Chapter - 10

Spam Legislation
Introduction

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. Given the severity of the issue and the potential damages spam can cause, legislative measures have been suggested in a number of countries to control and possibly eliminate spam. These legislations have introduced different parameters. However, legislation alone cannot prevent spam. Brazil, Russia, India and China are among the biggest emerging broadband markets worldwide and as such offer a tremendous opportunity for cybercrimes. These emerging markets will be more heavily targeted with spam delivered in local languages. It is to be combined with technological measures. There is no legislation in India controlling spam nor have courts yet found an opportunity to pronounce principles for the same [p-10]. This chapter discusses possible parameters which an anti-spam legislation in India, as and when enacted, may have [p-4]. These parameters have been analyzed in the light of trans-border legislative developments. Further, it provides an account of present legal solutions to the problem of spam in India taking cue from the judicial pronouncements on the subject in other jurisdictions.

10.1. Legislative Measures

Nevada is the first American state to enact legislation in 1997 specifically targeted at spam [10.1]. California, Washington and Virginia followed shortly thereafter. Today, at least 37 American states have statutes that regulate spam. There are around 51 out of 191 UN states presently having anti-spam legislations in place operating on different models of protection to consumers. These legislations prescribe different parameters for regulating spam as is shown in figure 57 below. These conflicting parameters of anti-spam legislations are discussed along with other possible measures which could be incorporated in an anti-spam legislation that may be enacted in near future in India.
10.1.1. Consent of the Recipient

There is no uniformity in laws regarding the manner in which recipient can refuse to accept the receipt's e-mails. Broadly speaking, there are two approaches: an 'opt-in' approach, which requires that the sender has the recipient's permission prior to sending and an 'opt-out' approach, which provides a mechanism for declining the receipt of further e-mails from a particular sender [10.2]. These mechanisms are not free from criticism. It is argued that the spam opt-out registers are unfortunate because they serve mainly as a source of confirmed e-mail addresses for spammers [10.3]. Opting out is not always effective. It may serve purpose, for instance, in direct mail solicitation and outbound telemarketing, at least with respect to each marketer who has given an opt-out choice which the subscriber has availed by submitting a request to that effect [10.4]. The cost involved in a single communication provides marketers with a sufficient incentive to refrain from communication with persons who have submitted opt-out requests [10.5]. As against this, bulk e-mail does not involve any analogous incremental cost that would persuade spammers to respect opt-out requests [10.6]. Sorkin contends that the effort required to remove an address from a spammer’s list is likely to exceed any negligible savings that would result from sending a bulk e-mail message to one fewer address. Furthermore, a
spammer typically must violate several providers’ policies by sending the spam in the first place, so it makes sense that spammers would be less likely than other marketers to be concerned with social or legal consequences of ignoring opt-out requests.

It is quite possible that opt-out requests may at times prove counterproductive and experts for this reason do not recommend it. Their apprehension is based on the fact that opt-out requests are rarely effective but it provides an opportunity to the spammers to collect and sell e-mail addresses of those who have submitted such requests [10.7]. It states that individuals who have submitted opt-out requests may not seem like particularly good prospects for a subsequent solicitation. However, the fact that they have responded to a spam confirms their addresses to be valid, and indicates that they are probably more likely to actually read unsolicited e-mail, that they probably receive less of it than many other users, and that they may be relatively unsophisticated Internet users and, therefore, more susceptible to questionable solicitations. The sender-specific opt-out is also unsuited to e-mail because the number of potential spammers disproportionately exceeds the number of direct marketers using other communication methods [10.8]. The learned author opines that the ephemeral nature of identity on the Internet effectively gives each spammer an unlimited stock of separate identities, some of which may exist only at the point in time that a particular solicitation is being sent, and spammers have little or no incentive to honour opt-out requests. Unsolicited e-mail messages frequently contain statements representing that they are a one-time mailing and promising never to contact the recipient again, often as an justification for not providing opt-out instructions, and the spammer naturally will send its next message out under a different name. For these reasons, even if there were very few separate entities engaged in spamming, contacting a significant proportion of spammers is likely to be much more difficult than contacting a comparable proportion of direct mailers or telemarketers all. The opt-out Policy alone cannot, therefore, prevent spamming.

In an ‘opt-in’ approach the recipient’s consent must have been obtained by the sender before any commercial mail is sent to him. This consent may be obtained in a number of ways.

“Express Consent”: Consent may be express where the recipient on his own fills up a form or responds affirmatively to a query seeking consents.

“Inferred Consent:” Consent may be inferred on the basis of the conduct and the business and
other relationships of persons concerned.

"Deemed consent" Persons are deemed to have given consent to receive messages related to their business or official capacity where, for instance, they published addresses without a statement saying they do not want to receive commercial messages [10.9].

The United States Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 or the Can-Spam Act of 2003 [10.10]. It came into force on January 1, 2004. This law chose, with its above stated attendant limitations, the opt-out method [10.11] and specified that once the recipient sends a request not to receive future messages from the sender, the sender had 10 business days to comply with the receiver's request to opt-out [10.12]. In the final rule, the FTC *inter alia* stated that senders must provide recipients with an easy unburdened way to unsubscribe from a commercial e-mail. Specifically, senders of commercial e-mails must not require any recipient to pay any fee or provide any more information other than an e-mail address, or make the recipient visit more than one single Internet web page in order to unsubscribe from receiving additional commercial e-mails from the sender. This requirement will not allow companies to make inquiries into why the person is unsubscribing, or ask for confirmation whether they really intended to opt-out from receiving commercial e-mails [10.11]. Israel is following the American opt-out model used for telemarketing. An electronic message may be sent to all persons except for those who have clearly stated that they do not wish to receive unsolicited mail (opt-out model) [10.12].

The Australian law chose the opt-in method. Spam must not be sent with an Australian link [10.13] unless the account holder has consented to receive the message [10.14]. The receiver may withdraw consent and the sender has five business days to comply [10.15]. Internet service providers (carriage service) are not liable for violating this section [10.16].

The Australian Spam Act seems to have been the model for the drafters of the New Zealand legislation. In addition to opt-in policy, the New Zealand Act provides that every commercial message must contain a functional unsubscribe facility expressed in a clear and conspicuous manner. Singapore is also following the same opt-in model in its Spam Control Act, 2007 [10.17]. Japan has discontinued its earlier policy of opt-out and has now come up with new anti spam law in which opt-in policy has been adopted with the hope of curtailing its continuing spam
problem [10.18]. Canada has adopted a soft opt-in Approach. The anti-spam provisions prohibit sending (or causing or permitting to be sent) a commercial "electronic message" (which is defined broadly to include a text, sound, voice or image message) to an electronic address, unless the recipient has given express or implied consent [10.19].

The European Union has introduced a hybrid approach to control advertising and, therefore, spamming. Firstly, the opt-in model is introduced pursuant to Article 13(1) of the Directive [10.20] concerning the processing of personal data and the protection of privacy in the electronic communication sector [10.21]. It applies primarily in the context of business to consumer (B2C) communications. In terms of Article 13(1), it is now required that prior consent be obtained from natural persons beforehand for the purposes of direct marketing through automated calling machines (fax). This requirement also covers advertising through short messaging systems (SMS). This commonly referred as a soft opt-in approach allows the maintenance of an opt-out registry system in marketing forms that are more costly for the sender and impose no financial costs on subscribers and users and in pre-existing relationships. The second approach, which is essentially an exception-based opt-out system, applies to B2B relationships. Since Article 13(1) read with Article 13(5) applies to B2C communication because of its explicit reference to natural persons", it stands that an opt-out approach applies by inference in business to business (B2B) communications [10.22].

There can be double opt-in subscription also which requires a subscriber to take two actions to get into a list of e-mail addresses maintained by the sender. They are i) enlisting of e-mail address of the subscriber by submitting a registration form and ii) confirmation of the enlisted address by correctly answering the question asked by the sender. This type of action is also called verified opt-in or closed loop opt-in. Similar to this approach is confirmed opt-in method with a difference that a user is required to do some action or has to answer any confirmation message if he wants to unsubscribe [10.23]. There is, however, no legislation in any jurisdiction which has adopted either double opt-in or confirmed opt-in method. Table 33 lists the type of consent followed by anti-spam legislations of some countries.
Chapter -10: Spam Legislation

Table: Type of Consent followed in various countries

<table>
<thead>
<tr>
<th>Consent</th>
<th>Country/Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt-Out</td>
<td>USA, Israel</td>
</tr>
<tr>
<td>Opt-In</td>
<td>Australia, New Zeeland, Singapore, China</td>
</tr>
<tr>
<td>Hybrid Approach</td>
<td>European Union</td>
</tr>
<tr>
<td>Soft Opt-In</td>
<td>Canada</td>
</tr>
<tr>
<td>Double Opt-In</td>
<td>A Possible Solution</td>
</tr>
<tr>
<td>Confirmed Opt-In</td>
<td>A Possible Solution</td>
</tr>
</tbody>
</table>

Indian legislatures have not paid much attention to the above mentioned transnational developments. The Information Technology Act (IT-ACT) has been recently amended [10.24]. Neither the original nor the Amended Act has provided any provision for controlling spam. However, the Telecom Regulatory Authority of India (TRAI) has established the National Do Not Call Registry (NDNC) with the primary object to curb unsolicited commercial communications on mobile phones. The Unsolicited Commercial Communication Regulations 2007 define UCC as any message through telecommunication service which is transmitted for the purpose of informing about or soliciting or promoting any commercial transaction in relation to goods, investment or services which a subscriber opts not to receive (Opt-out). Exceptions to UCC are messages received under a contract, communications relating to charities and communications transmitted under the directions of sovereignty and integrity of India.

Whether it is an opt-out or opt-in model, spam cannot be regulated when it has been sent offshore or has come from the jurisdiction where opposite model is in vogue. For instance, a sender may be in a country where opt out model is adopted and recipient in a country of opt-in. The sender may not be liable in his country of origin but liable in another country. It is not possible for the sender to know beforehand whether the recipient is in the state where opt-in or opt-out model is followed. The solution lies in having a global policy, be it opt-in or opt-out.
10.1.2. Scope of Legislation

The scope of any legislation in different countries on the subject of spam is bound to vary. The legislation may deal exclusively with the problem of spamming or an express provision may be incorporated in the existing legislation or existing legislations may be read to cover spam. The legislation may come out of the traditional principles and provide solution to the problem of spam or traditional principles may be stretched to enfold the legal issues surrounding spam. The legislation may make spamming a criminal offence [10.25]. This would require different set of standards to determine liability which would also require services of the state machinery. It is also possible to treat spamming a civil wrong only for which compensation will be a remedy which will require different principles to measure damages. The legislation may treat spamming a civil wrong as well as a criminal offence. The spammer may be asked to compensate the loss and also to face criminal prosecution. The spammer as well as any person who aided or abetted spamming may be held liable. Even the trader who is ultimate beneficiary or who is responsible for hiring the services of the spammer can be made liable. The obvious advantage of this liability is that the trader, whose interest is projected in the spam, can be easily identified as against the spammer himself.

10.1.3. Locus Standi

The spam may be received by an individual user or an organization. The scope of the legislation may vary on the question of locus standi. The complainant can be the receiver of the spam or an ISP or a voluntary consumer organization or NGO or competitor or Government [10.26].

10.1.4. Liability of E-mail Service Provider

The role of ESP is very crucial in sending spam. The liability of E-mail Service Provider (ESP) as an organization will depend upon whether its services have been used or not or whether ESP is itself a spammer or it is facilitating spamming. It is quite possible that spam may be sent directly to Mail Transfer Agents (MTAs) of receiving servers without using any sending server. ESP may send spam or facilitate sending of spam by either failing to install required security procedures or by selling e-mail addresses to spammers or in connivance with the spammer. Its liability may
be civil or criminal depending upon the legislation of a country. Its liability may vary according to its role in spamming. ESP may be asked to have annual security audit so that its liability is fixed if its security standards fall below the prescribed standard.

10.1.5. Spammer

The spammer may be a professional or a group of professionals who offer spamming service independently to the traders interested in advertising their goods or services or spammer may be a trader himself who is using spam for marketing his goods or services. The spammer may be a hacker who is using fake website to defraud consumers through phishing or cause crash of a mail server resulting in denial of service. It may include combination of any two services also.

10.1.6. Jurisdiction of Courts

Internet spawned issues pose a common challenge of choice of law, jurisdiction of courts and enforcement of decisions. Internet is essentially global in character and knows no political or geographical boundaries. Most of the e-mail addresses provide no indication of the addressee's physical location, and even an e-mail address that does include a geographic identifier frequently can be used from anywhere in the world. UCE may be sent outside the borders of one country, thereby avoiding any sanctions, that otherwise apply under the law of that country. Currently, more and more UCE are sent outside the borders of a country. The laws pertaining to jurisdiction are not uniform. The issues of personal jurisdiction are resolved differently in Common law and Civil law countries. This issue of jurisdiction becomes more complicated where spam has been sent from a state following opt-in model to a state where opt-out is the legislative policy and vice versa. It is also possible that the sender and recipient may be in one country following 'opt-out' or 'opt-in' model and server may be located in a country which follows opposite of either models.

The jurisdiction of courts within European countries is based on statute or regulation instead of case law as in the U.S. Unlike the American states, each country within the EU has prescribed rules to determine jurisdiction that are significantly different from each other. The French Civil Code, for instance, allows national courts to hear nearly any case where the plaintiff is French. The French defendant is free to insist on being sued in his own country. French courts will not
enforce a judgment against such defendant if he has not voluntarily submitted himself to foreign jurisdiction. The Germany's Law of Civil Procedure allows for jurisdiction over a non-resident defendant based solely on assets located in the forum.

This problem has been addressed by adopting Conventions in order to broaden the protection of their citizens against extraterritorial reach [10.27]. These Conventions include (a) Lugarno Convention (b) Brussels Convention; and (c) Hague Convention.

The Lugarno and the Brussels conventions are European Community conventions, primarily applicable to the EC member states. They are almost identical but the Lugarno Convention extends to EFTA states and other European states, which have ratified the Convention. The fundamental principles of these conventions are that a person who is domiciled in an EU member country may be sued in that country [10.28]. Where a contract has been executed between the parties of two member states, a person may be sued in the place of performance and in case of tort; a person may be sued in the place where the event causing harm has taken place [10.29].

In America, the out of state defendant can be brought within the jurisdiction of forum state only when he has certain minimum contacts within that state such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice [10.30]. Jurisdiction has been classified as general jurisdiction and specific jurisdiction depending upon the defendant’s contact with the forum. The general jurisdiction can be invoked even when the cause of action arises outside the forum state but the defendant has continuous and systematic contacts with the forum state. The specific jurisdiction requires that the dispute must arise out of defendant’s contact with the forum and can be invoked even where defendant had minimum contacts. The rules have been invoked by the courts to decide the disputes involving e-commerce. The American courts have classified websites into three categories (a) passive website (b) active website (c) interactive website [10.31].

Active websites works like a “window shop” for the defendant to do actual business on the Internet [10.32]. The courts have exercised jurisdiction where a defendant was found to be operating an active website on the ground that he purposefully availed the jurisdiction of the forum state as he intentionally reached beyond his own state to engage in business with
residents of the forum state [10.33].

Interactive websites enable users to exchange information with the host computer [10.34]. The exercise of personal jurisdiction depends upon the level of interactivity and the commercial nature of the exchange of information. The courts have failed to lay down any objective criteria with the result there has been no unanimity on the standard to determine the required level of interactivity and commercial nature of the information on the interactive website [10.35].

Passive website makes only information available and do nothing more. This passive website cannot form a ground for the exercise of the jurisdiction in a forum state where it has been accessed unless additional business contacts of the defendant within the forum state related to the issue in question have been shown [10.36].

Before the enactment of the Can-Spam Act, a District Court in Internet Doorway, Inc. v. Parks [10.37] examined jurisdictional issues involved in Spamming. The court observed that e-mail by its nature is purposefully directed at its recipients. In the instant case, one of the defendants, Davis, falsified "from" header of an e-mail to make it appear that the message was being sent by Internet Doorway, an Internet Service Provider, and sent e-mails to persons around the world, including residents of Mississippi, which advertised a pornographic Website. Internet Doorway filed a suit against several defendants, including Davis, invoking Lanham Act and a state law claim of trespass to chattels. Davis contended that the court has no jurisdiction because the alleged injury occurred in Texas, the location from which the e-mail was sent. E-mail over the Internet can be equated to traditional postal mail and phone calls with a difference that the sender does not know where the recipients e-mail is located. The court stated that, by sending an unsolicited commercial e-mail to a forum resident, the defendant had "committed a purposeful act that occurred in Mississippi, just as if she had sent an ordinary letter to a Mississippi resident advertising a particular product or service. The court declined to apply ratio of the cases which have decided jurisdictional matters in cyberspace and articulated a new test that is premised on e-mail contact unless the defendant or its agent sends the message for a pecuniary gain. The court held that the forwarded e-mail amounted to unilateral conduct by the plaintiff and was insufficient to establish personal jurisdiction.

The court, however, found that the defendant cannot take the benefit of fairness and due process
Chapter -10: Spam Legislation

rights as he has to be aware that the e-mail would be received and opened in numerous forums, including Mississippi. Accordingly, the Court found that it would be neither "unfair" nor "unjust" to subject her to personal jurisdiction in Mississippi. She must be taken to know that by sending an e-mail solicitation to the far reaches of the earth for pecuniary gain, the court even in a distant jurisdiction would call her to answer for the ramifications of that solicitation [10.38]. Now the Can-Spam Act has been enacted which has adopted 'opt-out' model.

The courts in India can exercise jurisdiction over a matter on the basis of (a) cause of action or (b) place of business or (c) place of residence. This jurisdiction can be exercised only within the specified territorial limits [10.39]. These rules are not compatible with either opt-in or opt-out model and cannot provide a solution to the spam originating beyond its borders.

10.1.7. Remedy

The possible remedies will depend upon whether spamming is treated as a cyber crime or civil wrong. The remedies will have to balance two constitutionally guaranteed competing rights, i.e. freedom of speech and right to privacy. The officer designated to initiate action against spammer has to work under the shadow of these rights. The possible civil remedies may be an injunction, cease and desist order, account for profit, and compensation for first and subsequent wrongs.

10.2. Possible Present Legal Measures in India

Spam impinges on the privacy of individual Internet users. It creates economic losses as well as time-related losses in terms of the time spent reading and deleting the messages [10.40]. Spam assists cyber-crimes in a variety of ways which includes theft of data, spoofing, spreading of virus [10.41] and poses a threat to consumer confidence in e-commerce. A significant proportion of spam contains fictitious information about the sender, misleading subject lines and extravagant earnings or performance claims about chain letters, pyramid schemes, advertisements for pornographic web sites, 'quack' products and remedies, and illegally pirated software. Spam, which most frequently takes the form of mass mailing advertisements, is a violation of Internet etiquette [10.42]. Spam is either unsolicited bulk mail or unsolicited commercial e-mail. This is a constant irritant to the e-mail user. Should then law of
nuisance be made applicable? Spam facilitates cyber crimes. Should spam itself be declared a crime or should it be dealt with reference to the crime which it assists. Spam violates privacy rights of an individual in cyberspace. If cyberspace is treated as a place in which user has a separate and safe home, should then law of trespass of property be invoked? The violation of privacy of e-mail user by sending him unsolicited bulk commercials brings in constitutionally guaranteed privacy right but then there is an equally protected right to commercial speech [10.43]. The constitution guarantees freedom of speech but this right cannot be stretched to include unwanted communications. The intersection of these rights leads to the conceptual confusion as to whether the right to avoid spam (if there is such a right) is a property right or a human right involving the preservation of human dignity and personal autonomy [10.44].

These issues need to be discussed in detail so as to provide alternative solutions in the backdrop of transnational developments to the problem of spamming in India.

10.2.1. Home Theory

The cyberspace has been equated with a home of an individual which needs protection from unwanted communications. William Mitchell contends that “many of the places in cyberspace are public, like streets and squares; access to them is uncontrolled. Others are private, like mailboxes and houses, and you can enter only if you have the key or can demonstrate that it belongs to you” [10.45]. Similarly Senator Oliver while responding to the Senate of Canada upon the introduction of the first version of his bill, the Spam Control Act said:

“I do not believe Canadians would tolerate pornographic magazine subscriptions or free edible underwear samples turning up in their traditional post each morning. I do not believe they would appreciate seeing their pre-teen daughter’s name on the address box of a coupon book for diet pills and breast enhancements. I do not believe for a second Canadians would allow such damaging messages to enter their homes, yet this is precisely what occurs over the Web. [10.46]”

If cyberspace is equated with one’s home, then the principles of trespass and nuisance as enunciated by the courts under tort law will be applied. This trend has already been set by the courts in other jurisdictions.

The first spam-related lawsuit in America was a small claims case filed by Robert Arkow against
CompuServe in early 1995 [10.47]. Arkow had received unsolicited e-mail advertisements from CompuServe. He argued that the federal law prohibiting unsolicited facsimile advertisements defined “facsimile machine” broadly enough to include computers that send and receive electronic mail. The parties settled out of court and the terms were never disclosed.

There have been relatively few spam-related suits involving individual recipients of spam since Arkow v. CompuServe. Most spam litigation has been brought by ISPs and other destination operators that have received large quantities of spam addressed to their users, or by third parties whose names or resources have been appropriated by spammers. The dearth of individual actions is probably attributable in part to the relatively small damages that would likely be available, together with the difficulty in proving actual damages [10.48]. ISPs are often in a better position than end users to demonstrate substantial damages [10.49]. This is not, however, true with Germany where a good number of claims were successfully filed by e-mail users [10.50].

ISPs have found some legal relief from spam even in those states of America that have no legislation against spam in particular. They have successfully sued spammers under the common law theories of trespass to chattels, misappropriation of name or identity, fraud, misrepresentations or deceptive practices, negligence, and tortious interference with contractual relations [10.51].

The doctrine of "trespass to chattel" has been invoked by several courts. These courts have held that under certain circumstances the transmission of Unsolicited Commercial E-mail through a computer system constitutes the tort of trespass to chattel [10.52]. "Trespass to chattels" is committed when a person uses or intermeddles with another's personal property without authorization [10.53]. It can obviously be applied to unsolicited e-mail messages even if they do not cause any physical damage to the recipient's computer system or prevent the owner from making use of the computer. In CompuServe Inc. v. Cyber Promotions Inc [10.54] a District court found an ISP could claim trespass to chattels where a spammer had sent unsolicited commercial e-mail, even after being advised that certain recipients did not want to receive these messages [10.55]. Trespass to chattels was found “to include the unauthorized use of personal property [10.56]. Compuserve successfully argued that it had been harmed by losing customers who were
upset by the amount of spam they were receiving and that the high volume of unsolicited
commercial e-mail was preventing CompuServe's customers from having full access to the
services they were paying to provide [10.57].

The Common law remedy of trespass against spam was invoked by the Supreme Court of
California's in *Intel Corporation v. Hamidi* [10.58] overruling Court of Appeal and trial court
decisions, where a trespass to chattels action was brought not against a spammer, but against a
labour organizer who sent about 200,000 e-mails to current Intel employees over the course of
two years. The Court stated that no action in trespass to chattels should be available where the
volume of e-mails is not high enough to likely cause damage to a plaintiff's computer system.
The court did not out rightly reject invocation of remedy of trespass but maintained that
trespass provide a means of seeking redress for more intangible damages, like loss of goodwill
or loss of productivity of employees. Consequently, it is contended that trespass to chattels
would not prove an appropriate cause of action to seek redress for invasion of an individual
user's personal space, since these are intangible wrongs [10.59]. Werdegar J, writing for the
majority, finds that the defendant had no tangible presence on Intel's property, since he was
speaking from his own home computer: "He no more invaded Intel's property than does a
protester holding a sign or shouting through a bullhorn outside corporate headquarters, posting
a letter through the mail, or telephoning to complain of a corporate practice." This finding is
not in line with the US Supreme Court's observation in *Rowan v. US Post Office* [10.60]. The US
Supreme Court held that a vendor does not have a constitutional right to send unwanted
material into someone's home, and that a "mailer's right to communicate must stop at the
mailbox of an unreceptive addressee and to hold less would tend to license a form of trespass."

This finding of Hamidi's court raises doubts about the effectiveness of common law of trespass
as a means of blocking spammers. Individual spam will rarely cause any material damage or
impairment to recipient systems unless it carries a virus. The harm caused by spam is more a
result of aggregation. While a single, unwanted message may be a mere annoyance, hundreds or
even thousands of unwanted messages sent to an individual can cripple e-mail as an effective
medium of communication for that user [10.61].

Design and Development of Efficient Techniques for Securing E-mail System from threats:
(M. Tariq Banday) Page 253 of 266
The law of trespass in India has grown on the above lines and could be used for curbing spamming.

The Common law remedy of nuisance is also considered as one of the options to address spam. One of the votaries of such option writes:

"That under the law of nuisance, certain more intangible intrusions onto private space – the playing of loud music next door, say, or the emission of pollutants – are only actionable if the harm they cause the property owner exceeds the benefits associated with the conduct. [...] It would allow us to as whether, in the context of the Internet, the defendant's conduct intrudes on some fundamental right we want to confer on the owner of a web server [10.62].

In *Parker v. C.N. Enterprises & Chris Nowak* [10.63], a spammer had used plaintiff’s domain name as a return address with the result millions of copies of junk mail were “returned” to the plaintiff and her business associates. This resulted into substantial harm, including substantial service disruptions, lost access to communications, lost time, income and business opportunities. The court considered the liability of spammer in nuisance. It is contended that nuisance actions could potentially take into account the plaintiff’s autonomy interests as a factor in the assessment of the intrusion [10.64]. This nuisance based action has a judicial support in America in the context of telephone calling. In *Wiggins v. Moskins Credit Clothing Store* [10.65], it was held that the excessive telephone calling constitutes a nuisance. On this analogy, it is argued that “the inbox can be viewed either as a fixed (or at least, semi-fixed) conduit into real property or an inherent part of residential use itself” [10.66].

The law of nuisance could be another possible option for control of spam in India [10.67]. Nuisance is defined as unlawful interference with a person’s use or enjoyment of land, or some right over, or in connection with it. It is to be borne in mind that principles of law of nuisance have been evolved with reference to tangible property or land. These principles are, however, flexible enough to encompass spam related issues by construing the words “property” and “land” as including mailbox of the user and cyberspace respectively.

Nuisance is of two kinds (a) Public, general or common and (b) Private. A person is guilty of a public nuisance who does any act, or is guilty of an illegal omission which causes any common injury, danger or annoyance, to the public or to the people in general who dwell, or occupy property, in the vicinity, or which must necessarily cause injury, obstruction, danger or
 annoyance to persons who may have occasion to use any public right [10.68]. Public nuisance is an act affecting the public at large, or some considerable portion of it. Public nuisance can only be the subject of one action and it does not create civil cause of actions for any person and is direct and substantial [10.69]. Public nuisance is a crime and can be invoked to control spam when it affects the public at large. It is quite possible that spammer may target a group of persons and thus may cause loss, discomfort or inconvenience to them.

Private nuisance is the using or authorizing the use of one's property or of anything under one's control, so as to injuriously affect an owner or occupier of property by physically injuring his property or affecting its enjoyment by interfering materially with his health, comfort or convenience [10.70].

Private nuisance is of three kinds: (a) nuisance by encroachment on a neighbour's land; (b) nuisance by a direct physical injury to a neighbour's land; and (c) nuisance by interference with a neighbour's quite enjoyment of his land [10.71].

The above mentioned three kinds of private nuisance are comprehensive enough to control spam. Spam can be equated with encroachment on a neighbour's cyber land which can cause loss in many respects; including neighbours quit enjoyment of his cyber land. The term "neighbour" in cyberspace can be construed to include any e-mail user. While liability for injury to person or property may arise in other modes than nuisance, disturbance of comfort is actionable only as a nuisance [10.72]. It is pertained to mention here that courts in India have acknowledged that the forms which a nuisance may take are varied and the reported cases are no more than its illustrations. The categories of interference are never closed [10.73]. Thus there is a scope to make spam actionable as nuisance under law of Torts in India.

10.2.2. Autonomy theory

The autonomy theory makes legal challenges against spam person centric and focuses more on an individual as a human being who is clothed with all the rights which include property as well as autonomy rights. The autonomy rights not only mandate common law actions of trespass and nuisance as discussed above but also an action on violation of fundamental right to privacy. The courts in US have addressed spam through common law actions, and have tilted
the approach in favour of property rights although that need not to be the case [10.74]. The US courts have maintained that e-mail system is essentially the property of ISPs who are entitled to it to the exclusion of others in the same way as they have rights over their other chattels which are their physical facilities.

The Autonomy theory gives more credence to the constitutionally guaranteed right to privacy but this is countered by an equally guaranteed right to free commercial speech.

The Indian Supreme court in Malak Sing v. State of Punjab; [10.75] R. Rajagopal v. State of T.N [10.76]; State of Maharashtra v. Madulkar Narain; [10.77] Mr. X. v. Hospital Z; [10.78] Peoples Union for Civil Liberties v. Union of India; [10.79] Ms X v. Mr. Z; [10.80] Surjit Sing Thindv Kamwaljit Kaur [10.81] and Shard v. Dharmpal [10.82] has in unequivocal terms held that right to privacy is a fundamental right having source in Art. 21 which guarantees right to life but this right, like other fundamental rights, is not an absolute right. Similarly, in Tata Press Ltd v. Mahanagar Telephone Nigam Ltd [10.83] the Supreme Court held that the commercial speech cannot be denied the protection of Art 19 (1) (a) of the Constitution merely because the same are issued by businessman. Modifying its earlier ruling in Hamdard Dawakhana v. Union of India [10.84] the court held that in a democratic economy free flow of commercial information is indispensable. There cannot be honest and economical marketing by the public at large without being educated by the information disseminated through advertisement. Describing the advertisements as the cornerstone of Indian economic system, the court said that low prices for consumers are dependent upon mass production, mass production is dependent upon volume of sales and volume of sales are dependent upon advertising. The reach of this right has been extended to consumers also. The court ruled that Art. 19 (a) also protects the rights of an individual to listen, read and receive the said speech. However, it is to be borne in mind that the right of one individual to speak does not carry with it the right to make others listen. Nor does it include the right to force private parties to facilitate an advertiser’s speech [10.85].

Any anti-spam legislation is likely to be debated on these two constitutional grounds. The courts in America have already taken a lead by declaring anti-spam statutes unconstitutional. For example, state courts in California [10.86] and Washington [10.87] initially held those states’ anti-spam statutes unconstitutional under the Commerce Clause because they place a burden on
interstate commerce. But later on, the California and the U.S. Supreme Courts have rejected these challenges [10.88].

**Summary**

Internet spam e-mails have proved a significant economic burden on users. Its regulation poses both technological as well as legal challenges. Furthermore, these legal and technical responses to spam, working individually, have been ineffective in solving the problem. The technology can reduce the level of spam but cannot eliminate it. The current technology focuses on content rather than the number of spam. Similarly, when it comes to the question of regulating spam the bottom line is what to regulate about spam. The choice between opt-in and opt-out models will depend upon the state’s policy to prefer constitutionally protected the right to privacy to the exclusion of equally protected the right to free commercial speech, thus requiring all commercial e-mails to be expressly solicited (“opt-in” solution). But if the state’s policy is to balance the right to privacy with the right to free commercial speech, then the “opt-out” solution may be the model to be adopted. A more effective solution will require combining together legal, technological and international efforts. The enforcement of law can be made effective by technologically improving the ability of e-mail users to identify message senders but the problem with the legal measures is their territorial reach. Internet being global in character, it cannot be regulated by national legislations. The national legislative efforts have to be integrated with the international cooperation. This cooperation at regional levels is gaining roots. For instance, the FTC has recently reached an agreement with Great Britain and Australia, permitting agencies in the three countries to share information in order to deal more effectively with the problem of spamming. This cooperation has to be stretched further to make it globally acceptable and legally tenable solution. As already stated, there is no anti-spam legislation in India. The courts may invoke Tort law principles to provide remedy for the problem of spam but that is not a lasting solution. The legislature has to come up with the express statutory provisions for regulating spam which may be possible either by appending a separate chapter on spam in the existing Information Technology Act 2000 or a separate legislation, as is on the unsolicited commercial calls, on mobile phones, has to be enacted in the light of the above discussion.
References


[10.8] See Supra note [10.54].


[10.14] Part 2, Section 16 (1), Subsection (1).

[10.15] Schedule 2, Clause 6 (1)(d))

[10.16] Part 2, Section 16, subsection (9) (10).

[10.17] Section 5 provides that an electronic message is unsolicited if the recipient did not (a) request to receive the message, or (b) consent to the receipt of the message


[10.24] The Act was amended in 2008. However, the amendment has not been yet notified in the official Gazette.
[10.26] As in case of Consumer Protection in India. See the Consumer Protection Act, 1986
[10.28] Article 2 of Brussels Convention
[10.29] Id. Article 5
[10.38] Id. 779-780
[10.39] Section 20 of Civil Procedure Code
Chapter -10: Spam Legislation


[10.45] Mitchell 'City of Bits: Space, Place, and the Infobahn' (Cambridge, MA: The MIT Press, 1995) at p23 As against this, Dan Hunter has argued that "thinking of cyberspace as a place has led judges, legislators, and legal scholars to apply physical assumptions about property in this new, abstract space"—assumptions which often limit or delay the ability of law to effectively address affronts to autonomy interests raised by Internet communications. Hunter 'Cyberspace as Place and the Tragedy of the Digital Anticommons' California Law Review, (2003), Vol. 91, No. 2, p. 443.


[10.48] America Online, for example, apparently attributes $0.00078 in equipment costs to each incoming e-mail message by pro rating its overall investment in e-mail hardware, enabling the company to quantify at least part of the costs it sustains when spammers send millions of messages to AOL subscribers. See, e.g., Am. Online, Inc. v. Prime Data Sys. Inc., No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226, at *4, *9 (E.D. Va. Nov. 20, 1998).

[10.49] Supra note [10.54].

Chapter -10: Spam Legislation


[10.53] See Restatement (second) of Torts § 217 (b) (1965)).


[10.55] Id. at 1020-24.

[10.56] Id. at 1020.

[10.57] Id. at 1019, 1022-23.


[10.59] Ibid


[10.63] No. 97-06273 (Tex Dist Ct Travis County, 10 November 1997) at para. 5.


[10.68] Section 268 Indian Penal Code.


Chapter -10: Spam Legislation


[10.75] AIR 1981 SC 760
[10.76] (1994) 6 SCC 632
[10.77] AIR 1991 SC 207
[10.78] AIR 1995 SC 495
[10.79] AIR 1997 SC 568
[10.80] AIR 2003 Delhi 217
[10.81] AIR 2003 P&H 353
[10.82] 2003 AIR SCW 1950
[10.84] AIR 1960 SC 554


Conclusion and Scope for Future Work

Simple Mail Transfer Protocol (SMTP) is the primary and most deployed protocol for e-mail communication which is being continuously improved by inclusion of new commands, security mechanisms, message formats and efficiency procedures. Some SMTP servers do not support all extensions of SMTP as the libraries with which they are implemented are not constantly upgraded to take advantage of improvements in SMTP. Telnet lacks several features and thus for study and development of SMTP extensions it is desired to build a SMTP E-mail utility that besides permitting to issue SMTP commands directly can also perform various other functions required during development and testing phases. These include format conversions, support for cryptography, handling of security certificates, support batch submission of SMTP commands, establishment of TCP and UDP sessions with other servers without need to disconnect the current session and to support various file operations. It would be our endeavor to build such a system in near future.

Unlike most other Internet applications, e-mail addresses are aimed to recipients rather than a specific machine. Gatewaying is used for conversion between TCP/IP based e-mail addressing and others. MIME permits non-ASCII characters including attachments to be sent through purely ASCII e-mail. An e-mail client can gain access to server mailbox without the use of a special protocol using one of several generic methods like by accessing SMTP Server Directly or through File Sharing Access or by Dial-Up Remote Server Access or through Telnet Remote Server Access. These methods are all variations of the online e-mail access model and work by establishing direct access to the server where the mailbox is located. However, with newer and more secure methods of e-mail access direct e-mail access is rarely used nowadays. POP is used for offline access; IMAP can be used for all three types of access. Online access is also possible using WWW which exploits the flexibility of the Hypertext Transfer Protocol
(HTTP) to tunnel e-mail from a mailbox server to the client. Use of conventional direct access methods is quick and easy to read through a mailbox and the same is true of access using POP3 after the mail is downloaded. In contrast, Web based mail services mean each request requires another HTTP request/response cycle.

SMTP servers incorporate one or more security features using several add-on e-mail security protocols to make communication secure and private. These protocols use diverse technological means like encryption, symmetric and asymmetric cryptography and domain validation through IP address verification and digital signatures. Currently Sender Policy Framework (SPF), DomainKey Identified Mail (DKIM) and secure Multipurpose Internet Mail Extensions (S/MIME) are dominant and standardized e-mail security protocols and are implemented on top of the fundamental Simple Mail Transfer Protocol (SMTP) which lacks security features. SPF/SenderID and DKIM are not secure against eavesdropping, do not guarantee message privacy and non-repudiation but is devoid of overheads to the users. Further, they are transparent to users at no additional cost. On the other hand S/MIME can ensure security against eavesdropping, ensures privacy, and integrity of message but is not transparent to users. These features incur additional costs to users.

To improve security of SMTP servers, configuration option should be set and some limit should be set for certain insecure SMTP commands. Due to insufficient awareness of security protocols very less users use them for security and thus there is a need to undertake a major educational campaign to make users aware about e-mail security issues and train them in use of security protocols and procedures.

Most of the commercial and corporate e-mail servers have no policy for dealing with the date-spoofed e-mails and thus accept e-mails which are spoofed or incorrect in date. Some e-mail programs sort their e-mails on send date field while others sort them by receiving date, both having its merits and demerits. Send date is not a classification
criteria for filters installed at most of the e-mail servers and as such date-spoofed e-mails can pass through spam filters. Date spoofing can be detected by sending MTA or transporting MTA or receiving MTA provided some mandatory date policy is applied to them. However, date spoofing can be detected by extensive header analysis to prevent possible forgery.

Spam e-mails are clogging Internet traffic, cause storage problems at receiving servers and serve as a vehicle to a variety of online crimes and abuses. Spam has spread to other Internet services that include wired and wireless telecommunication services like traditional telephone service, short messaging service (SMS) and multimedia messaging services (MMS) on mobile phones. Spammers and phishes obfuscate their e-mail content to circumvent anti-spam procedures. Spam originates from an illegitimate Sender or in some cases from ESPs for financial gains. Spamming with some reasonable assumptions can be grouped in six distinct classes depending on the type of the participating components. Efficiency of anti-spam procedures to combat spam entry into the system greatly depend on their level of operation and a clear insight of various possible modes of spamming. The dynamic structure of spam and the reaction of spammers towards spam filters makes spam filtering an active area for research and thus there exists a wide scope for development of new spam filters and improvements in the existing ones.

E-mail is also misused to send threat and disseminate other objectionable material related to terrorism that include threat of an attack to people or government in order to create panic or disturbance, terrorism propaganda for creation of ideology, resource gathering and fund raising. For law enforcement and intelligence agencies a threat e-mail is a source of investigations regardless of the threat being true or false and thus cannot be treated as spam. Naïve Bayesian filtering showed promising performance in filtering out threat-emails but since accuracy of filter evaluation is highly determined by relevance of training data, thus it is necessary to create a threat e-mail corpus to facilitate...
researchers in designing systems capable of automatically detecting and blocking terrorism threats by misuse of e-mail system.

There is no anti-spam legislation in India. The courts may invoke Tort law principles to provide remedy for the problem of spam but that is not a lasting solution. The legislature has to come up with the express statutory provisions for regulating spam which may be possible either by appending a separate chapter on spam in the existing Information Technology Act 2000 or a separate legislation, as is on the unsolicited commercial calls, on mobile phones, has to be enacted.

The use of CAPTCHA tests is not only limited to web services like online polls, chat rooms, search engines, blogs, password systems, social networking, etc. but is also used in e-mail systems for creation of free or paid e-mail accounts, challenge response type of spam control to verify that the sender is a human and not a bot, etc. Various classes of CAPTCHA tests are image based, text based, audio based, and collaborative Filtering. Security and usability are two parameters that decide its success or failure. Various security issues that need to be addressed while designing a new CAPTCHA test are its security against Image Segmentation, Shape Matching, Random Guessing, and Farming-Out attacks. Besides these, its security control against attacks on its underlying database and efficiency of implementation method also play a vital role in its security. Various usability issues fall under Distortion, Content and Presentation dimensions. A new image-based CAPTCHA technique has been designed by the authors that use small screen area in comparison to that used in other image-based CAPTCHA techniques. The results obtained through user studies and experiments have validated the efficiency of this new proposed CAPTCHA technique in terms of both security and usability aspects.