Spam and internet abuse in India

A brief history

Suresh Ramasubramanian Pranesh Prakash

2013-11-01

Proceedings of 2013 World Cyberspace Cooperation Summit IV (WCC4)

Abstract

This is a short paper on the historical growth and spread of spam and Internet abuse, including telemarketing and mobile messaging spam, in India. Additionally, it covers current and proposed Indian law, and regulatory / law enforcement actions against cybercrime.

The Internet in India

India's first exposure to the Internet was relatively late, compared to regional pioneers such as Korea (1981-82). At various stages from 1986 to 1992, the Government of India established three wide area networks, INDONET (to interconnect IBM mainframes running at different government, academic and industry installations around the country), ERNET, (Education and Research Network, to interconnect universities and research institutions) and NICNET (National Informatics Centre Network, to interconnect Government departments).

Meanwhile, companies with offshore development centers in India, with Texas Instruments being the first to set up a software design centre in Bangalore in 1985[1], were allowed to establish VSAT connectivity back to their US headquarters. These were expensive and subject to strict Government regulations[2], till the Software Technology Parks of India was established in 1991 to provide Internet connectivity to India's growing computer software industry.

Internet rather than WAN connectivity was first established in 1987, with email over UUCP, and Internet connectivity using TCP over X25 through UUNET in Falls Church VA and CWI in Amsterdam[3], first over dialup and in 1989, over a 9600 bps leased line to UUNET. India's .in ccTLD, originally established on 8 May 1989[4], was first hosted at UUNET and later operated locally in India by the

[1] "TI Celebrates 20 Years as a Technology Innovator in India", Press Release. Available: http://www.ti.com/wwlinlnewsdetail/200820051newsdetail_sc05161.html.

[2] "Emergence of Software Policy", Software Technology Parks of Bangalore. Available: http://www.soft.net/background/emrergence-software-policy.html.

[3] Available: http://netchakra.net/chronology/.

[4] "History of the Internet. ccTLDs in chronological order of Top Level Domain creation at the Internic", Nov 2002. Available: http://www.ccwhois.org/ccwhoislcctld/ccTLDs-by-

National Centre for Software Technology (NCST)[5]. X400 based email was also available from 1994, provided by the National Informatics Centre, government owned telecom provider Videsh Sanchar Nigam Limited and Sprint RPG, There was further a thriving local BBS community across several Indian cities.

All these networks, particularly the UUCP based mail systems, continued to be in operation for several years after 1995, when the Government monopoly telecom provider Videsh Sanchar Nigam Limited (VSNL) first provided dialup connectivity with two classes of service, shell accounts that could be accessed over a terminal emulator like HyperTerminal as well as SLIP/PPP connectivity. The shell accounts came with a server hosted mailbox that could be read using the PINE console email program, while PPP accounts were given a limited quota (20 MB) POP3/SMTP email account.

The Indian market was opened up to private ISPs in 1998 and broadband (then 64 Kbps) first appeared on the Indian market in 2003, with the Government of India formulating its first Broadband policy in 2004.

Homegrown websites such as portals (1995), newspapers (1996), free email (1996), newspapers (1997), online banking (1997) and online ticketing (2001) quickly followed, to compete with their international counterparts such as Hotmail and Yahoo, which were increasingly adopted by a growing population of Internet users.

History of spam in India

Spam was not a major problem in India till the introduction of TCP/IP based connectivity. The usual problem in those days was that slow UUCP links to Indian universities would often be saturated by just a few students exchanging email and usenet posts with their friends in the United States.

The first usenet and email spam campaigns worldwide date back to 1994-95[6], more or less coinciding with the introduction of TCP/IP internet connectivity in India, and the consequent widespread availability of email addresses from local as well as foreign email providers.

This was a particularly bad situation for Indian Internet users, who were faced with the problem of downloading large amounts of spam on slow, noisy and expensive dialup lines.

Indian ISPs initially operated usenet servers to provide NNTP access, but quickly withdrew such services and, in some cases, firewalled access to the NNTP port 119 to block usenet access from their service, because of massive amounts of abuse originated by a unknown but probably New Delhi based Internet vandal and author of Usenet and email spam software, who was only known by the moniker "HipCrime"[7].

---

date.html.

5 Sanjay Pathak Profile Information Technology and Services Professional. Available: http://www.linkedin.com/pub/sanjay-pathak/16/820/877.

6 "Keith Lynch's timeline of spam related terms and concepts", November 2002. Available: http://keithlynch.net/snamline.html.

7 Wikipedia Definition of 'Hipcrime, October 2013. Available: http://en.wikipedia.org/wiki/hipcrime/usenet.

HipCrime's activities[8], such as forged cancel floods and "sporgeries"[9] (spam forgeries) with steganographic / Markov Chain generated random gibberish content caused widespread havoc on usenet newsgroups in the mid to late 1990s. This led to several Usenet operators refusing to peer (that is, exchange traffic) with NNTP servers operated by Indian providers, or in some cases, even refusing to accept usenet posts originating from IP addresses controlled by Indian ISPs VSNL and SILNET – a so-called "UDP" or "Usenet Death Penalty"[10].

Indian email marketers quickly saw the economies of scale they could achieve with email spam, Commercial spam originating from India was then, and still is, primarily used to advertise legitimate goods and services, advertising everything from used computers to real estate and holiday timeshares.

Spamming Indian users was quite simple in the early days of dialup connectivity in India, as the monopoly ISP VSNL had set up an "allusers" alias[11] that mapped to all users on their service. This "allusers" alias existed, presumably from the beginning of VSNL's service, till 1998, when it was disabled following a hoax email sent out to all VSNL users by an unknown student, offering VSNL TCP/IP accounts at INR 2000 (about USD 34 at current exchange rates) for 500 hours, compared to the actual cost of a 500 hour account at that time – INR 10,000 (USD 165) – which, at the time, was a whole month's salary for a fresh graduate entering an engineering or computer related job.

By the time the allusers account was disabled, it, and other vulnerabilities in VSNL's email system, had allowed various spammers to download a copy of their complete user database. A wide variety of indigenously produced bulk mailers[12] and email harvesters[13] were released within a few years of the VSNL POP3/SMTP based email service. Several of these included filter avoidance techniques such as "direct to MX mail relay", which would avoid detection by using a mailserver installed on the spammer's desktop rather than routing mail through the ISP's smtp servers, as well as header forgery and the use of open mail relays and HTTP and SOCKS proxies to anonymize the spammer's identity.

Ironically, such software was generally used to advertise legitimate goods and services, with the spam including the advertiser's full contact information including phone numbers as well as postal, website and email addresses.

These bulk mailers' features, as well as their intended use of spamming violated the acceptable use policies of the mostly US based providers the bulk mail vendors' and their customers' websites were hosted on, which lead to several bulk

---

8 "Q: Cryptic writings in the Newgroups", Apr 2002. Available: http://answers.google.com/answers/threadview?id/6396.

9 "[LI] help: Notorious Usenet spammer - who has had India blocked from usenet in the past", Oct 1999. Available: http://linux-india.ooenscroll.onr/linux-india-helo/199910/msg:01396.html.

10 "UDP History". Available: http://www.rahul.net/falk/udphistory.html.

11 Ganapati Priya and Penn Zasha. Rediff on the Net, October 1998. Available: http://www.rediff.com/computer/1998/0ctI12vsnl.htm.

12 "AnonimousEmailBomber removal", August 2002. Available: http://www.spywaredb.com/remove-anonimousemailbomber/.

13 " NUKE: Indian spamware vendor samtecsoft.com ", October 2000. Available: https://groups.google.com/forum/#/topic/news.admin.net-abuse.emaillCcX6RY6bxa4.

mailer vendor and customer websites getting suspended[14] by their providers. Additionally, marketers hiring a spammer to promote their product faced vitriolic hostility from internet users, who would often call or email them back with abusive comments, when they were not using free tools such as Spamcop[15] to report the spam to the spam vendor and spammers' ISPs.

This mirrored a growing trend among US-based Internet users, so that US spammers increasingly began to include a so- called "Murkowski Disclaimer"[16] or "Murk" for short, at the bottom of their spam emails, citing a bill that was introduced in the 105th US congress by Senator Frank Murkowski to claim that their emails should not be considered spam.

> In accordance with Bill S.1618 Title III passed by the 105th U. S. Congress, this letter can not be considered spam as long as we include: (1) Contact information and (2) a way to be removed from future mailings.

Indian bulk mailers introduced a variant of this disclaimer that they began to include in their spam templates, and text like this was found in Indian origin spam till the mid- to late-2000s:

Since India has no anti-spamming law,[17] we follow the US directive passed in Bill.1618 Title III by the 105th US Congress, which states that mail cannot be considered spam if it contains contact information.

Not too surprisingly, the presence of such a disclaimer became a popular rule deployed in various spam filters, which would classify any email containing such a disclaimer, or even the URL of Senator Murkowski's website, as spam. For example, early versions of the popular open source filter, SpamAssassin, had a rule called "MURKOWSKI_CRUFT"[18].

Indian unsolicited email marketing has evolved since then, with several local[19] vendors[20] allegedly providing "snowshoe" spam services that use a succession of randomized domains and continuously switch from one cheap colocation service to another, as and when their existing IP addresses and domains get listed in

---

14 Reference #10—an archived post to news.admin.net-abuse.email, quoting an email from a US based ISP, informing me that they have suspended one such vendor of email harvesting software. Note the "Indian Murkowski" disclaimer at the bottom of the spam sample quoted in the post.

15 "Spam Cop". Available:http://www.spamcop.net/.

16 "Spam and the Law", October 2002. Available: http://www.jamesshuggins.com/h/tekl/spamandlaw.htm.

17 Importantly, India still does not have an explicit law specifically targeting spam, and there exists no graded system of penalties for e-mail spam – unlike the situation in telemarketing and SMS spam, where a do not call list and a tough enforcement regime exist, but are not widely known by the general public. A detailed discussion of telemarketing and SMS spam in India is presented in section IV of this paper.

18 "SpamAssassin rules file". Available: https:llsvn.apache.org/repos/asf/spamassassin/tags/spamassassinrelease150/spamassassin.ct.

19 SpamHaus Main Info. Available: http://www.spamhaus.org/rokso/evidence/ROK10022/century-infotech/main-info.

20 SpamHaus SARV. Available: http://www.spamhaus.org/rokso/spammer/SPMI282/sarv.

widely used DNS block lists such as Spamhaus[21] and SURBL[22], or suspended by their providers.

Even legitimate Indian email marketers face spam related issues due to a widespread lack of awareness of industry best practices[23], as well as a reluctance to audit paying customers' mailing lists, let alone suspend service to a paying customer for spamming. The same issues – lack of awareness of best practices[24] and a reluctance to penalize paying customers, have plagued local ISPs, for whom the effect of a DNS blocklist or ISP listing their IP space may actually last long after the spammer that caused the issue has been removed. Large, legitimate Indian ISPs and online marketers are members of nationwide industry associations such as ISPAI[25] and IAMAI[26], which are working on promoting best practices among their members. Some Indian ISPs and marketers are also joining the broader community of email marketers in international industry associations such as M3AAWG[27], and/or participating in M3AAWG's India outreach[28] initiatives.

Additionally, several best practice documents published by industry associations such as M3AAWG[29], as well as international organizations such as the OECD[30], London Action Plan[31] (in association with CAUCE and M3AAWG), APECTEL (in association with the OECD)[32] and ITU[33], are widely available online.

The challenge remains – as it does around the world, for multistakeholder cooperation between governments, Internet service providers, email marketers and the business community to work together and put in place on the ground implementations of these best practices, suitably customized to suit varying local conditions.

Malware, hacker wars and cybercrime

An increasing number of viruses originating in South Asia began to emerge, beginning with the first known PC virus, the fully stealthed "Brain"[34] written by

---

21 SpamHaus. Available: http://www.spamhaus.org/.

22 "Introducing SURBL URI reputation data". Available: http://www.surbl.org/.

23 "MAAWG Sender Best Communications Practices", September 2011. Available: http://www.maawg.org/sites/maawg/files/news/maawgsendersbcpver2a-updated.ddt.

24 SpamHause ISP Area. Available: http://www.spamhaus.org/isp/.

25 "Promote Internet/Broadband for All", ISPAI. Available: http://www.ispai.in/.

26 "Internet & Mobile Association of India". Available: http://www.iamai.in/.

27 "MAAWG (Messaging Malware Mobile)". Available: http://www.maawg.org/.

28 "India Anti-Abuse Working Group". Available: http://www.maawg.org/india.

29 "MAAWG Published Documents". Available: http://www.maawg.org/published-documents.

30 "OECD Anti-Spam Toolkit of Recommended Policies and Measures", September 2006. Available: http://www.oecd-ilibrary.org/science-and-technology/oecd-anti-spam-toolkit-of-recommended-policies-and-measures_9789264027176-en.

31 London Action Plan. Available: http://londonactionplan.org/node/35.

32 "Malicious Software (Malware): A Security Threat to the Internet Economy", OECD, June 2008. Available: http://www.oecd.org/internet/ieconomy/40724457.pdf.

33 "ITU Botnet Mitigation Toolkit". Available: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

34 "Brain", Wikia. Available: http://malware.wikia.com/wiki/Brain.

two Pakistani brothers Basit and Amjad Alvi[35] in January 1986. In May 1990, the first Indian virus "Happy Birthday Joshi"[36] was discovered. Both these viruses were mostly harmless with data loss, if any, being entirely accidental. Brain did no intentional damage beyond making an infected PC run slowly, and Joshi was a harmless "joke" that did not do much more than make infected PC users wish its creator, Manav Joshi, a happy birthday. The Joshi virus actually prevented PCs that it infected from being infected with the much more damaging "Stoned"[37] virus, which was also prevalent on floppy discs circulating in India at the time.

The first well publicized instance in India of the potential damage caused by cybercrime was in 1998, when members of an anti-nuclear collective of hackers called milw0rm[38] compromised servers belonging to the Bhabha Atomic Research Centre (BARC), and downloaded classified documents about India's nuclear weapons program, some pages of which they published along with a detailed description of the method they used to break into BARC's servers. The milw0rm crew was apparently later approached by a terrorist calling himself Khalid Ibrahim[39].

With an active hacker community in India and Pakistan, and with a decades old enmity between the two countries dating back to from when they were partitioned from colonial India when it became independent in 1947, it was not long before, in 2002, the first hostile virus targeted at Pakistan was released by a group of Indian hackers and spread worldwide - a worm called "Yaha"[40], which was sent out as spam that pretended to offer you a free screensaver, and would rebroadcast itself from infected machines.

Pakistani government websites and the Karachi stock exchange were severely affected by DoS attacks triggered by this worm, and Yaha variants were, in 2002, consistently on the worldwide top 10 virus charts by volume. A Belgian hacker, in fact, released a counter-worm called "Yahasux"[41], which spread by much the same method and would remove the Yaha worm on any PC that it infected.

Malware with political or geostrategic goals is extremely common in the region, with hackers from different countries being accused, and trading mutual accusations of installing malware on computers owned by government agencies[42],

---

35 "Brain: Searching for the First PC Virus in Pakistan", The Alvi brothers interviewed by Mikko Hyponen Chief Research Officer of F-Secure, 2011. Available: http://camoaiQ:lls.f-secure.com/brain/.

36 "Joshi", Wikia. Available: http://malware.wikia.com/wiki/Joshi.

37 "Stoned", Wikia. Available: http://malware.wikia.com/wiki/Stoned.

38 "Wikipedia Definition of 'Milworm.' ". Available: http://en.wikipedia.org/wiki/Milw0rm.

39 McKay Niall, "Do Terrorists Troll the Net?", November 1998. Available: http://www.wired.com/politics/law/news/1998/11115812.

40 Wikidot Definition of Yaha. Available: http://virus.wikidot.com/yaha.

41 Wikidot Definition of Yahasux. Available: http://virus.wikidot.com/yahasux.

42 Malcolm Moore, "China's global cyber-espionage network GhostNet penetrates 103 countries", The Telegraph. Available: http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html.

industries[43][44] and religious or politically sensitive groups[45].

There are also reports of the Indian government recruiting a "cyber army"[46] to breach systems in hostile countries, and promising immunity against prosecution to volunteer hackers hired to do so, and sponsoring a hacking contest[47] with cash awards for breaking into the command and control server of a hostile Advanced Persistent Threat that was targeted at Indian government agencies.

Under normal conditions, this would be immediately seen as unethical and would be widely condemned. However, the situation is much more complicated, given similar policies adopted by other countries, including the alleged use of malware to damage critical infrastructure in hostile countries, such as nuclear power plants[48] and water utility companies[49]. The difference between state and non-state actors is much thinner in online cyberattacks. Further, plausible deniability is much easier to achieve, and much more difficult to trace back and attribute to a government source, than when a regime uses non state actors (such as civilian armed militant groups and terrorist splinter cells) for a physical attack on a hostile country's soil and citizens.

On the surface, there is not much difference between recruiting a civilian militant group armed with army surplus weaponry, and recruiting a group of independent hackers driven by patriotic or monetary considerations, whose only weapons are computers and the Internet. The latter is much easier to achieve, and much more difficult to defend against. Digging deeper, the differences are in the targeted nature of the attack, the executive control and chain of command over the attackers, and the avoidance of harm to civilians and innocent parties. The first two are easy enough to achieve, but on the Internet, the third – avoidance of collateral damage – is extremely difficult if not impossible.

A lot of malware is hosted on compromised servers that have other innocent users on them. Other malware is hosted on sites that have lots of legitimate users, but are also lax in enforcing their acceptable use policies against Internet abuse. Taking down such resources can have, and has had, significant amounts

---

43 Shunal Doke, "BSNL Connecting India", August 2013. Available: http://tech.firstpost.com/news-analysis/pakistans-isi-may-have-installed-malware-in-bsnls-database-103695.html.

44 Norman. Available: http://blogs.norman.com/2013/security-research/the-hangover-report.

45 Graham Cluley, "Dockster Mac malware found on Dalai Lama-related website", Naked Security, December 2012. Available: http://nakedsecurity.sophos.com/2012112/031dockster-mac-malware-dalai-lama/.

46 Harsimran Singh and Joji Thomas Philip, "India Readies Cyber Army to Spy on Hostile Nations", Times of India, August 2010. Available: http://timesofindia.indiatimes.com/india/India-readies-cyber-army-to-spy-on-hostile-nations/articleshow/6260783.cms?referral/PM.

47 David Dittrich, "A New Infosec Era? Or a New Infosec Error?", The Honeynet Project, November 2013. Available: http://honeynet.org/nodel1031.

48 Sanger and E David, "Obama Order Sped Up Wave of Cyberattacks Against Iran", The New York Times, June 2012. Available: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted-allr-0.

49 Tim Simonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant", Technology Review, August 2013. Available: http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/.

of collateral damage[50]. Attacks targeted at critical infrastructure such as electricity and water utility plants can cause radioactive incidents or floods if the malware goes out of control, or spread into the wild and affect utilities in countries the worm was never targeted at in the first place[51]. The situation becomes even more precarious when the country adopting such tactics has millions of malware infected machines and poorly secured government and critical infrastructure within its own borders, making it vulnerable to retaliatory or first strike cyberattacks.

The malware threat to India is exacerbated by the fact that a large number of PCs in India use old and unsupported operating system versions, and frequently use pirated software and operating systems. This threat, coupled with poor implementation of security architecture and policies at ISPs, and a rapid growth in India's broadband penetration, has led to India being listed by the widely used Spamhaus CBL[52] blocklist as the world #1, ahead of China and Iran, in terms of the amount of malware infected devices as well as virus-generated spam. This is based on the absolute number of infected IPs, and countries in the CBL statistics page[53] that have a far lower number of blocked IP addresses may emit much more spam per infected IP. When measured on a pure volume basis, India moves down to #11 in the list[54] and #13 based on the number of infections per capita[55].

This may be due to a wide variety of reasons - local ISPs not implementing port 25 filtering on their dynamic IP addresses and reassigning IP addresses frequently with short lease times, ISPs providing relatively slower connectivity (such as older 2G cellular networks in small town and rural India) The graphs on the next page are provided courtesy of the Spamhaus CBL.

---

50 Michael Sandee, "Critical Analysis of Microsoft Operation B71", Fox IT, April 2012. Available: http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/.

51 Anirudh Bhattacharyya, "Stuxnet hits India the most", Hindustan Times, October 2010. Available: http://www.hindustantimes.com/world-news/stuxnet-hits-india-the-most/article1-608334.aspx.

52 "CBL breakdown by Country Highest by count", CBL, March 2014. Available: http://cbl.abuseat.org/country.html.

53 "January 2014 Rankings", Spam Rankings. Available: http://www.spamrankings.net/rankv2/2013/06/01/monthly/countries/volume/cbl/all/regular/.

54 "January 2014 Rankings", Spam Rankings. Available: http://www.spamrankings.net/rankv2/2013/06/01/monthly/countries/volume/cbl/all/regular/.

55 "CBL breakdown by CountryPerCapita Highest by count", CBL, March 2014. Available: http://cbl.abuseat.org/countrypercapita.html.

Fig 1 – Virus generated spam from Indian IPs

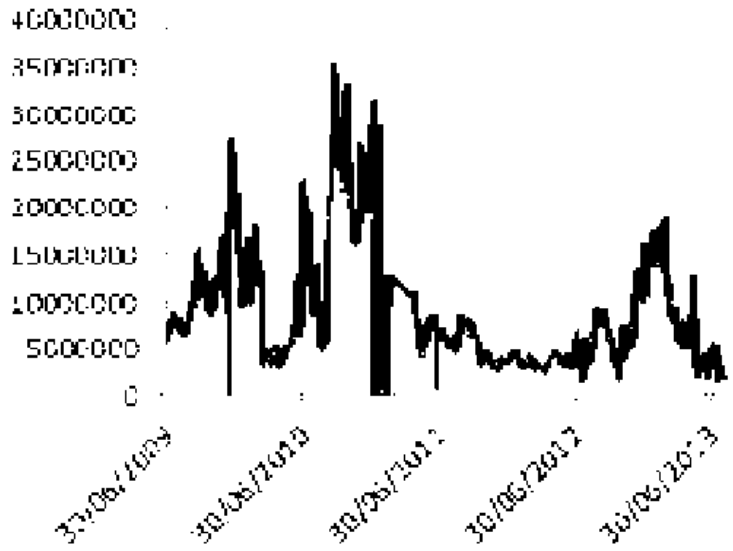

Figure 1: Virus generated spam from Indian IPs

Fig 2 - Virus infected Indian IPs in the CBL

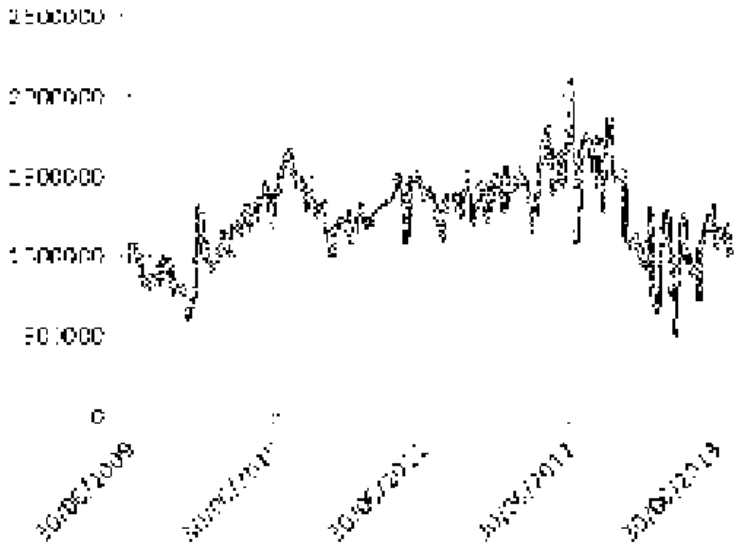

Figure 2: Virus infected Indian IPs in the CBL

Crime and Punishment

The Information Technology Act, a law based primarily on the UNCITRAL Model Law on Electronic Commerce was passed by the Indian legislature in 2000. While that statute had no provisions directly relating to spam, it did have provisions on hacking and on 'damage to computer, computer system, etc.' that were remarkably broad.

Section 66 of the IT Act 2000, a criminal provision relating to 'hacking', provided that any person who 'diminishes [any information residing on a computer resource's] value or utility or affects it injuriously by any means, commits hack'. Further, Section 43 of the Act provided that a person who unauthorizedly 'disrupts or causes disruption of any computer, computer system or computer network' is liable under that provision, with no definition having been provided of what would constitute a 'disruption'. These provisions, which could potentially be stretched to include spam, have never, at the time of writing, been tested against spam. In 2005, efforts were underway to overhaul the Information Technology Act, and to shift its focus from being mainly a law on e-commerce and digital signatures to including many aspects of online crime. An 'Expert Committee' was constituted, which in August 2005 proposed amendments to the Information Technology Act. The committee did not propose any amendments specifically on spam, despite there having been software industry representation on the committee. It did however propose that the extant Section 66, which provided for the criminal offence of 'diminishing the value' of any information residing on a computer resource be replaced by another similar to the extant Section 43. Based in part on the recommendations of the Expert Committee, 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. 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.

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[56] rupees to the person so affected.

and

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.

Apparently in response to the Standing Committee's comment that "the issue of spam had not been adequately covered", the government, when introducing the Information Technology (Amendment) Bill, 2008 added a new subclause (c) to Section 66A, and increased the maximum punishment to three 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.

The terms "electronic mail" and "electronic mail message" were defined in such a manner as to include all electronic communications and not just those that happen over SMTP, which we normally refer to as e-mail.

The flaws of covering spam with the above provision are obvious. The generally agreed-upon characteristics of spam include that it be (i) unsolicited, and (ii) sent in bulk[57]. Less- agreed upon characteristics that are sometimes associated with spam include that it be (i) commercial, and (ii) anonymous[58].

However, Section 66A(c) does not address any of those characteristics, and instead focuses on a message having been sent for the purpose of "causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages". Very few spam e-mails are sent with any

[56] Equivalent to ten million.

[57] "The Definition of Spam", SpamHaus. Available: http://www.spamhaus.org/consumer/definition/.

[58] "What is Spam", Secure List. Available: http://www.securelist.com/en/threats/spam?chapter-84.

of those as a purpose. Most are sent with the purpose of direct marketing, to defraud people of money, and various other purposes that the law does not address.

The elements of Section 66A(c) are disjunctive, (that is, because they use 'or', any of them is sufficient to constitute an offence) and not conjunctive (using 'and' to ensure that all the elements in the section need to be satisfied). This leaves people who send individual, one to one email that is seen as annoying or inconvenient potentially liable to a heavy fine and a prison term of upto three years. Thus, this provision is undoubtedly unconstitutional.[59]

In fact, the provision has never been used for prosecution of spam, while it has been prolifically used for what can be termed suppression of political and free speech. People recently arrested under this provision include a college professor who received and forwarded an email with a cartoon of a chief minister[60] and two young women who questioned, on their facebook pages, the shutdown of the city of Mumbai after the recent death of a regional politician[61]. Charges filed against the two young women[62] and the professors[63] were subsequently dropped. It is also proving to be popular among campaigners for women's rights as a means of attacking sexist remarks online[64].

All in all, the supposed anti-spam provision in the Indian law does not appear to cover spam, but is overbroad and subject to abuse that goes against the original intent of the provision.

Interestingly, in November 2012, a legislator from Odisha, Baijayant Panda, moved a private member's bill to repeal the extant Section 66A,[65] and replace it with a provision much more narrowly targeted at spam:

> 66A. Any person who sends, by means of a computer resource or a communication device,- a. any unsolicited commercial electronic message; or b. any commercial electronic message where the the identity of the person on whose behalf the communication has been sent has been disguised or concealed, or where a valid address to which the recipient of the communication may send a request that such communications cease has not been provided, shall be liable to a penalty not exceeding one crore rupees.

---

59 For detailed analysis of the provision, see P. Prakash, "Breaking Down Section 66A of the IT Act," at http://cis-india.org/internet-governance/blog/breaking-down-section-66-a-of-the-it-act

60 Aparna Viswanathan, "An unreasonable restriction", The Hindu, February 2013. Available: http://www.thehindu.com/opinionllead/an-unreasonable-restriction/article4432360.ece.

61 Pranesh Prakash, "Aribtrary Arrests for Comment on Bal Thackeray's Death", The Center for Internet & Society, November 2012. Available: http://cis-india.org/internet-governance/blog/bal-thackeray-comment-arbitrary-arrest-295A-66A.

62 "Facebook row: Court closes case against Palghar girls", The Economic Times, February 2013.

63 Orin Basu, "Ambikesh Mahapatra knocks on PMO door", Hindustan Times, May 2013.

64 Richa Kaul Padte, "Section 66A sexual harassment and women's rights", Internet Democracy Project, December 2012. Available: http://internetdemocracy.in/2012/12/section-66a-sexual-harassment-and-womens-rights-2/.

65 Jay Panda, "A Private Member's Bill To Amend 66A", Outlook India, November 2012. Available: http://www.outlookindia.com/article.aspx?283169.

The Telecom Regulatory Authority of India (TRAI) has sought to tackle SMS spam and unsolicited telemarketing through its regulatory powers, rather than using the Information Technology Act.

TRAI has used multiple means to deter SMS spam and unsolicited telemarketing, including mandatory registration for telemarketing and SMS marketing – which includes provisions requiring marketers to respect a nationwide "Do Not Call" list, the Telecom Commercial Communications Customer Preference Portal (NCCP)[66]. TRAI additionally approaches this from a pricing perspective, levying higher termination charges for 'transactional SMSes' to raise the costs of bulk SMS and make it uneconomical to send unsolicited SMS campaigns.

Recent TRAI regulations[67] provide strong disincentives to all players in the unsolicited telemarketing and bulk SMS ecosystem, from telecom operators who structure bulk SMS plans that are heavily abused by marketers, to telemarketers as well as the advertisers who hire them for spam campaigns.

TRAI will, going forward, levy a fine of five thousand rupees per complaint, for successive incidents of spam SMS originating from bulk SMS plans allotted to unregistered telemarkters. In addition, all telephone numbers allocated to both the telemarketer as well as the advertiser that hired the telemarketer are subject to disconnection, in an attempt to target the widespread use of throwaway prepaid phone numbers in telemarketing and SMS campaigns.

TRAI earlier attempted to enforce a blanket limit the number of SMSes that could be sent each day, which was halted by the courts stepping in to disallow such a restriction[68].

While the telecom regulator has, over a period of years, been able to come upon a reasonably functional solution against SMS spam, there still continue to be no useful legislative or regulatory provisions against email spam, and substantial work is required on enforcement against other forms of cybercrime.

Cross border mechanisms for Indian regulators and law enforcement to deal with their foreign counterparts on cybercrime prosecutions are limited.

Though India is not currently a member of the Budapest Convention on Cybercrime[69], India currently has Mutual Legal Assistance Treaties (MLATs) with thirty countries[70]. These are, in general, limited by a requirement for dual criminality (where the request must be on a matter that is a crime under the laws of both the requestor country and the country from which legal assistance is requested).

---

66 Telecom Commercial Communications Customer Preference Por-tal. Available: http://www.nccptrai.gov.in/nccpregistry/.

67 Rajeev Agrawal, "The Telecom Commercial Communications Customer Preference (Thirteenth Amendment) Regulations 2013", TRAI, August 2013. Available: http://www.trai.gov.in/writereaddata/whatsnew/documents/press%20release%200n%20uccfinal.pdf.

68 Anupam Saxena, "Supreme Court Stays Order Removing 200 SMS/Day Limit", MediaNama, December 2012. Available: http://www.medianama.com/2012/12/223-supreme-court-stays-order-removing-200-smsday-limit.

69 "Convention on Cybercrime", Council of Europe. Available: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT-185CL-ENG.

70 Central Bureau of Investigation. Available: http://cbi.nic.in/interoollmlats.php.

However, it is not unknown for information to be requested through an MLAT[71], particularly from US based messaging and social networking providers, in cases where political or other speech that may fall under US First Amendment protections is sought to be prosecuted.

Such requests have been routinely made, and rejected in the past, and more importantly, are a drain on already scarce resources that might be better focused on cross border cybercrime and spam related prosecutions. Clarifying the current lacunae in the Indian IT act (supra) will go a long way towards remedying this situation.

Acknowledgment

Suresh Ramasubramanian thanks his fellow moderators of the India-GII mailing list, Arun Mehta, Vickram Crishna and Udhay Shankar for reviewing and fact checking the section on Internet history in India. He also thanks the staff of CIS India for their reviewing and commenting on the paper, and in particular, Pranesh Prakash of CIS India for consenting to act as a co-author.

[71] "US unable to execute summons to websites including Facebook Google: MHA tells court", The Economic Times, May 2013.