Making Cyber Law Effective

Dwarkanath B. Prabhu*

Abstract

Purpose : Cyber law and its enforcement has been talked about for quite some time. Most countries cyber laws are effective to a limited extent. This paper attempts to look at the impediments to effective implementation of cyber law and proposes ideas to overcome those.

Design Methodology/Approach : This is a conceptual study based on literature review, case studies and learning from those cases.

Findings : The two major impediments found for effective implementation of cyberlaw are the borderless nature of the internet and the digital divide between the countries. By and large the nature of crime remains the same in the cyber world and the physical world, however due to the borderless nature, it is critical to have a common understanding about jurisdiction. Secondly, the digital divide can act as a breeding ground for cyber crime.

Research limitations / implications :
The study is based on existing literature, therefore may not consider all aspects of cyber law. However it does provide a decent understanding into the complexity of the issue and makes a few suggestions for effective implementation of cyber law.

Originality / Value : The paper suggests some ideas of practical value that may be used by global agencies. Not much work seems to be visible in this space.

Keywords : Cyber law, implementation of cyber law, impediments to cyber law, digital divide and cyber law,

Paper Type : Conceptual study

Introduction

With the advent of internet, the idea of marked territory and exchanges across boundaries has undergone a major change. The Internet is one and therefore there is no sovereignty from the cyber perspective (Rahman et al., 2009). Since it is a worldwide phenomenon, a common set of rules to ensure law and order in the cyberspace is required.

Sovereign law of every country has evolved to suit the best interests of the original inhabitants of the land, to confirm with local traditions and norms, and to suit societal structures. Each country's laws, therefore, differ widely. The USA is a classic example where laws change from State to State. Secondly, what may be an acceptable behaviour in one society may be perhaps a taboo in another. For example, abortion is illegal in some countries. In some other countries it is legal. In USA, in some states it is legal and some states it is not.

The 'world beyond international boundaries' is categorized in three spaces : Antarctica, High Seas and the Outer Space (Rahman et al., 2009). There are clearly established guidelines of international commercial contracts and clearly identified judiciary institutions that are responsible for

* prabhu.db@gmail.com, dwarkanath.p10@iimb.ernet.in, Affiliations IIM Bangalore (PGPPM)

settling such cases. Same institutions may be able to settle the above mentioned case as well. However, simply due to the nature of the transactions and the non identifiable, non physical characteristic of cyberspace where it takes place, implementing existing laws becomes slightly difficult.

Consider a transaction in which a buyer from country A contracts to buy a painting from a painter from country B on an auction site promoted by an entrepreneur from country C. Assume for simplicity that the auction site has its banker in the same country C. Let us say the payment is held in escrow account of the bank in country C. On confirmation from the bank, the entrepreneur confirms the buyer's payments to the painter. The painter ships the painting and the buyer confirms the receipt of the same in good condition. The payment is now released to the bank of the painter in country B. Later, the buyer discovers that the painting is on bad quality canvass and uses bad quality colour that fades. Assume that the buyer has sufficient protection through the contractual obligations mentioned on the auction site. However, now if he complains on the auction site, the painter may no more be there on the site. His address, bank account details may have been of temporary nature and the painter is untraceable. Which country's laws should be applied in such case? Who is the judicial authority to intermediate?

In yet another example, in course of a web based transaction, if the credit card details are hacked and the buyer is defrauded on some other web site, who is to be held responsible? The buyer himself for not having enough protection, the original website since its data was not well protected, or the website on which the defrauding actually took place? The hacker may have broken through the buyer's deterrent technology. It is also likely that the hacking took place at the e-shopping website or it may have happened during transit of data between the e-shopping web site and the payment gateway. At what point was the data hacked may be traced through advanced software forensics. However whether the point of hacking fell within the area of responsibility of any of the entities may be debatable.

The major issue, however, is in non-commercial transactions. It's plausible that a resident of country A passes a 'harmless' remark about a resident of country B where it is a derogatory offense. In such case, what should be the recourse available to the victim? Such and other cases that were unheard of earlier are now on the rise. It is therefore necessary to have another set of laws and institutions or extensions of the existing ones to make this fourth boundaryless (Rahman et al., 2009) space, the cyber space, free of misdeeds and mishaps.

Cyber Law in India

The Information Technology Act 2000 and the subsequent amendment in 2008 govern Indian laws regarding cyber space.

The key provisions under the ITA 2000 primarily address legal validity of electronic information[1], non tampering of information, electronic record keeping of transactions, protection against hacking, setting up of a Cyber Appellate Tribunal[2] and a few other provisions. The ITA 2000 considered 'providing electronic commerce a legal framework' as its prime objective and all its provisions were towards making e-commerce

safe and secure. In 2008 there were major modifications to include undesirable cyber behaviour such as cyber bullying, voyeurism, cyber porn, cyber stalking etc in the list of offenses (ITA, 2000; ITA, 2008). Notably in the 2000 version, Mobile phones, PDAs etc were not covered (Though such gadgets were in use, they were not rampant). In the 2008 amendment activities and transactions through PDAs, smart phones, mobile phones etc have all been brought under the IT act. Cyber cafes were made responsible for a certain code of conduct and a set of regulations was rolled out for them. The responsibility of the centre to act as a certification generation authority was diluted and private companies were encouraged to provide digital certificates. Another major change was that the adjudicator's powers were limited to claims upto 5 crores and power for claims beyond 5 crores were vested with the civil court. Perhaps the most important change of all was that the Cyber Appellate Tribunal was made a multi member entity where non Judicial members can be a part of the tribunal. Though this was provided to make room for more technical understanding, in reality how it works out on the grounds of fairness is yet to be tested. Section 66 was almost rewritten to accommodate changes that cast the net of offensive crimes wider than earlier and activities such as identity theft, sending offensive messages etc. were brought under the category of offenses.

Though ITA 2008 covers much ground, a lot remains to be done. Of the major internet user countries, India continues to be one among those having weakest cyber laws. Indian cyber law does not cover a few things. It does not say anything about the rights and liabilities of domain name holders. Since many companies use internet actively, and internet domain names are becoming synonymous with their identities, there needs a system and procedure for allocating domain names on the lines of the ROC. Domain name squatters are not yet under the purview of cyber crime. (Whether domain squatting is a crime is a matter of separate debate.) Secondly, ITA (2008) has only a fleeting mention of copyrights, but does not say anything concrete about Intellectual Property Rights. Thirdly there is no explicit regulation about the payment gateways. Currently payment gateways are mostly set up by banks and governed by laws pertaining to banks. Fourthly, the act talks about rights of the police (ranking DSP and above) to arrest anyone without warrant in regards to cyber crime irrespective of the person's seriousness, intent, plausibility etc. Can this be regarded as in line with the constitution is a question. Lastly, ITA 2000 as well as 2008 says that these laws are applicable in India and anywhere else in the world[3]. How the legal institution will enforce this clause is not known. By any standards, it is a widely open statement on the fringe of being vague and toothless.

State of International Cyber law and Institutions

The UN through its many bodies, is trying to create institutions and procedures for mitigating cyber crime through a global consensus. Though many nations individually have cyber laws since many years, official coordinated efforts in the arena of International Cyber laws were initiated by the United Nations in 2001 by calling upon all member countries to get together against cybercrime[4].

Worldwide the USA perhaps has the most comprehensive cyber laws in place. The Computer Crime and Intellectual Property Section of the United States Department of Justice plays a key role in execution of justice in cases related to Cybercrime. The US laws pertaining to cyber crime cover intellectual property comprehensively. However, given the nature of the USA legal structure, each State has its own separate laws.

The Cyber laws in UK seem to have evolved after the Shetland Times v/s Wills case (1996) (Edward, 2004). The major act was the UK data protection act 1998, followed by several amendments that today constitute UK's cyber laws. By comparison with world standards, UK's cyber laws are comprehensive.

Cyberlaw in Australia seems to be also of quite a matured nature. It revolves around the Cybercrime bill of 2001 and its subsequent amendments. The bill by itself, very similar to ITA 2000 was more focussed on enablement of the business environment to transact in a rule based fashion.

In the UAE, cyber laws are governed by the Telecom Regulatory Authority and the laws have been established by decree no 3 of 2003 – Telecom Law. It revolves around creating a fair environment for growth of e-commerce.

Interestingly, though most countries now have cyber laws in some manner or the other, none of them are explicit about border issues. Most laws simply say that their law is valid beyond their territorial boundaries. This looks like a harmless statement since there is no method of implementing it other than through bilateral or multilateral cooperation on a specific case. Especially as the internet and its applications continue to grow constantly, the laws also need to keep pace with the changes. For example the phenomenon of social networking sites on the web is a roaring fire.

Apart from the boundary-less nature of the cyber space, there is a great difference between the capabilities, reach and maturity levels of countries due to the digital divide (Broadhurst, 2006). This is one of the greatest impediments for uniformity of cyberlaws, their applicability and execution (Edwards, 2004; Broadhurst, 2006; Rahman, 2009,). Coupled with WTO's prescriptive conventions such as TRIPS (Trade Related Intellectual Property Rights) that further allow the digitally advanced countries to charge a premium on their innovations and go to the extent of patenting their e-commerce methods,[5] the digital divide only makes it even more difficult to implement global laws.

In the light of this, various institutions are working jointly and separately to arrive at a common standard. The EU, CoE convention, Europol, European Judicial network, ASEAN, APEC, OECD, Interpol etc., have all come with guidelines, suggestions, recommendations and notifications in order to fight cyber crime jointly. However there is a missing link of a central agency to coordinate all efforts. It may be a good idea for WTO to take it up as a responsibility.

UNCTAD has recently concluded a study on ways to attain cyber law harmonization. This study is the first of its kind where a comparative analysis and review of cyber laws in 11 members of ALADI (Association Latino Americana De Integracion) was done and a series of conclusions were drawn. Similar activities are being done in Asia and Africa by UNCTAD using its Train-for-trade

methodology under the ICT enablement initiatives to overcome the digital divide (UNCTAD, 2009)

Some Landmark Cases and Lessons

The first case of conviction under ITA 2000 in India was Suhas Katti versus Tamilnadu State (2004). This was a case of defamation of a woman on yahoo groups. After the complaint was lodged by the victim, the accused was traced to Mumbai, down to the cyber café from where he had launched the crime. The offender was declared guilty under section 469, 509 of IPC and under section 67 of ITA 2000. This is treated as a landmark case in India because of the quick judgment (7 months) from filing the FIR and the crime was committed in the cyberspace between two States (Naavi, 2004).

Operation "Phish Phry" (2009) is the case of a joint effort of Egyptian and American law enforcement officials where a group based in Egypt collected bank account information through phishing[6] and hacked into the accounts of Bank of America and Wells Fargo. The accused are American citizens who launched the phishing on American banks using ip addresses originating from Egypt. The trial is yet to begin (FBI, 2009)

John Racine agreed to plead guilty to felony charges after admitting his responsibility in hijacking the Al Jazeera website. Racine hijacked the website by defrauding Network Solutions with whom the site was hosted, diverted the traffic to other site and emails to another account controlled by him. The fraud was done by forging signatures and false photo identification of a system administrator of Al Jazeera. Racine, on his own contacted FBI and admitted to the crime. Racine's plea agreement contemplates a sentence of 3 years probation including 1000 hours of community service plus a fine of $1500 and full restitution to the victim (Layden, 2003)[7].

The first two cases are evidences that cyber law is effective when the accused are the citizens of the same country as that of the victim. The third one is a case of surrendering to the law. It may have been interesting to note the happenings if the accused would have been acquitted by a Qatar court.

Yahoo! Inc USA versus LICRA French Union of Jewesh students (Akdeniz, 2001) is an interesting case where Yahoo! displayed some Nazi objects on its auction website. Yahoo! France provided a link to this website through Yahoo.com website. As per the French court ruling, this constituted a violation of Article R645-1 of their penal code and was considered as a 'threat to internal public order'.[8] The Tribunal de Grande Instance de Paris ordered Yahoo! to block any access to this display for any French citizens. Yahoo France was also ordered to issue a notice to all internet surfers before they hit the site about risks involved in viewing such sites. Yahoo! Inc argued against the ruling citing incompetence and lack of jurisdiction of a Paris court. It also argued based on the internet being a 'space of liberty'. Further=more, Yahoo! Inc declared that it was technologically non feasible to adhere to the Court's ruling of filtering out French internet surfers from the specific page. This was proven false by a panel of experts appointed by the French Court (Yahoo! Inc was already using such technology for targeted advertising and web traffic tracking).

The French court rejected the plea of incompetence and ordered Yahoo! to comply

with its judgment within 3 months failing which they were to pay a penalty of 100,000 Francs per day. Yahoo! Inc in response approached the US district court, San Jose with an argument that the French ruling was in violation of the First Amendment and that French court cannot have any jurisdiction over a US business. The San Jose Court later gave a verdict that the French court order and fine are not enforceable against Yahoo! Inc in the United States. The case was rested when Yahoo! Inc voluntarily stopped the auction and announced a business strategy that they would not auction 'hate material'.

These and many such cases have been reported worldwide. Most of them have been pending for long due to the ambiguous nature, lack of conclusive evidence and many times other issues such as technical incompetence of the courts, issues of sovereignty, territorial issues etc.

Conclusions : The road ahead

Cyberlaws need to evolve beyond their current state. Most laws are currently based on their traditional territorial orientations. (Edwards, 2004; Rahman et al., 2009) While the nature of crime in the cyberspace remains more or less same as that in physical space, its treatment needs to differ. Because one can now commit a crime (knowingly or unknowingly) sitting in a location where common law cannot touch, the law needs to be modified.

The key issue here is largely political and cultural in nature. No country will want to allow the other to exercise powers of jurisdiction within its boundaries. Considering that the most important feature of the law is its enforceability, any attempts for global cyber laws have serious impediments. Even in the physical world, extradition of accused is a highly volatile affair subject to high level political drama. Currently the extradition treaties between nations address this issue. Usually, however, in extradition the actions have to be of criminal nature as per both countries.[9] Political high handedness, economic clout, military strengths etc are a potential source of major impediments in this process (Rahman, et al. 2009).

Apart from serious crimes of economic or political significance, the emergent phenomenon of social networking sites is another angle. Doing things that otherwise one would not do in the physical world is much easier in the cyberspace. However the good news is that given the communities that exist, most of them being of similar interests, identification of potentially dangerous or incriminatory activities can be nailed down. From the politico-legal perspective, though it may be difficult to impose standards and norms on netizens, some sort of good governance may be established through self control mechanisms. Categories of cyber crime such as cyber bullying, cyber stalking, defamation, voyeurism, pornography, phishing, denial of service attacks, defacing of websites, using worms, trojans and spiders[10] etc. can be easily identified and standard norms of punishment for the guilty irrespective of the political boundaries of sovereignty may be agreed upon.

From the ecommerce perspective organizations such as UNCITRAL, UNCTAD, OECD, WTO and WIPO need to work out a widely acceptable framework of conducting transactions on the web. The intellectual property rights need to ensure that they do not increase the digital divide. Just because a country is not in a position to deploy

the best practices of ecommerce due to IPRs, such cyber criminals may be able to take advantage of substandard transaction models and get away (Broadhurst, 2006).

Finally if an effective global tribunal can be established specifically for treating cross border cyber crime, it may provide a good foundation for evolution of cyber laws. Especially when the cyberspace is buzzing with excitement around things such as cloud computing, Genome, etc, there must be strong institutional support and clear guiding principles defined by international cyber laws.

References

Ajala, E. (2007), 'Cybercafes, Cybercrime detection and prevention', Library Hi Tech

News, Number 72007, pp. 26-29, Emerald Group Publishing

Akdeniz, Y. (2001), 'Case analysis of LICRA, French Union of Jewish Students v/s

Yahoo! Inc', USA interim court order November 20, 2000, Electronic Business Law Reports, Vol 1, issue 3, pp 110-120

Broadhurst, R(2006), 'Developments in global law enforcement of cyber crime',

Policing : An International Journal of Police Strategies & Management Vol. 29 No.3, pp.408-433

Burnett, R (2008), Summary of talk given in Mauritius, Oct 2008, British Computer Society, Archives of Government of Mauritius.

Edwards, L., (2004), 'Changing the shape of cyber law', Scripted, Vol 1, No 3, editorial.

FBI, (2009), 'Operation Phish Phry : Major cyber fraud takedown', FBI stories,

October, 2009 available at http://www.fbi.gov/news/stories/2009/october/phishphry_100709, last accessed 21 April, 2011

Kaplan, C.(2001), 'Was the French ruling on Yahoo! such a victory after all', The New York Times, November 16,2001

Layden, J. (2003), 'Al Jazeera Hacker gets community service', The Register, available at

http://www.theregister.co.uk/2003/11/14/al_jazeera_hacker_gets_community/, last accessed 21 April, 2011

Naavi, (2004), 'Chennai Cyber Crime Cell gets its first case in record time', available at http://www.naavi.org/cl_editorial_04/suhas_katti_case.htm (last accessed 21 April, 2011)

Rahman, M., Khan, M., Mohammed, N., Rahman, M.,(2009), 'Cyberspace claiming new dynamism in the jurisprudential philosophy', International Journal of Law and Management, Vol. 51 No.5, pp. 274-290,

ITA, (2000), The Information Technology Act , 2000 : Government of India, Ministry of Law, Justice and Company affairs, Legislative Department, The Gazette of India, June 9, 2000.

The Information Technology (Amendment) Act, 2008 : Government of India,

Ministry of Law, Justice and Company affairs, Legislative Department, The Gazette of India Feb 5, 2009.

Notification under IT (Amendment) Act 2008 : Government of India, Ministry of

Law, Justice and Company affairs, Legislative Department, The Gazette of India, November 27, 2009

UNCTAD (2009), Information note from UNCTAD. UNCTAD/PRESS/IN/2009/015, 12/06/09

(Endnotes)

(1) Till the IT act 2000, though the country had been using internet and e-commerce right from 1996-97, electronic documents were not considered valid in the court of law.

(2) Cyber Appellate Tribunal was established under the IT Act under the Aegis of Controller of Certifying Authorities (CCA). It has the same powers as are vested in a civil court under the Code of

Civil Procedure, 1908. However, is not bound by the procedure laid down by the Code of Civil Procedure, 1908 but is guided by the principles of natural justice. The Cyber Appellate Tribunal has powers to regulate its own procedure including the place at which it has its sittings. Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

Source : Ministry of information technology website.
http://mit.gov.in/content/cat

(3) "It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person." – ITA 2008, section 1(2), Ch 1.

(4) UN general assembly, resolution 55/63, adopted on 22nd Jan 2001.

(5) "the thrust of global e-commerce law apparently supported by the WTO Trade Related Intellectual Property (TRIPS) Agreement promotes restrictive practices by permitting patenting of ebusiness methods"

– Source Legal Regulation and Uneven Global Digital Diffusion, Abdul Paliwala, University of Warwick, Warwick.

(6) Phishing refers to a type of Internet attack where the hacker originates email from the identity of another entity and gets back information to his own email. This is similar to impersonation in the physical world.

(7) US Department of Justice, Release no 03-089

(8) Collecting, buying, selling, displaying, soliciting objects resembling or connecting with the Nazis is an offence under French Law.

(9) This is the double criminality rule.

(10) Worms, Trojans and Spiders are all types of software written with malicious intent.

Albert Einstein's wife often suggested that he dress more professionally,
when he headed off to work.
"Why should I?" he would invariably argue.
Everyone knows me there."
When the time came for Einstein to attend his first major conference,
she begged him to dress up a bit.
"Why should I?" said Einstein.
"No one knows me there"

Guidelines for Research Paper contributors

With the intention of providing a forum for research scholars and academicians to disseminate knowledge across all aspects of Ethics in profession, management and public governance, we invited contributions of Research Papers. We have received a number of contributions. Our Referees observed that the contributors have not followed the methodology for standard Research Papers. Standards of approach, content and expositions being universal we do not specify any guidelines.

Some specific guidelines (as per references) needed for processing the manuscripts outside the intellectual part, are appended below:

1. The paper should bring out objectives of the Research and Development, Methodology of Research carried out (Is it based on survey, Is it based on Case Study, Is it based on Experiment). The paper should give details of Survey, Case Study, and Experiment as applicable, followed by detailed discussions of results and conclusions.
   - Objective of Research and Development
   - Methodology of Research and Development (Survey, Case Study, Experiment)
   - Result and Discussions
   - Conclusion
2. Length of the manuscript – between 2,500 to 3,000 words (including tables, figures, references).
3. An abstract of around 200 words and author's academic profile with e-mail address in about 60 words, should accompany the paper.
4. Tables and figures should be appropriately created and given at the end of the paper. Where ever such tables are relevant, it should be marked ("see table No…") at that place.
5. Two hard copies of the manuscript should be submitted, with a soft copy sent either as an e-mail attachment or on a floppy formatted in MS Word, Times New Roman font, size 12pt., 30 mm margins on sides and 18 pt. space between the lines should be given.
6. References should be given only at the end of the manuscript. References must be complete in all respect and alphabetically arranged.
7. Authors should give undertaking that the Paper has neither been published nor has been submitted for publication elsewhere. It is the author's responsibility to seek permission to reprint quotations or use tables, figures and graphs earlier published with copyright restrictions.
8. Manuscripts not considered for publication will not be sent back.
9. All contributors to this Journal will receive a complimentary copy of the issue along with an exclusive reprint of their paper.
10. Manuscripts and all editorial correspondence should be made to the Managing Editor, Asian Journal of Professional Ethics & Management, Aeronautical Society Bldg. (First Floor), Suranjandas Road, Off.: Old Madras Road, Bangalore 560 075. Our telephone numbers (09243114261) may be written on the top of the envelope containing the hard copy. Soft copy to be sent to our e-mail address: ethics.asia@gmail.com

– Editor