The Legislative Approach to Regulate Objectionable Internet Content

By

Apar Gupta*

I. Introduction

I.1. Moore's Law, with its eighteen-month increments, seems almost leisurely [according to Intel founder Gordon Moore, the efficiency of microprocessors doubles every eighteen months][1] compared to the cancerous growth of cyber crime.[2] The *genus* of cyber crime contains, publishing pornographic, defamatory, politically motivated and other objectionable content on the Internet. In the absence of legislation, plenary directives measures fail two fold, firstly they prove inadequate to punish cyber criminals an illustration being many a crime is committed in multiple extraditions and foreign states may be reluctant to extradite fugitive offender on a *vapor* law, secondly the arbitrary nature of such regulations stifle growth of commerce and industry. Thus generic directives are an inadequate device to prevent and punish cyber crime.

I.2. There are four broad areas where legislation with respect to regulation of deviant content is necessitated. [3] This chapter in Part II will demonstrate a need to create substantive provisions of law keeping in regard the *sui generis* character of the internet, Part III will propose procedural enactments and/or amendments to exiting statute(s), and finally in Part IV the protection of civil rights is discussed.

II. Substantive Law

II.1. Since the Internet's strength and purpose is facilitation of communication, it be used as well as abused. The inherent incapacity of traditional penal statutes is writ large to regulate the novel and evolving field of cyber crime, this coupled with the traditional approach of territorial jurisdiction[4] makes a cogent argument for a *lex specialis*.

---

* Final Year Candidate, Bachelor in Laws (Hons.), Guru Gobind Indraprastha University, New Delhi.

[1] Gordon Moore, Experts Look Ahead, Electronics Magazine, 27 (1965).

[2] See CERT/CC Statistics 1988-2005, http://www.cert.org/stats/cert_stats.htm, last visited 12th July 2005.

[3] Judge Stein Schjølberg & Amanda M. Hubbard, Harmonizing National Legal Approaches On Cyber Crime, WSIS Thematic Meeting on Cyber Security, 10 (2005).

[4] See Nandan Kamath, Law Relating to Computers Internet & E-Commerce 267 (2004).

Pornographic matter is greatest constituent of cyber crime, statistics revealing it being 35% of all cyber crime reported in 2000.[5] The example of legislative control of pornographic content will be utilized to display the utility of a special statute.

II.2. The publication of pornography, does not involve a single actor on the internet. It is not necessary that, the content creator, the publisher, the web host and the Internet Service Provider are the same person. Though they may be tried as abettors of crime, there will be difficulty in such an interpretation forced upon, a statute not designed for it. Moreover, it may be committed in different jurisdictions or published or hosted on a server in a foreign country.

II.3. The new statute can prescribe, or can incorporate a differentia as to the culpability and the liability of the actor. The new regulatory regime should seek to regulate Internet content hosted within a country and content which, while hosted outside a country, can be accessed within the country. All national Internet Service Providers (ISPs) and Internet Content Hosts (ICHs) will be required to comply with both the new law and any industry codes of conduct or mandatory standards imposed by the State. The test and criteria to be satisfied for the commission of the offence can be incorporate in the text appropriately, as it not a uniform inflexible standard but varying according to different societies and nations.[6] The statute after laying down broad criteria may provide that a detailed list of content deemed to be injurious to public welfare, may be prohibited by publications in the official gazette by the government.

III. Procedural Law

III.1. Adopting procedural laws necessary to establish powers and procedures for the prosecution of criminal conduct against the information technology infrastructure of computer systems and networks is essential for the investigation and prosecution of cybercrime.

III.2. The search and seizure of content should be allowed in tangible objects (Compact Disks and other storage media) as well as intangible objects (such as pure data residing on a website, through compulsorily obtaining its access). It should adopt measures that enable the authorities to order a person on its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium. Or a service provider to submit stored subscriber information relating to such services in that service provider's possession or control. Subscriber information means information on subscribers in the form of computer data, as well as in any other form, including paper records.[7]

---

[5] Http:// www.intergov.org/public_administration/information/latest_web_stats.html., Web Usage Statistics.

[6] See Abbas v. Union of India, AIR 1971 SC 481.

[7] Accord Article. 18, Council of Europe Convention on Cybercrime Articles.

III.3. The admissibility of evidence also is an issue which needs to be addressed. Clear standards will be laid down for the admissibility of electronic records. The UNCITRAL Model Law on Electronic states in Article 9(1) the admissibility and evidentiary weight of data messages and the same can be relied upon.[8] The use of 'Forensic Computing' in this process will aid in the appreciation of evidence.[9]

III.4. A country has to dispense with the traditional territorial principle of jurisdiction, which states that the courts have jurisdiction in relation to the offence committed within a state's national territory.[10] The statute should instead rely upon the 'long arm' interpretation of the territorial principle states that even if an offence not consummated on state territory, though its effects are felt within the same, the court has jurisdiction, becoming ostensibly extra territorial in effect.[11]

IV. Protection of Civil Rights

IV.1. Security and freedom are both important principles for the growth and development of States. Efforts should be made not to impose blanket restriction on content publication, thus an effort against online pornographic material should not target exhibition of body parts at a medical website. One of the great American statesmen and scholars, Benjamin Franklin, once said: "They that give up essential liberty to obtain a little temporary security deserve neither liberty nor safety".

---

[8] Article 9, Model Law on E-Commerce, United Nations Commission on International Trade Law.

[9] Peter Sommer, Downloads, Logs and Captures: Evidence in Cyberspace, 2 J. F. C. 138 (1997).

[10] See North Atlantic Coast Fisheries Case (United States of America v. Great Britain), (1910), RIAA, 11, Pp. 167, 180; Ahlström Osakeyhtiö and Others v. Commission (Op. Darmon, J) (In re Wood Pulp Cartel), CJEC, (1988), Pg. 19.

[11] See Timberlane Lumber Co v. Bank of America, (1976-77), 66 ILR, 270; Mannington Mills Inc v. Congoleum Corpn, (1979), 66 ILR, 487; Domiicus American Bohio v. Gulf and Western Industries Inc, (1979), 66 ILR, 378; Laker Airways Ltd v. Pan American World Airways, (1984), 23 ILM, 748; US v. Bank of Nova Scotia, (1984) 740 F 2d 817; Graco Inc v. Kremlin Inc and SKM, (1984), 23 ILM, 757;Remington Products Inc v. North American Philips Corpn, A.J.I.L., 80 (1986), Pg. 664; Re Grand Jury Investigation of the Shipping Industry, (1960) 31 ILR, 209; Montship Lines v. Federal Maritime Board, (1961) 295 F 2d 147; US v. Anchor Line, (1964), 35 ILR, 103; Armement Deppe SA v. US, (1968) 399 F 2d 794; US v. Aluminum Company of America, (1945) 148 F 2d 416; US v. Timken Roller Bearing Co, (1949) 83 F Suppl 284; US v. General Electric Co, (1953) 115 F Suppl 835; Holophane Co Inc v. US, (1956), 23 ILR, 130; Vanity Fair Mills Inc v. Easton Co, (1953) 115 F Suppl 134; Ramerize & Feraud Chili Co v. Las Palmas Food Co Inc, (1953) 115 F Suppl 276.

V. Conclusion

V.I. On the basis of the above mentioned recommendations it is my opinion that the Government should enact a new act for the control of internet content, which may even contain other species of internet crimes as the existing penal statute(s) are incapable of handling such sophisticated technological crimes. The substantive provisions will be futile until an enactment of a new procedural law, or the amendment of existing ones is carried out with regard for protection of civil rights.