"Right to Privacy is A Myth in This Digital Era"

Written by Abhimanyu Arya

4th Year Law Student, Manipal University Jaipur

ABSTRACT

This article focuses on the'Right to Privacy' in today's world, an in particular focuses on privacy and information technology. Nowadays, it has become much easier for an outsider to gain access to sensitive information despite proper precautions are taken to prevent the same. Despite having the right to privacy enshrined under Article 21 of the Indian Constitution which guarantees right to life and personal liberty, citizens are frequently asked to share details like Aadhaar Card/PAN Card, phone numbers, address, etc. and the same is often misused in many ways. Despite having the Information Technology Act, 2000 to primarily ensure cyber security, the provisions are not strong enough to curb the same offences committed in unconventional forms. The databases having important personal details, are always on the verge of getting hacked by anonymous people and this had caused severe problems for almost everyone. This article ultimately points out the loopholes in this sector and gives possible solutions to prevent such offences in future.

Keywords: **Privacy, Information Technology, Information**

INTRODUCTION

To begin with, a famous quote by Gary Kovacs, *"Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet."* In the generation we live in, privacy is something which most of the people try to maintain in every aspect to prevent any unnecessary interference in their lives. In simple terms, privacy is defined as a private space maintained by an individual without catching anyone's attention. But there is an important question which most of the people have – is our privacy at risk?

This question is completely valid as our data is being collected almost everywhere for various reasons be it our PAN card or Aadhar card details or our phones numbers, these details are technically easy to access. Though, there isn't any specific policy or law for the same in the recent judgement, it has been observed that the 'Right to Privacy' is a part of Article 21 of the Constitution of India which enshrines personal life and liberty. It might not be an extra right, but it can be subjected to certain restrictions. Probably, that becomes a point where we feel that right to privacy is nothing but just a myth in this generation.

CASES OF DATA-BREACH

Over the time, there have been various cases where sensitive data were reported to have been stolen. Taking an example of a recent case where the State Bank of India exposed the sensitive information of over 422 million customers because one of the servers was left exposed in January 2019. There was another case in which Bigbasket reported its data breach where the sensitive information of over 2 crore customers were sold to a dark web forum in November 2020. Resultantly, India witnessed an increase of 37% of cyberattacks in the starting of 2020.

The same year, the electronic information of over 111 million users at Unacademy was compromised and the same was sold on the dark web for Rs 1.5 lakh approximately. The biggest breach involving the leaking of confidential information was the case of Kudankulam Nuclear Power plant in Tamil Nadu. In September 2019, a malware attack was reported by the Nuclear Power Corporation of India in which all the information was illegally taken using Track malware following which, nobody could access the data or other information stored in the system. The investigation revealed that the malware was originated from North Korea and was executed by a group based there called Lazarus Group.

Not just India, there are numerous cyber attacks being reported in different parts of the world. In 2012, Russian based firm Kaspersky disclosed a type of malware called Red October which was commonly used as a part of cyber warfare, particularly for espionage. It was commonly used to transmit information be it personal or top-level governmental. Following this, 60 domains were shut down.

The cyber attacks of 2017 not just affected Ukraine but also other countries like France, Germany, Italy, Poland, Russia, United Kingdom, the United States and Australia. This was perpetrated using the infamous Petya malware. It also included ransom ware and cyber terrorism. As per the reports, Ukraine was severely affected after which Germany became the second country affected by the same.

There are some groups across the globe notoriously known for cyber-attacks at a large scale. These include:

1. **LulzRaft**
   This group based in Canada, was known for low-profile attacks. They started with their attacks from 2011, targeting groups like Husky Energy and Conservative Party of Canada, coming up with false information.

2. **World of Hell**
   This group was known for its high-profile attacks in 2001. It was considered as a grey hat computer hacker. They usually targeted the servers which had weak security. They would also post light-hearted messages after completing their attack.

3. **Vulcanbot**
   This was a Trojan botnet that struck Vietnam in 2009. It was known for political motives. Initially, they targeted Vietnamese Professionals Society by spreading the

botnet over the website. As per the reports, over 15,000 computers were affected under this attack.

4. **Zeus**
   This has been subjected to controversy as this was a Trojan horse malware package commonly found over several versions of Microsoft Windows. Through man-in-the-browser keystroke logging and form grabbing, sensitive information were reported to have been stolen. It further added problems when CryptoLocker ransomware was automatically installed in the systems. In July 2007, the United States Department of Transportation reported a case of data-theft. Phishing and Program downloads were other methods used under the same.
   In 2010, The Federal Bureau of Investigation (FBI) launched a crackdown. It was reported that the hackers who were responsible for the creation of the malware package along with the ransomware were from Eastern Europe. More than 100 people including the infamous hackerHamza Bendelladj were arrested by the FBI along with others from UK and Ukraine on the charges of bank fraud and money laundering.

METHODS INVOLVED

Looking at the cases above, there are several methods which are commonly used in such offences. Some of them are:

A) ***Hacking and Cracking***
This is one of the most common methods in the world of cybercrime. Defining the same, hacking involves accessing data in other systems and can be done in a good or bad sense whereas cracking is considered as negative as it is done maliciously.

B) ***Phishing***
Phishing is perhaps one of the easiest ways of getting information. In this, an email or message is sent to a user under the cover of a reputed organisation asking for their details such as passwords, bank details etc.

C) ***Virus Transfer***
This method has been quite common. A mail or folder is sent to a system which secretly contains virus. It is considered as a program which disrupts the system maliciously and makes it completely unusable.

D) ***Targeting Ads/Pop-up Ads***
These are advertisements which are quite common over the Internet based on the preferences of the users. Pop-up ads are those which appear on the browser just after a click. However as per the FTC standards, they tend to have malicious content and they are not completely banned till now.

Disrupting a system using any of these methods is a cyber contravention under Section 43 of the Information Technology Act 2000. This sectionincludes gaining access, damaging, providing services, denying, disrupting, stealing, concealing and

deleting system information and the accused is held liable to pay the damages for the same.[1]

Cyber-crime is defined Section 65 of the Act which states any person who alters, conceals or destroys the computer or source code. [2] The punishment can be imprisonment or fine or both.

CONCLUSION

The only law implemented in India for cyber security is the Information Technology Act, 2000. Even then, it can be considered as a strong legislation to provide remedy to the citizens. But the problem does not endthere. The common nemesis of such attacks is targeted ads which are quite prevalent over the internet. Nothing significant has been done to curb them. The IT Act only has provisions for safeguardingdata, information or records stored in various systems and to prevent unauthorised or unlawful use of the same by any person. However, in February 2020, the Ministry of Electronics and Information Technology reported that the IT Act will have a better structure in terms of having proper focus on the cyber-security and to improve the same.[3] With reference to the case of ***Sharda v. Dharampal*** [4]in which the Court stated about balancing public as well as privacy rights. That is why, India needs to have a strong legislation for protecting such data by maintaining a perfect balance so that the same is not misused by anyone because somebody has rightly said, "The more technology we bring into our lives, and the more our privacy seems to slip away."

[1] Information Technology Act 2000, Section 43 ([Penalty and compensation] for damage to computer, computer system, etc.)

[2]http://www.karnikaseth.com/cybercrimes-defined-under-the-indian-it-act2000.html

[3]https://www.ikigailaw.com/cyber-security-framework-under-the-it-act-in-india/#acceptLicense

[4] AIR 2003 SC 3450