Page 671 - 680 **DOI:** *https://doij.org/10.10000/IJLSI.11791*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 3 | Issue 3

2020

An Analytical Study of Emergence of Spamming and Cyber Squatting as Major Cybercrimes

IPSITA SARKAR[1]

ABSTRACT

The internet is rapidly expanding in India. It has given rise to new possibilities in every industry, including entertainment, marketing, sports, and education. Every circumstance has two outcomes, which is universally true. Furthermore, it is the same with the internet, whose applications have both advantages and downsides, with cybercrime being one of the most serious downsides. Cybercrime is becoming a severe menace to governments, police departments, and intelligence agencies throughout the world. Initiatives to curb cross-border cyber terrorism are taking form. Indian police have established better cyber cells around the country and have begun training personnel and workforces.

Understanding spam behavior and the threat that harmful spam poses, including the prevalence, frequency, length, and severity of these frequent kinds of cybercrime. Cyber Squatting is the registration of the internet domain names, devoid of the intention of using them in the names of popular brands or personalities merely to encase money.

This research paper is an attempt to provide a glimpse of cybercrime in India and the world, especially Spamming and Cyber Squatting.

Keywords: *Cybercrime, Spamming, Cybersquatting, Internet Domain*

I. INTRODUCTION

The Internet is quickly becoming an integral component of a million people's lives and a way of life. It has become an identical type of existence and living in the sphere of the Internet. The general people are now capable of performing activities that were unthinkable only a few years ago. It is due to humanity's increasing reliance on emerging technologies, that communication of nearly any type of information has become incredibly easy and rapid because of the internet and the usage of websites. The fast rise of information technology in today's age has engulfed all vocations. Whereas computers are intended to preserve privileged material of political, social, and economic importance to society, the global expansion of the internet and computer technology has increased internet-related crimes.

[1] Author is a student at Student at Alliance University, India.

 [ISSN 2581-9453]

In the Asia-Pacific area, India is listed as the number two internet-user country. As a result, as we progress in terms of development, cybercrime increases. In recent years, India has emerged as a key destination for cybercriminals, the majority of whom are hackers and other dangerous individuals. India is rated sixth in the world in terms of cybercrime. There is no explicit definition of cybercrime in Indian law, but Indian Technology 2008. In the words of Dr. R.K. Tewari, "cyber-crime may be said those species, of which, genus in the conventional crime, and where either the computer is an object or subject of the conduct constituting crime."[2]

Dr. Debarati Halder and Dr. K. Jaishankar mentioned that cybercrimes are "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)."[3]

II. SPAMMING

(A) Overview

Spamming is the practice of sending unsolicited mass communications over electronic messaging systems such as e-mail and other digital delivery systems and transmission mediums. Spamming may also occur in media such as online forums, instant messaging, and mobile text messaging, as well as social networking spam, junk fax transmission, television advertising, and sharing network spam. It is particularly widespread due to economics, as it has very low to no operational expenses and requires just a minute response rate to produce a profit. The majority of them are commercial adverts that may include malware, adware, or fraud. With an aim to boost confidence in online commerce and protect interest of consumers, Governments have introduced anti-spam legislations to protect consumers and businesses.[4]

(B) Prominence and Persistence of Spamming

The opportunities provided by a low-risk, low-cost, profitable illegal activity such as spamming, particularly the embedding of malware in spam, appeal to criminals and criminal networks. Responses such as the London Action Plan recognize that malicious email is a global concern since it is a primary avenue for the spreading of malware, which may have a significant social and economic impact. If we go further, we can discover the following

[2] Petter Gottschalk, 'Policing Cyber Crime' [2002] (2) Lexis Nexis Publication 75
[3] Jonathan Clough, Principles of Cybercrime (2nd edn, Cambridge publication 1998) 12
[4] MTariq Banday, 'Design and Development of E-mail Security Protocols and Forensic Tools' [2011] International Conference on Recent Advances in Electronics and Computer Engineering 224

reasons why spamming is so prevalent and persistent among cybercriminals:

1. Lower charge and wider scale: Although the volume of malevolent spam may seem inconsequential if looked from an individual's perspective, it has been estimated that, in 2013, approximately 183 billion emails were sent and received every day, and the volume of malicious communication was substantial.[5]

In 2015, the Internet Governance Forum reported a lower estimate of 116 billion emails sent each day.[6] It has been estimated that 80 to 85 percent of this mass email traffic is spam. An additional study of spam and phishing recognized a small number of high-risk ISPs that were 'internet bad neighbors' which were mainly concentrated in India, Brazil, West Africa and Vietnam.

2. Performance and profit: Spam allows malware to reach high-volume, low-value targets that are less likely to have effective anti-virus or other countermeasures in place. Botnets ensure spam delivery and account for between 80 and 90 percent of all spam sent globally. This mass spam comprised 750,286 unique spam messages. Spam offers a high return with little investment. Spammers collect gross global revenues in the order of US$200m per year, while some $US20b is spent fending off unwanted emails.[7]

3. Social engineering: Social engineering is the improved method of the depiction of chances of malware infection are increased. Malware that requires user interaction, such as campaigns that entice users to download and execute a malicious file, account for almost half (44.8%) of the identified compromised emails and are often referred to as other propagation tactics like autorun, file infector or brute-force methods.

4. Low risk: Cybercrime is a lucrative and less dangerous growing sector. Cybercriminals may easily operate practically from anywhere in the world, and with the aid of technologies such as The Onion Router (TOR), the Dynamic Domain Name System (DDNS), and virtual private networks (VPN), they can easily remain anonymous. source Such approaches evade network surveillance and traffic analysis, which may lead to the location of the attack's origin.

5. Crime networks: This is responsible for the increasing engagement of networked criminal groups, which has affected the scope and sophistication of cybercrime. These organizations can take the shape of classic, hierarchically organized criminal syndicates or they can just

[5] The Radicate Group, Inc. A Technology Market Research Firm "Email Statistics Report" 2013-2017
[6] Internet Governance Forum "IGF Report November 2015"
[7] Mamoun Alazab and Roderic Broadhurst, 'Trends & issues in crime and criminal justice' [2016] (526) Australian Institute of Criminology

perpetrate digital crime. Malware coding, email address collection, social engineering of communications, and message distribution are all essential talents. The spammer engineers the emails to avoid anti-spam filters and ascribes malware to them, which then administers the granted PCs.

(C) Spamming in India

The first UseNet and email spam campaigns worldwide date back to 1994-95[8], more or less overlapping with the start of TCP/IP internet connectivity in India, and the resulting widespread accessibility of email addresses from local as well as foreign email providers.

Indian internet service providers firstly functioned with UseNet servers to provide NNTP access, but soon drew back such services and, in some cases, blocked UseNet access from their service, because of massive amounts of abuse originated by an unknown but probably New Delhi based Internet vandal and author of Usenet and email spam software, who was only known by the signature 'HipCrime'. Indian email sellers saw the economies of scale they could attain with email spam. Commercial spam initiating from India was then, and still is, mainly used to promote goods and services, advertising everything from used computers to real estate and holiday timeshares.

India's first potential damage caused by cybercrime was in 1998, an anti-nuclear collection of hackers called 'milw0rm' conceded servers of Bhabha Atomic Research Centre (BARC), and downloaded confidential documents about India's nuclear weapons program. They published some pages along with a detailed description of the technique they used to break into BARC's servers. The milw0rm crew was apparently later approached by a terrorist calling himself Khalid Ibrahim.[9]

(D) Anti-Spam Laws in India and The World

Anti-spam legislation is legislation governing unsolicited communications that protect citizens from getting undesired spam emails. Many of these rules were preempted by the CAN-SPAM Act of 2003; nonetheless, most email service providers require all users to adhere to anti-spam measures in their terms of service. It is also crucial to understand that anti-spam rules vary based on the state and nation in which you live.

Given the severity of the issue and the potential damages spam can cause, legislative measures have been suggested in several countries to control and possibly eliminate spam.

[8] Keith Lynch, 'Timeline of spam related terms and concepts' (*Keith Lynch's timeline of net related terms and concepts*, 2006) <http://keithlynch.net/index.html> accessed 13 May 2021

[9] Niall Mckay, 'Do Terrorists Troll the Net?' (*Wired*, 4 November 1998) <http://www.wired.com/news/politics/0,1283,15812,00.html> accessed 5 May 2021

These legislations have introduced different parameters.[10] Legislation, however, cannot prohibit spam on its own. Brazil, Russia, India, and China are among the world's largest developing broadband markets, providing a huge opportunity for cybercrime. In India, there is no legislation to prohibit spam, nor have courts found an occasion to issue guidelines on the subject.

In 1997, Nevada became the first American state to pass anti-spam legislation. Following that, California, Washington, and Virginia did the same. In today's environment, over 37 American states have anti-spam legislation. Almost 51 of the 191 UN member nations have anti-spam law.

In 2005, India attempted to fix the Information Technology Act of 2000 to make it a law governing e-commerce, digital signatures, and many aspects of online crime. In August 2005, an 'Expert Committee was formed. They recommended a few changes to the IT Act. Even though there were no particular spam amendments, the software industry was represented. It proposed that Section 43, which is comparable to Section 66, be used to replace Section 66, which provides for the criminal crime of 'diminishing the value' of any data residing on a computer resource.

In 2006 the government introduced a bill amending the Information Technology Act. The Parliamentary Standing Committee reviewing that bill noted that while examining the Information Technology (Amendment) Bill, 2006, the Committee were apprised by the industry representatives/legal experts that ‘spam’ or the issue of receiving unwanted and unwarranted e-mails have not been addressed under the proposed amendments.[11]

In the above context, the Committee asked whether it would not be prudent to incorporate specific provisions in the proposed law to protect the e-mail account holders from unwarranted mails. In reply, the Department of Information Technology stated that Sub-Section (b) of Section 66A and Clause (i) of Section 43 of the IT Act addressed the issues pertaining to spam.

As a close scrutiny of the above said two Sections revealed that the issue of spam had not been adequately covered, the Committee in evidence desired to know how could the menace of spam be appropriately tackled with. In response, the Secretary, DIT replied that unwarranted e-mails could be generated from anywhere in the world.

[10] Evangelos Moustakas and others, 'Combating Spam Through Legislation: A Comparative Analysis of US and European Approaches' [2005]
[11] Suresh Ramasubramanian and Pranesh Prakash, 'Spam and Internet abuse in India: A brief history' [2013] World Cyberspace Cooperation Summit IV (WCC4)

The sections that the Department of Information Technology was referring to --- Sections 66A (b) and 43(i) --- had been newly introduced in the amending bill, and they read as follows:

43. If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network --- (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. [12]

66A. Any person who sends, by means of a computer resource or a communication device, --- (b) any content which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently makes use of such computer resource or a communication device, shall be punishable with imprisonment for a term which may extend to two years and with fine[13].

In response to the Standing Committee's remark that "the problem of spam had not been sufficiently covered", the government, when introducing the Information Technology (Amendment) Bill, 2008 added a new sub clause (c) to Section 66A, by setting the maximum punishment to 3 years:

66A. Any person who sends, by means of a computer resource or a communication device, --- (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.[14]

III. CYBERSQUATTING

(A) Overview

Cybersquatting is the situation that indicates the cases where an individual or a company enrols a domain, where such domain name is identical or like a trademark of any other party. These cyber squatters then maliciously try to trade the same for profit.

Because of the decrease in the value of domain names and the growth in numerous top-level domains (.biz, .cn, .mob, and lately.in), it appears that cybersquatters are generating a lot of criminal income. The cyber squatters then sell the domain to the genuine person or

[12] Information Technology (Amendment) Bill 2006, s 43 (i)
[13] Information Technology (Amendment) Bill 2006, s 66A (b)
[14] Information Technology (Amendment) Bill 2008, s 66A (c)

corporation that owns a trademark that has been utilised in the domain name to generate illegal money. This may be considered as ransom, as that domain name has already been registered by someone else and cannot be registered again in the name of the trademark owner. In this demeanour, a cybersquatter infringes the fundamental rights of the owner of the trademark to use its trademark.

Cybersquatting is achievable in many way, and typosquatting is the most popular form of cybersquatting.[15] It relies on the fact that people using the internet, make typographical errors while entering domain names in the browsers. Some of the common examples which we can see are the exclusion of "dot" while entering the domain name: wwwexample.com; misspelling the name of the proposed site: exemple.com; using a distinctively phrased domain name: examples.com; or add any other top-level domain: example.org.

The other fact that a cybersquatter relies on is that in the case when the holders of the trademark himself own the domain name he often overlooks to re-register his domain names. A domain name is not registered for a fixed period, and if not re-registered before its expiry, then the domain name can be purchased by anybody. In such cases, the cybersquatters enrol that particular domain name in their name. This process is called "renewal snatching."

(B) Global and Indian Scenario

U.S. Anti-Cyber-Squatting Consumer Protection Act (ACPA) of 1999 defined cybersquatting as an act introduced to protect the trademark owners of distinctive trademark names against cybersquatters. The victim has two options:

Either sue the cyber squatter under the provisions of the Anti-cybersquatting Consumer Protection Act (ACPA) or use the International System of arbitration by the Internet Corporation of Assigned Names and Numbers (ICANN).

The jurisdiction is always a matter of obstacle in the case of courts. The seat of the trial should be the place of the plaintiff, the defendant or the place of the service provider through which the name is enrolled.

The World Intellectual Property Organization (WIPO) Arbitration and Mediation Centre has taken a step to render an Internet system for the administration of commercial conflicts concerning intellectual property. This is an unusual form of dispute solving mechanism that it is proposed to be used both for filling of evidence and for document exchange. It is an economical and reasonable service where the arbitration takes place online.

[15] Vernita Jain, " (What Is Cybersquatting And It's Position In India, 20th January) <https://blog.ipleaders.in/cybersquatting-position-india/> accessed 1 June 2021

Globally, the United Nations copyright agency WIPO (World Intellectual Property Organization) has provided a negotiation system wherein a trademark holder can strive to profess a squatted site. In 2006, there were 1823 accusations filed with WIPO, which was a 25% increase over the 2005 rate. In 2007, it was stated that 84% of claims made since 1999 were decided in the complaining party's favour. It is an agency which is specialized to form a balanced system that is easily accessible.[16]

In India, victims of cybersquatting have been provided with several ways to deal with the situation such as sending cease-and-desist letters to the cybersquatter, opting for arbitration under ICANN's rules, going for a trial to a state or federal court.

By relying on the interpretation given by Delhi High Court in Manish Vij v Indra Chugh[17], the Indian courts have defined 'cybersquatting' as "an act of obtaining fraudulent registration with an intent to sell the domain name to the lawful owner of the name at a premium".

To conduct the case on a fast-track form of resolution, a case could be filed with the National Internet Exchange of India (NiXI).

In India, the Information Technology Act holds no provisions to punish cyber-squatters and does not provide for any legal compensation. Apart from this, the registry has taken steps to provide compensation to companies who are the victims and to dissuade such cybercriminals from further stealing domains.

Few cases that elaborate the situation of the crime cybersquatting in the country are:

1 Yahoo! Inc. v Akash Arora[18]

It is the first case that was reported in India concerning cybersquatting. In this case, the plaintiff was a registered owner of the domain name "yahoo.com". He obtained an interim order which delimited the defendants from dealing the name "yahooindia.com" or any other trademark similar to the trademark of the plaintiff.

The decision, in this case, is brief in clarifying the law of passing off for infringing trademarks and domain names, as well as in situations of services. Most significant, this lawsuit raised awareness of the notion of cybersquatting and established the remedies accessible to plaintiffs in such situations. The case is also seen as a pivotal point since it was the first time in India that a domain name was equated to a trademark and afforded similar

[16] Vernita Jain, " (What Is Cybersquatting and Its Position in India, 20th January) <https://blog.ipleaders.in/cybersquatting-position-india/> accessed 1 June 2021
[17] *Manish Vij v Indra Chugh* [2002] Del 243
[18] *Yahoo!, Inc. v Akash Arora & Anr.* [1999] Del 229

protection from passing off. By affirming the aforementioned criteria, the court established that domain names that pass the test of distinctiveness are entitled to protection from passing off and infringement.

2. Tata Sons Ltd v Ramadasoft[19]

Tata Sons, a subsidiary of the Tata Group, successfully evicted a cybersquatter from ten contested internet domain names. They filed a complaint with WIPO, which determined that the domain names used by Respondent were confusingly similar to the Complainant's trademark TATA, implying that Respondent had no rights or legitimate interests in the domain names and had registered and used them in bad faith. The order transferring the domain names from the Respondent to the Complainant was based on these specifics.

3. Arun Jaitley v Network Solutions Pvt. Ltd.[20]

The Hon'ble High Court of Delhi resorted to Uniform Domain Name Dispute Resolution Policy Rules 4(a) and (b) (UDNDR Policy). Essentially, the regulations allow for a complaint process in the event of a domain name being registered in bad faith. The defendants' behaviour was determined to be in violation of ICANN regulation on the basis of bad faith registration as well as inadequate justification to maintain the domain name in its possession after the expiry term.

IV. CONCLUSION

Internet crimes have proven to be a considerable financial burden on users. Its regulation raises both technological and legal issues. Furthermore, legal and technical remedies to spam and cybersquatting have been ineffectual in addressing the issue.

However, if the state aims to strike a compromise between the right to privacy and the right to free commercial expression, the "opt-out" alternative may be the way to go. A more effective solution will need the collaboration of legal, technical, and international initiatives. Law enforcement may be made more successful by technologically increasing e-mail users' capacity to identify message senders, but the difficulty with legal procedures is their geographic reach in cases of spamming and validating trademarks before granting or reissuing a domain name. The national legislative efforts must be integrated with international cooperation. This 'cooperation at regional levels is gaining roots.

Tough regulation must be adopted in this area to discourage squatters and, as a consequence,

[19] *Tata Sons Ltd. v Ramadasoft* [2001]
[20] *Arun Jaitley v Network solutions Pvt. Ltd.* [2011] DLT 716

avert repeat occurrences. Because squatters may deceive clients and steal bank data for profit, cybersquatting raises risks for organizations involved in financial/commercial activities. People who acquire domain names in bad faith that are identical or confusingly similar to a brand should have access to expedited judicial remedies. Stricter penalties, such as imprisonment and/or substantial fines, may deter cybersquatters and provide trademark owners with a fighting tool in protecting their intellectual property in cyberspace.

*****

 [ISSN 2581-9453]