan, P., 2020. Data Leak Prevention System: A Survey.
[3] Worldpay Editorial Team, 2019. How the Consequences of a Data Breach Threaten Small Businesses - Insights | Worldpay from FIS Global.
[4] Schwartz, P. M., and Solove, D. J. 2008. Information Privacy: Statutes and Regulations, Austin, TX: Wolters Kluwer.
[5] Semdinghoff, T. J., and Hamady, L. E. 2008. "New State Regulations Signal Significant Expansion of Corporate Data Security Obligations, "BNA Privacy and Security Law Report (7), October 20, p. 1518.
[6] Payment Card Industry Security Standards Council (2006)
[7] Ghosh, Dr. Jayanta & Shankar, Uday. (2016). 'Privacy and Data Protection Laws in India: A Right-Based Analysis.
[8] Shruti Verma B.B.A. LL. B (Hons.) AMITY LAW SCHOOL, NOIDA. (n.d.). Contemporary Relevance of RTI Act and Right to Privacy. Central Information Commission.
[9] Benjamin Wilson - Data privacy in India: The Information Technology Act by Benjamin Wilson: SSRN. (n.d.). Home: SSRN
[10] Jatin Verma - Data Protection in India
[11] Legislative Department, Government of India
[12] Xiaokui Shu, Ke Tian*, Andrew Ciambrone* and Danfeng (Daphne) Yao, Breaking the Target: An Analysis of Target Data Breach and Lessons Learned. https://arxiv.org/pdf/1701.04940.pdf
[13] Settlement of target data breach consumer class action is derailed on appeal. (2018, April 27). Data Protection Report.
[14] Stempel, J., & Bose, N. (2015, December 3). Target in $39.4 million settlement with banks over data breach. U.S.
[15] Cyble Inc. (2020, May 5). Unacademy, India's largest learning platform has been breached by professional hackers. Cyble, Inc.
[16] Lawrence Abrahams. (2020, May 6). Hacker sells 22 million Unacademy user records after data breach. Bleeping Computer.
[17] The Week. (2020, May 7). Unacademy hacked, data of 20 million users up for sale.