INDIAN JOURNAL OF LAW, POLITY AND ADMINISTRATION

ISSN: 2582-7677

Vol.3 Issue 1, 2022

SPAM AND ITS POSITION IN INDIA: AN ANALYSIS

Diya Malik

Amity Law School, Noida

Abstract

Technology is becoming the driving force behind any economy. When we use the internet, the web sites save our most recent search, the IP address used to conduct the search, and the e-mail address of the person who conducted the search. Most organizations have easy access to these facts, which they utilize to carry out actions such as mailing UBEs and UCEs which are categories of spams. Thus, promotional enterprises not only send spam e-mails against our will, but when we use a search engine for a separate unrelated search, the same institutions track us through pop-ups and other means in reference to the aforementioned search. We occasionally receive spam in our inboxes, the vast majority of spam and there is a lot of it, is positively detected. Spamming is the act of sending unsolicited bulk and/or commercial messages to a large number of people all over the world via the internet. Spam mail clogs the service provider's network, messing with and disrupting services to subscribers. Spam emails not only deplete the user's/limited consumer's resources, but they also impose cost burden on the service provider. Spam is defined as unsolicited or unwanted communications received on mobile phones via short messaging service (SMS). These SMS spams are a real pain in the neck for mobile subscribers. This type marketing strategy disturbs service providers because it irritates their customers or perhaps causes them to lose subscribers. Fighting against Spam is global issue. In this paper, I tried to carefully analyze the problem of spam and its current position in developing country like India, and how this rising problem of spam can be curbed and controlled.

Introduction

Spam doesn't need much of an introduction. Anyone with an e-mail account has experienced the exasperation of being bombarded with offers of pills from virtual pharmacists, financial pitches and images for fetish sites that should not exist. Receiving unsolicited and

ISSN: 2582-7677

Vol.3 Issue 1, 2022

unsubscribed promotional e-mails and messages, or unsolicited e-mails/text messages referring to the augmentation of particular organs of the body, or unsubscribed sexually explicit e-mails, are all examples of "spam." Spam is the cheapest approach to reach out to a potential client base, and it somehow offers the visibility to the receiver of the e-mail because one has to open the spam e-mail to delete it or read it. By the time the recipient of the e-mail uses the delete option, the e-labeling, mail's the brand's name, and other details have already unconsciously registered in the recipient's mind. Electronic spamming is the most widespread type of spam. It is the practice of sending unsolicited communications, often advertisements, using electronic messaging systems, as well as sending messages repeatedly on the same website. Email type of spam is the most recognized spam. Similar type in other forms , such as message spam, newsgroup spam, Web search engine spam, blogs, wiki spam, online classified ads spam, and so on, are also referred to as spam.

“By way of a Monty Python joke about a menu that includes Spam in every dish, the word "Spam" was coined after a luncheon meat. As the meal is typically loathed and despised, the word was transferred by an analogy.”

While some spam e-mails are not so harmful, such as a promotional email, commercial e-mail, or transactional e-mail, others are malicious and might compromise important data maintained on the system. Advertisers continue to spam as they have zero operating costs, they only have to manage their mailing lists, servers, IP, and domain ranges. Due to which it's arduous to hold senders accountable for the mass mailings. Another key reason for sender non-accountability is because the obstacles to entry are low, which explains why there are so many spammers and so much unsolicited mail.

Unsolicited Bulk e-mail (UBE) and unsolicited commercial e-mail (UCE) are the two most important categories of spam . UCE, as defined by international legislation, is a advertising, promotion, and marketing of a certain good/product or service, whereas UBE comprises mass mail that isn't necessarily sent for promotional purposes. UCEs and UBEs are distributed via one of two methods: the dictionary approach or the e-mail harvesting method. E-mails are sent to series of e-mail addresses or to common address through the dictionary method. The problem with this strategy was that not the existence of e-mail addresses, but the return of

ISSN: 2582-7677

Vol.3 Issue 1, 2022

such emails with the virus or any other problem. The second method, e-mail harvesting, was slightly more complicated. This was done by creating software that would detect e-mail addresses and the code of the web pages which can alert the user.[1]

History

Spamming can be traced back to the late 1800s, Central Western Union permitted telegraphic messages to be transmitted to various destinations across its network. However, the earliest known event of a mass unsolicited commercial telegram can be traced back in May 1864, when several British officials received an unsolicited telegram advertising during a practice.

The first known instance of email spam occurred in 1978, when a message announcing the availability of a new Digital Equipment Corporation model was sent to 393 ARPANET subscribers. A single mass email was sent instead of mailing to the individual email address. Despite the unfavorable reaction from the internet community, the spam managed to produce some purchases. Spamming was used as a prank by participants to send unwanted garbage emails to their opponents' accounts. 'Make Money Fast,' which was posted in 1988, was the first known electronic chain of unsolicited junk emails.

Electronic spamming was overlooked in major countries until the early 1990s. The first big commercial spam incidence occurred when a group of lawyers began advertising immigration law services on bulk Usenet. Because of the subject line of the posting, this event became known as the 'Green Card Spam.' The lawyers asserted that they had the right to free speech, which included the ability to deliver unwanted commercial messages, to the response of criticism.[2]

On March 31, 1993, the first registered case among Usenet users was filed. This is frequently misrepresented as the first use of the term spam to refer to spam mail. The first Usenet case

[1] Aaditya Vijaykumar, The scam of spam: The fallout of Supreme Court's decision in Shreya Singhal v. Union of India | SCC Blog SCC Blog (Sept 26,2017), https://www.scconline.com/blog/post/2017/09/26/the-scam-of-spam-the-fallout-of-supreme-courts-decision-in-shreya-singhal-v-union-of-india/

[2] Rebecca Furtado, An Overview On Laws Against Spamming In India - iPleaders iPleaders (Sept 3,2016), https://blog.ipleaders.in/overview-laws-spamming-india/

ISSN: 2582-7677

Vol.3 Issue 1, 2022

occurred when Richard Depew, while experimenting with moderation software, mistakenly posted over 200 duplicate messages to the newsgroup. Joel Furr is thought to have been the first to report spam on March 31, 1993. MUDs(multi-user-dungeons) are a more likely source of the term "spam," which refers to some electronic messages. The term "spamming" can be used to illustrate a number of actions, including spamming a computer with random data, "spamming the database" by flooding it with new items, and flooding a chat session with a large amount of undesired material. Basically, anything involving dumping undesirable electronic trash into the accounts of other members. MUDders used the term "spam" for the first time in 1990, when they were, ironically, discussing the origins of the term "spam" as referring to electronic garbage messages. According to undocumented sources, it has been known among MUDders for quite some time before that, as the substance of the reported message shows.

Within a few years, the focus of spamming shifted to email, and it has remained there to this day. From the mid-to-late 1990s, some high-profile spammers used aggressive email spamming to make spam primarily an email phenomenon in the public mind.

Forms Of Spamming

There are major 4 types or forms of spams. Each and every person is atleast familiar with one type of spam in his daily life. Some major forms are explained below:

1. **SMS**: The majority of spam is generated by telecommunication companies (telcoms) sending SMS to their users, the Telecom Regulatory Authority of India (TRAI) issued guidelines to telecom companies in 2020, requiring them to be mandatory registered under the Telecom Commercial.Communications Customer Preference Regulation (TCCCPR), 2018. The majority of telcoms, on the other hand, are either unregistered or expired, and they continue to send unsolicited messages to everyone by just changing the header or code.

2. **Calls**: Over 1.8 million telemarketers were disconnected as a result of the Union's actions between 2011 and 2019, but the calls continued. The TRAI's Do Not Call (DNC) registry, which allows customers to restrict which telemarketing calls they receive, is yet another

ISSN: 2582-7677

Vol.3 Issue 1, 2022

failed attempt. The TRAI has levied financial penalties worth thousands of crores on telecoms for failing to prohibit Unsolicited Commercial Communications (UCC), yet this hasn't stopped telemarketers from making spam calls.

3. **WhatsApp**: Many websites have added the option of 'Click to Chat,' which, when clicked, automatically begins a WhatsApp chat without the user having to store the number in their contact list. This gives spammers access to the user's personal information, which they can then easily exploit.

4 **E-mail**: Spammers download software from the internet, compile a list of e-mail addresses, and send them emails through third-party servers. When users open such emails, they are exposed to a variety of risks, including but not limited to: registration at unscrupulous sites in which is a threat to privacy (e.g. passwords, mobile numbers, bank account details), damage to IT security (e.g. targeting government officials at ISRO, MEA, Nuclear scientists), harvesting of e-mail addresses in one's contacts, viruses from attachments, and so on.[3]

Problems caused by Spam

1. **Limitations on Bandwidth**: Spam entering an organization's network uses network bandwidth that could be used elsewhere for legitimate purposes. With the rise in spam quantities, especially newer varieties of spam, more bandwidth is being used for non-legitimate purposes per message. This necessitates the adoption of larger data pipes in certain circumstances just to maintain acceptable performance.
2. **Storage Requirement**: As more spam hits an organization's network, more of it must be sent to spam isolation for review. Because spam is typically retained for at least 30 days to allow staff to analyze the material for false positives, an increase in spam volume in an organization will eventually result in increased storage requirements.

[3] Sasmitha Kumaravadive, THE CHRONIC PLIGHT OF SPAMMING IN INDIA IRALR (2021), https://www.iralr.in/post/the-chronic-plight-of-spamming-in-india

ISSN: 2582-7677

Vol.3 Issue 1, 2022

3. **Staff Productivity Loss:** While some feel that staff productivity loss is a big worry for many firms, A research has discovered that it is a minor concern in the overall context of the spam problem. However, it is a problem for some smaller businesses that do not sufficiently filter spam at the server or gateway.
4. **Various Issues**: There are a variety of other issues related to spam, such as phishing attempts that appear to come from a legitimate source, such as a bank, but instead direct recipients to enter their confidential information on a phisher's website; some employees wasting time exploring products and services offered in spam; links provided in spam messages that may re-route users to harmful or offensive websites. Spam is delivered through e-mail and might involve attractive subject lines such as "free" "once-in-a-lifetime opportunity," and other similar phrases to entice one to open and read the message. This is just what the spammer wishes. Opening an email, reading it, and then deleting it takes time and money from the internet connection. The mail servers that deliver the mail across a network of servers use money and capacity to deliver trash that is inconsistent. Furthermore, for the sake of delivery, trash mail would have taken precedence over urgent correspondence. A few spam e-mails include attachments and request that open them. Furthermore, the costs of removing a virus from the computer are enormous.

Methods Opted By Spammer

A spammer can obtain email addresses in a variety of methods. Here are some of the most common tactics spammers use to obtain individual e-mail addresses:

- User newsgroup postings
- User registrations on dubious websites
- Chat sessions with users
- From spammer-purchased email lists
- Spam bots that scour the internet for any @ symbol
- From user-subscribed mailing lists
- Collecting all of the email addresses stored on company's server

ISSN: 2582-7677

Vol.3 Issue 1, 2022

- By generating name combinations for domain at random.

Some more methods :-

- **Hostile ISPs**: Spammers with sufficient funding run hostile ISPs. They can now utilize several domain names as a result of this. The inter NIC provides it with its own network numbering and various domain names. One might be able to block a domain, but one won't be able to block an ISP.
- **'On-the-fly' Spammers**: These are spammers who register as several legitimate users with various ISPs. They build an identity by fabricating one or stealing credit cards and using them to create one. They then start spamming from these accounts. The spammer switches to a different account by the time the ISP realizes they are sponsoring a spam run.
- **Blind Relays**: Some servers with bad configurations allow for blind relaying, or sending anonymized communications. Blind relays are used to route spam.

Why Spammers Use Spam ?

Spammers send their messages to people around the world in the hopes that someone will react. They earn money by selling the products themselves or by receiving a percentage fee from the sale of such products. Response rates, benefit margins, and expenses are typically poor. The massive number of messages spammers can post in a single day can add up to a substantial sum of money. For example, a spammer may make Rs.6,00,000 by sending 10 million email messages with a Rs.60 per unit profit margin and a 0.1 percent response rate. All that is required of the spammer in order to send spam is the following:

- **Spamming software**: This is a low-cost option that can be found simply on the Internet.
- **An email address list**: These can be purchased through various sources.

ISSN: 2582-7677

Vol.3 Issue 1, 2022

- **A cash opportunity**: Spammers appear to have no shortage of options. Spam emails frequently include information about product sales, special offers, and adult site membership, among other things.
- **An email server**: Spammers frequently use the mail servers of a trusted third-party to hide their identity. These servers have previous open relay server experience.[4]

How And Why Spam Is Harmful

1. **Information or content**

Mostly the criticisms of spam are based on its content or subject matter. Commercial messages that encourage dubious projects or messages that contain sexually explicit information are frequently objected to. The single most significant objection concerns messages that contain hazardous embedded programming and hostile file attachments.

2. Internet Resource Consumption

Spam consumes a substantial quantity of bandwidth usage, memory, storages, and other resources, accounting for a substantial chunk of all e-mail traffic. Web users and server

[4] P. Mohan Chandran, A Comparison of Spam Laws between India & The U.S., Boloji.com (Sept.9,2020), https://www.boloji.com/articles/52001/a-comparison-of-spam-

ISSN: 2582-7677

Vol.3 Issue 1, 2022

admins spend a significant amount of time reading, deleting, filtering, and blocking spam, resulting in higher Internet connection costs.

3. Internet Security Threat

Spammers mostly make use of Simple Mail Transfer Protocol (SMTP) servers to transmit same type of a message to a large number of people. Because it is an illicit use of computing resources, third-party relaying is usually considered service theft. The reputation of a corporation may be harmed if it is linked to spam as a result of third-party relaying.[5]

Whether Spamming should be considered as crime ?

Now the disputed question emerges whether spamming should be considered as crime.

For this we need to know what is cybercrime and whether spamming can be considered as offense or not in law.

In simple words Cybercrime can be defined as "criminal action committed on the Internet." The involvement of criminal activity in the definition of cybercrime is a deciding factor in determining whether spamming is a cybercrime or merely a waste of time. The key issue is to determine how to punish email spamming if it is deemed as cyber-crime. In other words, how would it be able to determine whether email spamming constitutes criminal activity?

The intention of old legislations suggest that the email spam should be included in the junk mail category and should be criminalized. In the case of junk mail, the sender covers the cost of sending the email, whereas in the case of spam email, the receiver endure the price through higher Internet Service Provider operating money. When dealing with the challenge of categorizing offenses, criminal law frequently refers to outdated laws that no longer apply to modern crime. As a result, in the case of email spam, the line of attack is to classify spam

[5] Sudhiriiita, Email Privacy & Anti-spam Law, Legalservicesindia.com (2017), http://www.legalservicesindia.com/article/107/Email-Privacy-&-Anti-spam-Law.html

ISSN: 2582-7677

Vol.3 Issue 1, 2022

emails as trespassing. However, the offense of trespass would be valid in the eyes of the Internet Service Provider, but not in the eyes of the recipient of spam and junk email.

One group of people argues that it can take away the right of freedom of speech and expression. The argument is that because the Internet is largely used for sending and receiving emails, and because it is an unregulated domain, there is a right to free speech. This point is likewise not to be overlooked. The major two issues are content of the email and the forum which has disseminated the spam email. The right of freedom of speech and expression is not always absolute as there are some limitations imposed on the expressions. If any email contains any racist, sexist remarks then it will come under the criminal law. However, most of the spam emails doesn't contain such content, which keeps such mails out of the ambit of criminal law and crime. Another debatable matter in question is whether email spam is a public or private medium depends on whether it is a wrong done against the receiver or wrong done against the internet service provider, which might be counted as a public medium. This is the central point of difference between supporters and opponents of a campaign to criminalize spam email, where the disagreements are based on deeply held fundamental ideas.[6]

Spam laws in India

Technology is becoming the driving force behind any economy. However, all governments require rigorous regulation to ensure that such driving forces follow the law and act in the greater good of society. The Internet is one such technology that spans the globe and is not under the direct jurisdiction of any single government or law. Countries such as the United States and the United Kingdom have introduced a legislative framework to safeguard the interests of its residents and traders. By 1994-1995, the world started to acknowledge and understand the internet's capability for uploading and disseminating information, for research and development, for corporate transactions, and for e-commerce, among other things. To

[6] Ib.id

ISSN: 2582-7677

Vol.3 Issue 1, 2022

coherently constrain the virtual world, as it came to be known, the United Nations General Assembly chose to adopt a model law on ecommerce, which gave thorough guidelines for safeguarding and protection of digital data, and how certain wrongdoings such as hacking could be eluded, and how data transmission could be made more expedient. India was one of the signatories of this resolution. India was required to adopt the United Nations resolution into municipal legislation because it had signed it. As an outcome, the Information Technology Act of 2000 (IT Act) was enacted, proclaimed, and implemented. While the enactment of the IT laws it was suggested that other laws, such as the Penal Code of 1860, the Evidence Act of 1872, the Bankers' Books Evidence Act of 1891, and the Reserve Bank of India Act of 1934, can be revised, and re-enacted at the same time.[7]

In 2000, India sanctioned it's very first legislation , the Information Technology Act, to command and oversee the Internet and e-commerce. However, as technology progressed, the nature of the offenses in this field changed, and the provisions of the current statute were discovered to be inadequate. A few isolated incidences of customer data theft from BPOs/call centers shocked India's entire information technology sector. It was quickly evident that the existing Act needed to be updated to incorporate measures dealing with the misuse of advanced technology. An Expert Committee was composed by the Indian government concerning to amend and revamp the Information Technology Act of 2000. The Committee has submitted its recommendations and ideas to the Government of India after considering a number of problems, including privacy and data protection Electronic contracts, violation of privacy and privacy, child pornography, e- signatures and other issues have been addressed by the Committee. However, the suggestions include no mention of phishing, pharming, or spamming being prosecuted. Spamming is the act of sending unsolicited bulk and/or commercial messages to a large number of people all over the world via the internet. Spam mail clogs the service provider's network, interfering with and disrupting services to subscribers. Spam emails not only deplete the user's/limited consumer's resources, but they also impose financial strain on the service provider.

[7] Ib.id

ISSN: 2582-7677

Vol.3 Issue 1, 2022

The Information Technology Act of 2000 (the "IT Act") makes no provision for the regulation of "spamming." The IT Act, on the other hand, regulates obscenity, which includes publishing, transmitting, or causing to be published in electronic form any anything that is lascivious or appeals to the prurient interest, among other things. Is it possible that a "spammer" may be prosecuted under such a clause, given that pornography makes up a major amount of "spam e-mail"? In any case, Section 67 phrasing is vague, and it's feasible that an ISP may be held accountable if it's alleged to be "transmitting" such electronic information. An action for nuisance arises when an act causes material injury to property or causes human distress. The term "nuisance" comes from the French word "nuire," which means "to hurt" or "to irritate." In the lack of any statutory protection for checking spam email on the Internet, classic tort law doctrines of "trespass to goods" and "law of nuisance" may be required to handle the issues created by spammers. Until new legislation specifically regulating spam is enacted, it appears likely that Indian courts will employ existing tort statutes to deal with the issue of spam. Trespass to goods comes in picture when the defendants' unlawful disturbance of the plaintiffs' possession of the goods, emanate in harm to the goods. According to the International Telecommunication Union, "Although there is no one-size-fits-all strategy to combat spam, suitable laws and efficient enforcement are two key components in the fight. Because spam is such a new phenomenon, not all countries have spam laws, and even those that have are having difficulty enforcing them on a national and international basis. Spammers are proactively gripping the advantage of the Internet's global availability. As a result, crossborder collaboration is critical in the development, implementation, and subsequent enforcement of new legislation."

It does not, however, encompass conduct pertaining to online deception, which may lead to consumers voluntarily transferring their personal data. Phishing and pharming are examples of such acts that are not fully covered by the proposed modifications. In such circumstances, the criminals/offenders build a website with a strikingly identical domain name as well as a comparable appearance and feel to the company's actual website. The consumer/user, believing he is accessing the company's website, enters personal information that is recorded by criminals/offenders. These offenses are related to misrepresentation and passing off and are distinct from hacking, unauthorised access, or tampering, for example. The consumer/user

ISSN: 2582-7677

Vol.3 Issue 1, 2022

may not suffer a direct financial loss, making it difficult for authorities to punish the perpetrator under the Information Technology Act. [8]

Right To Privacy And spam

Online privacy is jeopardized because users frequently lack control over the information they generate, and the border between what is private and what is public information is frequently blurred. This has resulted in a situation in which information shown on social networking sites can be utilized as evidence against a person or to make conclusions about that person. The occurrences, among other things, raise the question of whether social media discourse is private or public. Another important aspect of internet privacy is how law enforcement can access online messages and habits through interception, access, or surveillance.

In India, the legality of intercept is based on its compliance with constitutional requirements that allow for legitimate limitations on the exercise of rights by Indian individuals. Interception of private or personal communications violates both the right to free expression and the right to privacy. While the Constitution does not expressly guarantee the right to privacy, Indian courts have consistently interpreted it into the concept of the fundamental right to life and personal liberty. Countries around the world have taken steps to address internet privacy issues, such as enacting legislation enforcing do not track rules, the right to be forgotten, breach notification, legitimate access standards, and data retention regulations. Spams are considered as violation of the individual's right to privacy through breach of their personal data.[9]

Steps Taken By TRAI

[8] Rahul goel, The Indian Information Technology Act and Spamming Icommercecentral.com (April, 2006), https://www.icommercecentral.com/open-access/the-indian-information-technology-act-and-spamming-1-3.pdf

[9] Telecommunications and Internet Privacy in India, CIS India (2014) https://cis-india.org/internet-governance/telecommunications-internet-privacy.pdf

ISSN: 2582-7677

Vol.3 Issue 1, 2022

On March 12, 2021, the Telecom Regulatory Authority of India ('TRAI') published a statement mandating organisations that use telecom resources to deliver bulk messages to their customers to comply with the Telecom Commercial Communications Customer Preference Regulations, 2018 ('the TCCCP Regulations'). The TRAI also underlined that the TCCCP Regulations provide a framework for managing unsolicited commercial conversations and enable telecom service and access providers to establish codes of behaviour. Additionally, the TRAI stated that, in accordance with the TCCCP Regulations and norms of practise, a bulk communication sender must, among other things, register as a "primary entity" and, when relevant, obtain consumer consent.

On March 23, 2021, the TRAI issued a second order requiring that all organisations that use telecom resources to deliver bulk messages to consumers promptly comply with the regulatory requirements under the TCCCP Regulations.

The TRAI issued a third order on March 26, 2021, demanding that all organisations that use telecom resources to deliver bulk messages to consumers meet the regulatory obligations under the TCCCP Regulations by March 31, 2021. The TRAI, in particular, highlighted a number of defaulting businesses and warned that continued failure to comply will result in the barring of non-compliant messages beginning April 1, 2021. All these taken by TRAI eventually failed to get the desired result, these regulations were not enough to combat the menace of spam.[10]

Analysis of Shreya Singhal Judgment

While the IT Act was long overdue, there were many failures in the legislation which consisted of a great fiasco in acknowledging the growing number of junk mails and messages. Multifold possibilities, such as measures to defend or protect privacy, identity theft, cyber terrorism, and others,that were not foreseen or given in the IT Act. In order to

[10] India: TRAI orders compliance with spam regulations, DATA GUIDANCE (2021), https://www.dataguidance.com/news/india-trai-orders-compliance-spam-regulations.

ISSN: 2582-7677

Vol.3 Issue 1, 2022

address the aforementioned scenarios, the legislature enacted a series of reforms in 2008 to enhance the information and technology regime. The newer reforms or amendments strengthened up the IT Act, but also, for the very first time, it also included the provision for an anti-spamming law [Section 66-A(c) of the IT Act], which ultimately made intermediaries and corporates accountable for providing personal information (Section 43-A read with Section 72-A of the IT Act), and also confected the junk or spam website accountable in case the spam alters or destroys information on the website. Any provision of law can be exploited or misused, and because Section 66-A of the IT Act is very hazy and unclear about the whole scenario, it was misused and exploited by certain politicians against two upright citizens, which led to the filing of a writ petition titled **Shreya Singhal v. Union of India** before the Supreme Court of India, which challenged the validity of Section 66-A of the IT Act. The Supreme Court nullified Section 66-A in its totality, ruling that it violated Article 19(1)(a) of the Indian Constitution, which safeguarded the fundamental right to freedom of speech and expression, and was not saved or rescued by Article 19(2) of the Indian Constitution. The decision also made critical comments about Section 66-A of the IT Act's obscurity and vagueness. It becomes very important to outline that the anti-spamming regulation sanctioned by the legislature [Section 66-A(c) of the IT Act] was awfully indefinite, speculative, and failed to furnish sufficient and effective parameters to combat spamming. The government adopted relatively simple and poorly defined privacy standards in an attempt to define what constitutes appropriate security policies and processes. These standards only apply if the parties have not agreed on their own reasonable security practices and procedures, as mentioned above .There is currently no law in India that addresses the issue of spam, nor has one been adopted.

The freedom of speech and expression which is a fundamental right must take ascendancy, as the Supreme Court has held in a series of decisions, the Court must have apprehended that Section 66-A(c) of the IT Act was enacted to obviate the misusers and spammers from sending spams, and the striking it down would allude that the companies' right to advertise can override. The main aim of Section 66-A(c) of the IT Act was to make sure that national security was not endangered or compromised by spam emails, as it was previously done with the Bhabha Atomic Research Centre, the Supreme Court made a blunder. Section 66-A(c) of

ISSN: 2582-7677

Vol.3 Issue 1, 2022

the IT Act should not have been invalidated as averting spamming can also comprise of jeopardizing state and national security and safety. The Supreme Court failed to recognize that the law [Section 66-A(c) of the IT Act] was secured by the conception envisioned and elevated in Article 19(2) of the Indian Constitution, depicting decency and morality, as the law [Section 66-A(c) of the IT Act] attempted to protect receiver from receiving any type of brazen sexual e-mails/text.

The right to privacy of the spam recipient was another factor that could be examined. Some e-mails when it comes to spam usually send viruses or threats to computer that can ingress the receiver's personal and private information without modifying or annihilating it, but may also re-send the data through the infected connections. The receiver has a right to privacy under Article 21 of the Indian Constitution, which is equally important right as right to freedom of speech and expression argued by the petitioners, it was solely up to the Hon'ble Supreme Court to decide which one of the following will carry out the greater public interest, i.e., to entirely struck off the statute or to strike down the unconstitutional portion of the Act. Yet other development of the repeal of Section 66-A(c) of the IT Act is that if any organization sends a spam, it can be sued for wrong under tort law and the Penal Code.[11]

Recommendation and Solution

As Section 66-A of the IT Act was repealed in its totallity, it is now felt like a need to enact legislation which eventually governs and regulates spam. Given the volume of spam mail that a person receives on a daily basis, the suggested law would need to be implemented quickly.

The legislature should consider enacting a separate law on the subject that includes:

(a) A clear definition of spam , what constitutes spam, and separate definitions for UBE and UCE.

(b) An opt-in and opt-out approach, an organization must first obtain the user's permission to send the e-mail/spam, the reciever need to verify that he or she desire to subscribe to such e-

[11] Ib.id

ISSN: 2582-7677

Vol.3 Issue 1, 2022

mails, and if the user has already subscribed, as long as an opt-out alternative where the reciever can unsubscribe at his or her own wishes; this opting out option must be fulfiled by the organisation.

c) Parameters pertaining to:

i. correct labeling or substance in the spam's subject title. sexually explicit material
ii. the method of obtaining reciever's email address by the sender
iii. identification of the spammer, including address, contact number, and information;
iv. a one-year limit on the number of UCEs that can be sent; and
v. A systematized enforcement mechanism should be there. A civil and criminal action for the same should also be suggested by the legislature.

(d) If the corporation that has broken the law's requirement is based in a foreign country, the government should allow for extraterritorial application of the Act.

(e) The legislature can also opt for a " zero disturbance" or "block spam " choice , similar to the one implemented by the TRAI.

(f) Promotional activities can be opted by the State or its instrumentalities to check the performance and sovereign functions.

(g) Another way to reduce spam is to add human interaction proof to each e-mail, which would make it impossible for businesses to send mass messages.

(h) The creation of a strong and proactive Tribunal to enforce the Act's provisions.

Other Legal Methods

ISSN: 2582-7677

Vol.3 Issue 1, 2022

Stringent legislation is required to address the problem of spam in the absence of appropriate technological protection. Despite the fact that anti-spam legislation exists all across the world, the tactics for battling spam are nearly identical, as evidenced by the following:

1) Prohibition

A strict anti-spam legislation that can proactively forbid unsolicited bulk commercial e-mail messages. For example: Unsolicited commercial email is not prohibited by the European Union, however it is permitted by individual member states. UCE is illegal in Finland, Germany, and Italy, while both UCE and UBE are illegal in Austria.

2) Anti-Spam policies are enforced

ISPs and other destination operators have policies in place that control the use of their facilities for various purposes, and almost all of them prohibit spamming in particular. As a result, some legislation places a extra attention on adhering to these standards.

3) Opt-out provision

Several laws, including the CAN-SPAM Act in the United States, allow senders to contact with anybody except those who have explicitly opted out. Therefore opt- out provision can prove to be helpful and efficient.

4) Statutory Requirements

Some states' have data protection laws which can control the storage , use, and transfer of personal information, including e-mail addresses, and legislation can be proposed to limit spammers' ability to harvest e-mail addresses from domain name registration records.

5) Mechanisms of Enforcement

In addition to or instead of private actions, several jurisdictions provide for criminal sanctions or other state enforcement tools.

ISSN: 2582-7677

Vol.3 Issue 1, 2022

The vast number of anti-spam laws implemented and the harsh penalties meted out to spammers demonstrate that the international community has acknowledged the spam threat and is taking effective measures to counteract it. It's past time for India to jump on board. [12]

Suggestions at individual level

- In India, a coalition of Internet-related firms and associations is required to assist consumers and businesses in combating spam.
- A permission to send an email to a stranger must be requested, and only one reminder should be issued. When a request for permission is declined, it should be assumed that the request has been rejected, and use of the email address for any purpose other than self should be strongly restricted.
- Spammers employ techniques such as evading detection and luring unsuspecting consumers into opening spam emails. The sender's email address should be required to be disclosed with every email sent, so that his identity may be confirmed and tracked.
- Sending an email with false information in it should be considered a significant violation.
- Any ambiguous email shall not be sent to anyone; if someone acts on the basis of any ambiguous email sent to him and suffers a loss as a result, he should be paid appropriately and adequately.
- It should be made illegal to send any greedy or seductive email to anyone.
- Details on industry standards for sending business e-mail must be discussed and developed.
- Both long-term and short-term projects should be used to assess the scope of India's spam problem.

[12] Rahul dhonde, Spam: Is it time to legislate - Internet law in India Legalservicesindia.com (2017), http://www.legalservicesindia.com/articles/spamli.htm

ISSN: 2582-7677

Vol.3 Issue 1, 2022

- A comprehensive study or survey should be conducted to ascertain the effcacious of anti-spam legislation.
- Sharing information would aid in the development of efficient countermeasures against high-volume spammers.
- Anti-spam legislation must pertain to businesses and people that intend to send emails with misleading subject lines.
- Fraudulent e-mails should be punished criminally and civilly.
- A thorough assessment should be conducted to prevent reaping and dictionary assaults, as well as the usage of scripts to deliver massive volumes of e-mail accounts.
- Civil society organizations that demonstrate consumer and business interests; active end users who monitor and assess spam; anti-spam legislation that encompasses not only organizations and people whose products are advertised in spam email, but also those who willfully assist in the transfer of illegitimate spam.[13]

There are numerous reasons for establishing a complete law that prohibits, controls, and punishes spammers —

The Honourable Delhi High Court recognised the lack of proper spam legislation, holding that in the absence of statutory measures to check spam communications, classic tort, trespass, and nuisance concepts would have to be applied. The ever-increasing number of Internet users, along with the ever-increasing portion of spam email, therefore it becomes imperative to control spam before it reaches epidemic proportions, similar to the United States. The Ministry of Information Technology has begun discussions to include anti-spam laws. However, the Ministry has yet to decide whether spammers should be punished after determining the nature of the spam, i.e., whether the spamming was done accidently or on purpose.

[13] Ib.id

ISSN: 2582-7677

Vol.3 Issue 1, 2022

The government is considering establishing a Centre for Communication Security Research and Monitoring to keep an eye on criminals' online activity. Development of Telematics centre can be made a nodal implementation agency for the project. The Centre's Research wing would focus on a variety of communication technologies and monitor all types of traffic, including satellite, wireline, wireless, the Internet, email, VoIP, encrypted communication for de-encryption of net-based encryption methods, regulatory standards for telecom operators to adopt, and system design. In addition to the aforementioned activities, the Coalition Against Unsolicited Emails has developed an Indian branch to address the spam problem. All efforts to combat spam would be difficult in the absence of strict legislation and technological developments.[14]

Current Analysis

With India's growing Internet population, the government should strengthen its Cyber Crime Prevention Initiative to combat this threat. Following the repeal of Section 66A (of the Information Technology Act 2000, which was replaced by the Information Technology Amendment Act 2008), India require a legislation to curb the problem of spamming. To combat the spamming threat, anti-spam rules, opt-out clauses, prohibitions, statutory restrictions, and enforcement procedures must be implemented. However, we must first determine if we need to eliminate or simply regulate Spam. Some civil rights groups argue that anti-spam law could lead to constitutional difficulties like restricting free expression on the Internet, hence anti-spam legislation must be highly targeted. The Supreme Court said that 'commercial advertising' is an intrinsic feature of the right to free expression safeguarded by Article 19 of the Constitution. As an outcome, anti-spam legislation can only be applicable to ‘commercial email’.

We already have consumer protection regulations in place to protect netizens from any fraudulent or deceptive advertising. There is also legislation against the transmission of

[14] Ib.id

ISSN: 2582-7677

Vol.3 Issue 1, 2022

pornography, but it has to be amended so that netizens are protected from getting sexually explicit information via spam. As of now, the Indian government has yet to enact laws that directly addresses the problem of spam. Spamming is not covered by the Information Technology Act of 2000 (IT Act 2000), but it does involve obscenity, which includes publishing, transmitting, or causing to be disseminated in electronic form any anything that is lewd or appeals to sexual curiosity.

To prepare legislation for cyber security and IT regulations, including spamming, the government should convene a panel and include more technical individuals and professionals from the IT business. The government is also considering whether spammers should be punished after determining the nature of the spam attack, such as if spamming was done accidently or on purpose. In India, cyber law is still in its infancy, and more measures are required to develop it into a competent legal instrument. To make the existing IT Act 2000 safer, sturdier, and more pertinent, the government has to give it a new and distinct design. It must also keep in mind India's critical ICT and cyber security requirements, which are woefully lacking.

Conclusion

Legal Framework should take their time dealing with societal issues, especially when the nature of the issues is obscure and the technology that underpins them is quickly evolving. In any case, the question of spam is not a merely a legal one: no matter how carefully crafted a legislation is, it will not address the problem. At a time when most developed countries are revising their existing legislation and enacting new legislation to combat spamming, phishing, and pharming, it is critical that India implement suitable provisions to prosecute criminals in such circumstances. The law should be time to time updated to include all new technological advancements and related offenses. The importance of spam warning awareness and education cannot be overstated. This will aid in the creation of a fair competitive environment and a consumer-friendly cyber market. Because spam takes up so much of our time and resources, it will indirectly boost our productivity. Stopping spam will allow actual marketers to communicate with their customers more efficiently, resulting in increased demand and supply for the economy. The less spam there is, the more customers

ISSN: 2582-7677

Vol.3 Issue 1, 2022

will trust online businesses. Controlling spam will reduce our spending on anti-spam software, allowing us to put that money into more worthwhile projects. After learning about the benefits of anti-spam legislation, let us hope that India adopts a strong anti-spam legislation that punishes spammers severely. Through its multiple telecoms marketing rules and standards, India has already achieved a large degree of control over telephone call spam. Furthermore, it has a high success rate in penalizing defaulters for non-compliance with these communications regulations; if we can apply laws similar to our own mechanism for emails, the day will not be far off when our country will be among the top-three spam control laws.