INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN: 2455-0620 [Impact Factor: 6.719]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 8, Issue - 5, MAY - 2022 Publication Date: 31/05/2022

DOIs:10.2015/IJIRMF/202205012 --:-- Research Article

PRIVACY INVASION – A THRIVING ISSUE IN CYBER CRIMES

[1] By Dr. S. K. Nayak, [2] Dr. Jaswinder
[1] Director, [2] Assistant Professor in Laws,
[1, 2]G. H. G. Institute of Law for Women, Sidhwan Khurd, Ludhiana, Punjab
Email - jasrupdhamija1985@gmail.com

Abstract: *The protection of privacy is one of the most important issues on the Internet today and is of concern to the users of the Internet. Websites are collecting personal information from users through online registrations, surveys and forms. Information is also collected from users in the form of 'cookies' and most of the users are even not aware of it. People of all fields are increasingly using the computers to create, transmit and store information in the electronic form instead of the traditional papers, documents. Information stored in electronic forms has many advantages, it is cheaper, easier to store, easier to retrieve and for speedier to connection. Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection.*

Key Words: *Privacy, Invasion, Cybercrimes, Information Technology, Internet.*

1. INTRODUCTION:

Cyber-crimes or a crime committed in the virtual world of the Internet wherein "the computer is either a tool or target" is the most pervasive of all forms of privacy intrusions in the modern world. Owing to the extensive use of the Internet and technological up gradation in the e-world people use the Internet for a wide variety of purposes which include social networking sites such as Facebook, Twitter, LinkedIn, etc. These sites have more than 400 million users and applications such as chatting, uploading, photographs and others have the capacity to retain a lot of private information in their databases.[1] Now-a-days companies are hired to watch what internet sites people use and collect the information to create a database for marketing purposes. More malicious acts concerning invasion of privacy include spreading of spyware and the exploitation of various forms of bugs (software, faults). Children and adolescents using social networking sites are easy prey for privacy intruders as they can easily track any information fed by them on the Internet. Threats may include e-mail scams and attachments that get them to install malware and disclose personal information.[2]

In Today's Techno-savvy world, digitalization has replaced the practice of storing and submitting documents in physical form, rather all are now stored in a computer device by the use of electronic form. This practice has many advantages as it is easy to access, retrieved quickly, and hence it is very speedier to communicate. Therefore, the peoples are feeling very reluctant to use this electronic form of data storing and exchanging, as it helps them to carry out their business very smoothly and without any hassle.[3]

The Right to Privacy is a part of the human right, as it has been specifically declared as such, in the United Nations Declaration of Human Rights and many national and other international treaties. Most of the developed nations even added the right to privacy as a fundamental right of their citizens. Privacy is best understood as a cluster covering interest in:[4]

- Control over information about oneself.
- Control of access of information both physical and mental.
- Control over one's ability to make an important decision about family and lifestyle in order to be self-expressive and do develop varied relationships.

2. PRIVACY INVASION TRENDS:

Privacy International has identified a number of important trends that contribute to privacy invasion[5]

1. Globalisation which removed geographical limitations to the flow of data, one of the best examples of which is the Internet.

2. Convergence which is leading to the elimination of technological barriers between systems. Modern information systems are interestingly interoperable with other systems and can mutually exchange and process data.
3. Multimedia which fuses many forms of transmission and expression of data and images so that the information gathered in a particular form can be translated into other forms.

Now a days Data is considered a commodity online and offline by both legal and illegal actors. For this reason, data is a primary target of cybercriminals. Data also plays an integral role in the commission of many cybercrimes, primarily because it is not adequately protected and can be illicitly accessed and obtained. Data breaches have resulted from lost or stolen encrypted flash drives and other storage devices (mainly laptop and smartphones), poor system and data security, unauthorized access to the database or the exceeding of authorized access to a database, and accidental disclosure, release or publication of data. Some notable examples of data breaches include[6]:

- India's national centralized government ID database (Aadhaar), which stores the biometric data (i.e., thumbprints and iris scans) and identity data of 1.2 billion Indians, and is used to verify nationals' identities for financial, government, utilities, and others services, was subjected to a database breach in 2018, resulting in the compromise of identity of data, such as access names, twelve-digit identity number, phone numbers, email addresses, and postal codes, but not the biometric data.
- The information of approximately 30 million South Africans was leaked online in 2017, including their names, genders, income, employment history, identity numbers, phone numbers, and home addresses, because of a data breach suffered by one of the top real estate companies in the country, Jigsaw Holdings.
- Over three billion Yahoo users' data were compromised in 2013, including names, email addresses, passwords (with encryption that could be easily bypassed) and birth dates.
- Deloitte, a global consulting firm was accessed through an unsecured account compromising the usernames, passwords, among other information, of approximately 350 clients.
- The personal data (i.e., national identifier, name, gender, parents' names, home address, date of birth, and city of birth) of over 49 million Turkish citizens was made available in 2016, through an online searchable database.
- The personal and biometric data of over 55 million voters in the Philippines were compromised in 2016, after black hat hackers gained unauthorized access to the Commission of Election (COMELEC) website.

It is true that knowingly or unknowingly a lot of information is uploaded by us on the Internet which can be used by a criminal for harassment or for committing a crime. The crime may involve the data provided by the person or the physical person himself. This is called cyber stalking where the stalker uses the Internet or other modes of electronic communication to harass the persons the virtual world of the Internet provides the stalker with anonymity. In this context, the harassment of the victim due to concealing of identity of the stalker assumes significance. The methods of contact adopted by cyber stalkers include Live Chat or IRC (Internet Relay Chat), Message boards and newsgroups, e-mail and data brokers. Data brokers are the people who sell information collected from private databases. Due to immense increase of Internet use, incidences of cyber-crime or crimes involving use of computers coupled with the use of the Internet is on the rise globally.[7]

3. Steps to be taken for protection against cybercrime[8]

Data theft has become a very common cyber crime now a days. Few steps that can be taken to protect against the cybercrime are:

- **Keep software and operating system updated**
  Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.
- **Use anti-virus software and keep it updated**
  Using anti-virus or a comprehensive internet security solution is a smart way to protect your system from attacks. Anti-virus software allows you to scan, detect and remove threats before they cause a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you peace of mind. If you would use anti-virus software, make sure you keep it updated to get the best level of protection.
- **Use strong passwords**
  Be sure to use strong passwords that people will not guess and do not record them anywhere, or use a reputable password manager to generate strong passwords randomly to make this easier.

- **Never open attachments in spam emails**
  A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.
- **Do not click on links in spam emails or untrusted websites**
  Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.
- **Do not give out personal information unless secure**
  Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.
- **Contact companies directly about suspicious requests**
  If you get asked for data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal. Ideally, use a different phone because cybercriminals can hold the line open. When you think you've re-dialled, they can pretend to be from the bank or other organization that you think you're speaking to.
- **Be mindful of which website URLs you visit**
  Keep an eye on the URLs you are clicking on. Do they look legitimate? Avoid clicking on links with unfamiliar or spammy looking URLs. If your internet security product includes functionality to secure online transactions, ensure it is enabled before carrying out financial transactions online.
- **Keep an eye on your bank statements**
  Our tips should help you avoid falling foul of cybercrime. However, if all else fails, spotting that you have become a victim of cybercrime quickly is important. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

4. PRIVACY INVASION AND INDIAN LAW:

For quite a long time in India there was no law governing cyber laws involving privacy issues, jurisdiction issues, intellectual property rights and a number of other legal issues. To optimize benefits of ICTs and secure confidence of user's information society should be safe and secured not only through cyber laws per se but also appropriate enforcement mechanisms. In order to formulate strict statutory laws to regulate the criminal activities in the cyber world the Indian Parliament passed the ''Information Technology Act, 2000"to protect the fields of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber-crimes. The Act was further amended in the form of Information Technology Amendment Act, 2008. The Information Technology act, 2000 contains a number of provisions which can be used to safeguard against online/computer related privacy. The Act provides for both civil and criminal liability with respect to hacking (Sections 43 and 66)[9], imprisonment for a period up to three years for electronic voyeurism (Section 66E), phishing and identity theft (66C, 66D) and offensive e-mail (66A). Section 72A of the I.T. Act penalizes the unauthorized disclosure of personal information by any person who has obtained such information under a lawful contract. Besides these the Act also contains provisions with respect to data protection under Section 43a.[10]

Section 43a of the IT Act 2008 asks corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable security practices' failing which they would be liable to compensate those affected by any negligence attributable to the failure.

Sensitive personal information includes:

a. Password
b. Financial information such as bank account, credit card or debit card details
c. Physical, physiological and mental health conditions
d. Sexual orientation
e. Medical records and history
f. Biometric information
g. Any detail relating to the above clauses as provided to body corporate for providing service.
h. Any of the information received under the above clauses by the body corporate for processing, storing or processing under lawful contract or otherwise.

Any corporate body is forbidden by the rules from collecting sensitive personal information unless:

a. The information is collected for a lawful purpose connected with a function or activity of the agency and
b. The collection of the information is necessary for that purpose.

Apart from this there are many other offenses that are included under the information Technology Act, such as:

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offence or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offences.

5. CONCLUSION:

Privacy does not exist in cyber space. The various websites that offer varied services to its consumers fail to protect their personal data time and again. The Sony website including its play station and music website was hacked at least three times this year. Scores of personal data was stolen and the consumers were kept in dark regarding the breach for almost a week. Speaking as a consumer, if a large corporate company like Sony cannot protect its website from being hacked into, it is hard to imagine other websites protecting itself from attacks. The rise of the Internet has brought with it a new dimension of crime. The IT Act 2000 has brought some reprieve to the aggrieved according to the NCRB. Despite this, the IT Act clearly will not completely deter criminals from hacking into websites, as was demonstrated in the NCRB report. The cyber criminals of the February 2000 cyber-attacks have yet to be apprehended and the attacks on various websites have been increasing every year. Despite progress being made on enacting cyber laws and implementing them, cybercrime is still not nipped in the bud. Governments can do precious little to stop it and only hope that a cybercriminal can be traced back and be punished. Hence, Internet users need to more careful of the sites they visit; know the privacy policy of these websites to protect their personal data as much as possible.[11]

REFERENCES:

1. Black, Jay (1994). Aeropagitica in the Information Age, Journal of Mass Media Ethics, 9 (3), 134.
2. Westin, Alan F. (1967). Privacy and Freedom, Athenum, New York.
3. Chinmoy Patra, "A Study Of Indian Law On Protection Of Right To Privacy In The Cyber World", *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 (Visited on: April 27, 2022)
4. *Ibid*
5. Nair, Pradeep (2008). Cyber Journalism Legal and Ethical Issues, Media Law and Ethics: Readings in Communication Regulation, edited by Kiran Prasad, B.R. Publishing Corporation, New Delhi
6. *Available at*: https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html (Visited on April 30, 2022).
7. The State of Privacy (2014). Privacy International at www.privacy.org
8. "Tips on how to protect yourself against cybercrime", Available at: https://www.kaspersky.co.in/resource-center/threats/what-is-cybercrime (Visited on April 30, 2022)
9. Information Technology Act,2008
10. Anish Roy, "Privacy issues in Cyber World", *INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES*, Volume 3, issue 3, 2020 Page 1388 – 1397.
11. "Cyber Crimes & Privacy", *Available at*: https://cis-india.org/internet-governance/cyber-crime-privacy#:~:text=Cyber%20Crime%3A%20Its%20Implications%20to%20Privacy&text=Attacks%20such%20as%20these%20demonstrate,to%20extort%20and%20blackmail%20individuals (Visited on: April 27, 2022)