Journal of Banking and Insurance Law

Volume No. 12

Issue No. 1

January - April 2024

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

Journal of Banking and Insurance Law

Aims and Scope

Journal of Banking & Insurance Law (JBIL) is a peer-reviewed bi-annual journal for Banking and Insurance Laws. JBIL aims to promoting the research which is not only academic in nature but can also pave a way for relevant law reforms in future. Law and policy makers are under constant pressure to guard the interest of consumers taking up banking and insurance services. JBIL aims to review the banking and financial regulations, and corporate governance practices of emerging market nations.

Journal of Banking and Insurance Law

Journal of Banking and Insurance Law

(Volume No. 12, Issue No. 1, January - April 2024)

Contents

Cyber Space: Crimes and Laws Against

Mithilesh Kumar Jha
[1]*Assistant Librarian, Judges Library,*
High Court of Jharkhand, Ranchi.
Email: Mithileshjha009@gmail.com, Phones 8935990506, 7070458342

ABSTRACT

The changing environment demands more affirmative protective laws to guard or protect new challenging space of crime i.e. Cyber Crime like; Unauthorized Access, Cyber Fraud, Cyber Hacking, Flowing Viruses, Cyber Terrorism etc. Computer crime, Cyber crime, e- crime, or hi- tech crime generally refers to unlawful act wherein the person uses computer or network as tool, target or both. Since virtual world has no boundaries, the jurisdiction issue is very important to adjudicate a dispute. It is the time when world is not run by weapons, energy or money any more, it is run by ones, zeros and information…it is all electronic. In this paper not only literature review is being done but also some practical cases, Statistical data and news highlight related to cyber crime during 2012, 2013 and 2014 are exhaustively reviewed and applied. We will also discuss IT Act, 2000 and find out the answer of the question "is this IT Act enough against such a cyber terrorists?" here we will also point out some jurisdiction issues in this paper. During discussing on cyber crime we will also focus on the present challenges related to Intellectual Property Right and Copy Right in this Virtual Space.

Keywords: Cyberspace, Cybercrime, Information Technology, IT Act, IPR

1. INTRODUCTION

Cyber crime is an evil having its origin in the growing dependence on computers in modern life. When there are no boundaries of either of wall or person between one to one, one to many and many to many for the sharing of information, and the media of information traveling through is not physical generally refers to virtual world. Now the time come when we are addicted to the virtual world in each and every step of our life. Virtual world means "images, sounds and text used by a computer to create a world where people can communicate with each other, play games and pretend to live another life"[1] The age of the internet has revolutionized the world; the method we communicate, do business, store information,

or run machines is totally dependent on single click of mouse. The internet is nothing but largely a network of computers spread all across the world and connected to one to others through hardware, software, satellite and cables. The days demand everyone to be cyber men. There are numerous private or government agencies that keep our precious data in electronic form. In the race of making money or leaving wealthy & luxurious life people are ready to push or harm others in any step. The mentality of this generation not hesitates to perform any bad and unethical activity to gain false fame. The number is too large to count who do such activities professionally. It is said that "your area of right of freedom ends, from my nose is starts" the same applies in the field of computer performing activity with the help of internet or without, and when this is not being applied and the activity harms others known as cyber crime. Crime is a general word which always means in negative sense either it is performed physically or virtually doesn't matter. Cyber cafes have emerged as hot spots for cyber crimes. Even terrorists prefer the anonymity of a cyber cafe to communicate with each other. These days e-crime increasing very fast way and the reason behind is limitation of defined Acts and the adjudication. One foreigner performs cyber activity in India to harm another country or countries, the question is who will take action and according to which country the performer may be punished? One well known example here "attacks on Parliament by Pakistani in the year 2010 are the result of high-tech crime" by making false gate pass. During this work, it was observed that an attempt to combine all these aspects on one paper is the requirement of the time. This work attempts to gather the basic information about the cybercrime in one paper for better understanding of this area. The main purpose of this paper is to analyze the infield definitions of cyber crime and to determine characteristics of cybercrime to understand in a better way. During the compilation of this paper the IT Act 2000 is also being discussed and tries to find out the competency of the same according to the time. We have put some exciting and statistical news which makes the topic more interesting and statistically strong. After that, this work will help to know about the origin, history and development of the cybercrime.

Definitions

Before going onwards, it is necessary to be quite clear about some important terms by defining and elaborating the same in own words;

Cyberspace: A common mental geography, built, in turn, by consensus and revolution, canon and experiment; a territory swarming with data and lies, with mind stuff and memories of nature, with a million voices and two million eyes in a silent, invisible concert of enquiry, deal making, dream sharing, and simple beholding.2 "cyberspace, amorphous, supposedly "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's

infrastructure. As opposed to the Internet itself, however, cyberspace is the place produced by these links. It exists, in the perspective of some, apart from any particular nation-state. The term CYBERSPACE was first used by the American-Canadian author William Gibson in 1982 in a story published in OMNI magazine and then in his book Neuromancer".3

Crime: An act that the law makes punishable; the breach of a legal duty treated as the subject matter of a criminal proceeding.[4]

Cyber Crime: "A crime evolving the use of a computer, such as sabotaging or stealing electronically stored data" [5] Oxford Advanced Learner's Dictionary, defines Cyber Crime as "crime that is committed using the Internet, for example by stealing sb's personal or bank details or infecting their computer with a virus".

Law: the whole system of rules that everyone in a country or society must obey.[6]

Cybercrime & Cyber Laws

Undeterred by the prospect of arrest or prospect, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security.[7] Cyber crimes such as online banking frauds, source code thefts, virus attacks, phishing attacks, email and website hacking, etc. have become common place. It is for these reasons that 'cyber law', that is, the legal aspects of the cyber world has become important. The cyber law of India is mostly found in the Information Technology Act of 2000. "A crime is an act or default which prejudices the interests of the community and is forbidden by law under pain of punishment. It is an offence against the State, as contrasted with loot or a civil wrong, which is a violation of a right of an individual and which does not lead to punishment.[8] To understand the meaning and concept behind Cybercrime we will go in detail in step by step.

Nature of Crime

Crime never results in positive aspect in any sense. When we only pronounce the word crime our mind hit simultaneously to understand that something went wrong. The origin of word crime is "Crimean" which means 'charge' or 'offence'. The Waverly Encyclopedia defines it as, "An act forbidden by law and for performing which the perpetrator is liable to punishment". The concise Encyclopedia of crime and criminals, has defined 'crime' thus:

Crime as Public Wrong

According to Blackstone crime is a public wrong. He defines crime in two ways (1) Crime is an act committed or omitted in violation of a public law forbidding or commanding it. This definition we cannot accept in its entirety because Constitutional Law, Administration Law, etc. are Public Law Violations of which are not crimes. (2) He modifies his definition and says that a crime is a violation of the public rights duties due to the whole community, considered as a community. Stephen modified Blackstone's definition and defines as such: a crime is a violation of a right, considered in reference to the evil tendency of such violation- as regards the community at large.[9]

Crime as Social Wrong

Crime is a social wrong as defined by John Gillin. He says crime is an act that has been shown to be actually harmful to society, or that is believed to be socially harmful by a group of people that has the power to enforce its beliefs, and that places such act under the ban of positive penalties.[10]

Crime as Legal Wrong

Crime is human behavior which are prohibited by law and defined in Criminal Law. Therefore, when criminal law defines any act of human being as prohibited conduct then it is to be treated as crime but not all the activities of human being. Section 40 of the Indian Penal Code defines offence which is not definition rather explanation of crime. This section runs thus: “except in the chapters and sections mentioned in clauses two and three of this section, the word “Offence” denotes a thing made punishable by this code. In chapter IV, chapter V-A and in the following sections, namely ss. 64-67, 71, 109, 110, 112, 114, 115, 116, 117, 187, 194, 195, 203, 211, 213, 214, 221, 222, 223-225, 327-331, 347, 348, 388, 389 and 445, the word 'offence' denotes a thing punishable under this code or under any special or local law as hereinafter defined. And in ss. 141, 176, 177, 201, 202, 212, 216 and 441, the word 'offence' has the same meaning when the thing punishable under the special or local law is punishable under such a law imprisonment for a term of six months or upwards, whether with or without fine.[11]

Elements of Hi-tech Crime

For the prosecution to obtain a conviction, they must prove the existence of all elements of a crime to the requisite criminal standard of proof, being beyond a reasonable doubt, and for that e there are two main elements, namely:

- Actus reus: refers to the actions (or in rare cases the failure to act/the omission) of the accused; that is that the accused actually did the act
- Mens rea: refers to the mental state of the accused; i.e. that the accused intended the actions.

The general principle of the criminal law says no one is to be punished unless it is proved beyond reasonable doubt by the prosecution that one's conduct is prohibited and liable for the same and also that one had a defined state of mind in relation to the crime commission. Dasgupta shows a mathematical equation to understand the same is;

Actuas reus + Mens rea = Crime
Actus reus + No Mens rea = No Crime
No Actus reus + Mens rea = No Crime

This is the general principle that crime consists of two essential elements. There are five essential requirements for imposing criminal liability. These are: (1) human conduct; (2) circumstances; (3) consequences or result; (4) voluntariness; (5) foreseen or forcibility of result of his conduct in a circumstance which has causation of crime and there must be chain of causation and probable or natural consequences. Fifth one i.e. forcibility represents mens rea and other four requirements represent actus reus. So it is not permissible and unjustified for the State to impose punishment where anyone of the elements is absent; except exceptional cases.[12]

Categories of Cyber Crime

On the basis of affecting person, thing or group we put such crime in three following categories;

Cybercrimes against persons:

- Cyber stalking
- Privacy Issue
- Posting of Obscene Material.
- Harassment with the use of computer.

Cybercrimes against property

- Computer Trespassing
- Computer vandalism
- Divert of funds
- Stealing information & data
- Copy Right

Cybercrimes against government

- Hacking of Government websites
- Cyber Extortion
- Cyber Terrorism
- Computer Viruses

Cyber Law

Understanding anarchy about computer, it become contradictory to frame a law and regulation for Internet. Cyber law deals or governs a system of law and regulation related to e- space or may be called cyberspace. "Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age, taken from kybernetes, Greek word for "steersman" or "governor," it was first used in cybernetics, a word coined by Norbert Wiener and his colleagues. The virtual world of internet is known as cyberspace and the laws governing this area are known as Cyber laws and all the netizens of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet. One definition is not enough to make a person quite clear. One short definition accepted by many is "a generic term that refers to all the legal and regulatory aspects of Internet and the World Wide Web".[13]

Need and Role of Cyber Law

- *Cyberspace is open to participation by all***;** Cyber Laws have an important role in representing and defining the norms of the cyber society.
- *The laws of real world cannot be interpreted in the light of emerging cyberspace to include all aspects relating to different activities in cyberspace***;** Cyber Laws help in giving the right to enter into legally enforceable digital contracts.
- *Internet requires an enabling and supportive legal infrastructure in tune with the times***;** Cyber Laws help in maintaining the Cyber properties.
- *General laws create Confusion*; Cyber Laws help in providing legal reorganization for Electronic documents and Digital signature.

History and Development of Cyber Crime

The first recorded cyber crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened.[14] Professor Susan W. Brenner in his book Cyber Crime20) divided the origin of cybercrime in two phases, first from the era of mainframe computers to 1990, when the internet and personal computers were becoming more sophisticated and more pervasive. And the other phase is from 1990 to present.[15]The same can be divide into two era i.e. before Internet and after Internet era.

Before Internet Era: The first report about the use of computer to commit crime was made public in 1960's when computers were large mainframe computers. After World War II mainframe business computers were developed to recent computers. In 1946, several companies began working on a commercial mainframe, and by 1951, the UNIVAC (UNIVersal automatic computer), created by the company of the same name, and were being used by the census bureau.) In 1956 transistor Computer systems were introduced with a name of second generation computers. Later in 1960's third generation was introduced with multiprocessing and operating systems. After development of computer in 1960, there emerged an issue of computer crime more prominently. But Computer crime in 1960s and 1970s differed from the cybercrime we deal with today. There was no internet, mainframe were not networked to other computers. In 1960, a typical IBM mainframe chose several million dollars, needed as an entire room to house it, and needed a special air-conditioning system to ensure that its vacuum tubes would not overheat and fry the data in the computer.) Only selected researchers were allowed to use a mainframe. Due to limited use and non-connectivity with other computers, the chances were less to commit a computer crime and if so, by selected people only. They must be the employees for these systems. The crime was mostly limited to finance.)[16]

After Internet Era: The other phase was distinguished since the commercialization of the Internet in the mid 1990's, this was the period when internet growth was tremendously fast. This was the time when the Personal computers and Internet were becoming increasingly sophisticated.) In December 1995 there was an estimated 16 million Internet users worldwide, by May 2002, this figure had risen to over 580 million, almost 10 percent of the world's total population.(NUA, 2003). But this was also the fact that this rise is unequal for the worlds, for example, over 95 percent of the worldwide total internet

connections are located in the USA, Canada, Europe, Australia and Japan.) And this was the time when the new type of crime was introduced in the history of crime which sensitized the utilities of the internet. This was continued till the emergence and frequent use of internet. Thus, opening new avenue for criminals. Prominent cyber crimes done in its history through various methods like in 2000, computers users received email with the subject line "I LOVE YOU" and with the attachment entitles LOVE-LETTERFOR- YOU.txt.vbs. On opening of this attachment the computer automatically send this virus to the addresses to the people in address book of the recipient and thus creating trouble for many individuals and corporations.)[17]

Classification of hi-tech Crime and IT Act

Classification of cyber crime is very complex task due to its represent as new spectacle of crime with multi dimensional and ever growing phenomenon. Since we have to focus IT Act 2000 in latter section so hare we will firstly classify the cyber crime according to the same. In IT Act, 2000 cyber crime in 6 types, namely; (*i*) Tampering with computer source documents (*ii*) Hacking (*iii*) Publishing of information, which is obscene in electronic form (*iv*) Child pornography (*v*) Accessing protected system (*vi*) Breach of confidentiality and privacy.

- **Tampering with computer source documents**: Whoever knowingly or intentionally conceals, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.[18]

- **Hacking***:* 'Hacking' is a term with multiple meanings. It can refer to testing and exploring computer systems, highly skilled computer programming or the practice of accessing and altering other people's computers. Intension behind this is to harm a person or a large by getting privet information about them or by changing the working of software in the computer system too. Hacking involves cracking systems and gaining unauthorized access to the data stored in them. A hacker can be a Cyber Punk, Code Hacker or Cracker.

- **Publishing of information, which is obscene in electronic form***:* Hyderabad: Man arrested for mailing obscene pics morphed on boss' wife [19] is the right and recent example.

- **Child pornography**: A photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,

  (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or

  (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years.[20]

- **Accessing protected system***:* The appropriate government may, by notification in the official Gazette, declare any computer resource which directly or indirectly affects the facility of critical Information Infrastructure, to be a protected system.[21]

- **Breach of confidentiality and privacy***:* Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc.[22]

Cyber crimes other than those mentioned under the IT Act

- **Cyber stalking:** Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

- **Cyber squatting:** This crime is being done for the purpose of marketing or making fame through registering a famous domain name and then selling it for a fortune.

- **Data diddling:** Data diddling is the changing of data before or during entry into the computer system. diddling. Examples include forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements.[23]

- **Cyber defamation**: defamation law in law, attacking another's reputation by a false publication (communication to a third party) tending to bring the person into disrepute.[24]

- **Trojan attack:** A Trojan Horse Virus is a common yet difficult to remove computer threat. This is a type of virus that attempts to make the user think that it is a beneficial application.

- **Forgery:** In this people copy documents to cheat others.

- **Phishing and Vishing**: Both phishing and the more recent vishing is obtaining financial information, such as bank account records or credit card details, by sending what look like authentic messages to the recipient informing them they need to comply with certain procedures to reactivate their account. Once the information has been obtained, the criminal then defrauds the victim.[25]

- **Email bombing:** A common proclaim faced by maximum email user; in which E-mail box overloaded with innumerable number of E-mails, to disable to concentrate important message at times.

- **Salami attack:** it is being done by unauthorized access to source code of software application and database to deduct small amounts from an account without coming in to notice, to make big amount.

- **Sabotage of computer:** Another type of hacking involves the hijacking of a government or corporation Web site. Sometimes these crimes have been committed in protest over the incarceration of other hackers. Attack on New York City on 11 Sep. is the example of the same.

- **Cyber-extortion**: where criminal gangs threatened to close down internet-based businesses if protection money was not paid. Worse still, threats can also be made to infiltrate the businesses security system to access financial or personal information stored therein that may then be used for financial gain. [26]

Intellectual Property Right (IPR)

As the www has become a Modern and ever growing virtual platform due to advancement and improvement in technology. Almost every type of business is virtually interconnected via the W3. Modern technology is almost indispensable owing to modern methods of communications. Technology which has made us addicted in the form of to connect to the world for each and every work like email services, mobile commerce, supply chain management, internet marketing, electronic funds transfer, online transaction processing, inventory management systems and automated data collection systems. This in turn has made such businesses vulnerable to various kinds of cyber crimes including misuse of intellectual property and intellectual property rights, identity thefts, and many more. Businesses

establishment, distribution of product, promotional work etc. on www or through w3 became common for this technological era. Due to the ease entry into E-space, people commit mistake to understand that the obligations and restrictions which apply there are similar to those which apply in the world of print communication. Intellectual property (IP) rights are rights awarded by society to individuals or organizations principally over creative works: Inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. They give the creator a right to prevent others from making unauthorized use of their property for a limited period. IP is categorized as Industrial Property (commercial innovations), and Artistic and Literary Property (cultural creations).[27]

IPR Cyberspace

Intellectual property rights apply on the Cyberspace but the question is to make them enforceable. The complains regarding doing impairs of intellectual property interests by fundamentally transforming the nature and means of publications and thus making their works extremely vulnerable to Internet piracy. Authors, Database Creators, Musician, Lyricists, Photographers, Computer Programmers and others copyright holders are being affected by impairs problem in this Internet era. The decentralized nature of Internet's management makes it possible for any user to widely disseminate a work on the electronic network termed as Cyberspace through any number of channels.

IPR and Cyber Law

Continuous, rapid changes and explosive growth in the pervasive computer technologies demands new focus with thorny legal questions and scrutiny in cyber society especially when information technology is used in negative way. Every component of the computer is an instance of the class Cyber world. Hence, all aspects of the laws of the cyber world are applicable to every component created. It is essential to realize that, Legal knowledge of Cyber law, and cyber ethics are the prerequisites for every stake holder irrespective of their positions and roles in IT industry. The next equally important legal issue to be considered in software product and technology companies is IPR. To succeed in the world market companies from India today need brand building skills and protect their IPR.[28]

IPR and CL based system development life cycle

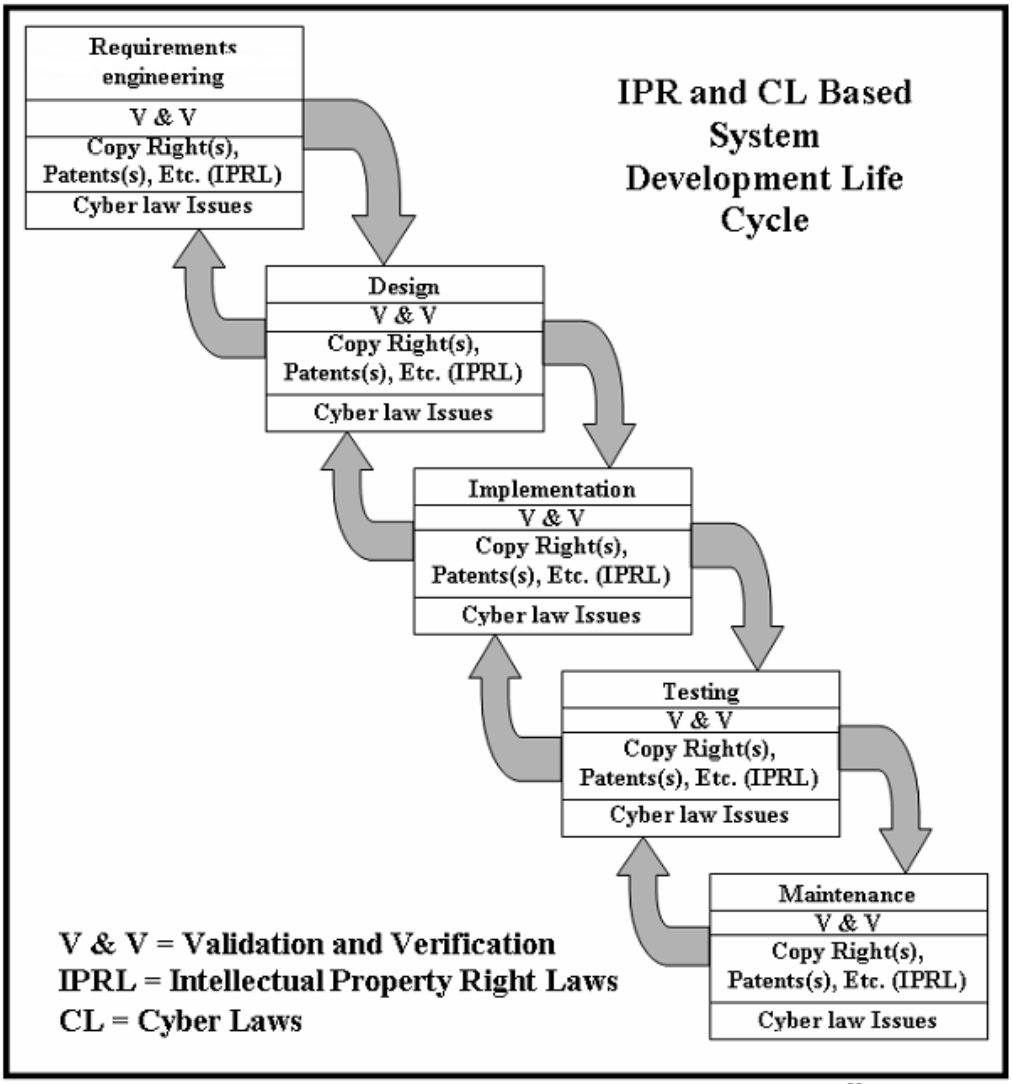


Fig 1. IPR and CL based system development life cycle.[29]

Cyber Law In India (ITA 2000)

When we see the one and only Act available in India i.e. IT Act 2000 which is amended in 2008 term Cyber Crime is not defined. Offence or crime has been dealt with the help under the Indian Penal Code, 1860 and quite a few other legislations too, which elaborately listed various acts and the punishments for each. So we can say that, act done by combination of crime and computer can be categorized under cyber crime. " *An Act to provide legal recognition for transaction carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Panel Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891*

and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto"[30] The Information Technology Act, 2000, which has 13 chapters and 90 sections (the last four sections namely sections 91 to 94 in the ITA 2000 dealt with the amendments to the four Acts namely the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934) was finally passed as the Act No.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000.

The Act essentially deals only four following issues namely;

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

As per the demand of time, some amendment in the same was required and finally the act is being amended in 2008. This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Features of ITAA 2008 are as follows;

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offences.[30]

Section, Offence and Punishment

Here with the help of table, I tried to make aware about the Section, Offence and the punishment against;[31]

Section	Offence	Punishment
43	Damage to Computer, Computer system etc.	Compensation to the tune of Rs.1 crore to the affected person.
44 (a)	For failing to furnish any document, return on report to the Controller or the Certifying Authority.	Penalty not exceeding one lakh and fifty thousand rupees for each such failure.
44 (b)	For failing to file any return or furnish any information or other document within the prescribed time.	Penalty not exceeding five thousand rupees for every day during which such failure continues.
44 (c)	For not maintaining books of account or records.	Penalty not exceeding ten thousand rupees for every day during which the failure continues.
45	Offences for which no penalty is separately provided.	Compensation not exceeding twenty five thousand rupees to the affected person or a penalty not exceeding twenty five thousand rupees.
65	Tampering with computer source documents.	Imprisonment upto three years, or with fine which may extend upto two lakh rupees, or with both.
66	Hacking with computer system with the intent or knowledge to cause wrongful loss.	Imprisonment upto three years, or with fine which may extend upto two lakh rupees, or with both.
66 A	For sending offensive messages through communication service etc.	Imprisonment for a term which may extend to three years and with fine.
66 B	For dishonestly receiving stolen computer resource or communication device.	Imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
66 C	For identity theft	Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
66 D	For cheating by personation by using computer resource.	Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.
66 D	For cheating by personation by using computer resource.	Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.
66 E.	For violation of privacy	Imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
66 F	For cyber terrorism	Imprisonment which may extend to imprisonment for life.
67	Publication of obscene material in an electronic form.	Imprisonment upto 5 years and with fine which may extend to one lakh rupees on first conviction and its double punishment for second and subsequent convictions.
67 A	For publishing or transmitting of material containing sexually explicit act etc. in electronic form.	Imprisonment upto 5 years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

67 B	For publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form.	Imprisonment upto five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of seven years and also with fine which may extend to ten lakh rupees.
67 C	For preserving and retention of information by Intermediaries.	Imprisonment upto three years and also liable to fine.
68	For failing to comply with the directions of the Controller.	Imprisonment upto 3 years and fine upto two lakhs, or both.
69	For failing to extend facilities to decrypt information which is against the interest of sovereignty or integrity of India.	Imprisonment which may extend to seven years.
70	Securing or attempting to secure access to a protected system.	Imprisonment which may extend to 10 years and fine.
71	For misrepresentation or suppression of any material fact from the Controller or the Certifying Authority.	Imprisonment upto 2 years, or fine upto rupees one lakh or with both.
72	For break of confidentiality and privacy	Imprisonment upto two years or fine upto rupees one lakh, or with both.
72 A	For disclosure of information in breach of lawful contract.	Imprisonment upto three years or with fine upto five lakh rupees or with both.
73	For publishing digital signature certificate false in certain particulars.	Imprisonment upto two years or with fine which may extend to one lakh rupees or with both.
74.	Publication of Digital Signature Certificate for any fraudulent or unlawful purpose.	Imprisonment upto two years or fine upto rupees one lakh.
76	Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto used for contravention of this Act, rules, orders or regulations made thereunder.	Liable to confiscation.

Conclusion/ Recommendations

Ignoring the progress, going in same rules and relies on standard law and also to handle or prosecute cyber crimes is the biggest thing to provide mental strong strength to do the same or repeat, which result the growth percent high. Decreasing value of money making the monetary punishment against the crime is tolerable as the gain from the crime is incising, which is also very big factor in crime growth. E-Space security Management is now becomes an important challenge for National Security Management, Military related Scientific Security Management and Intelligence Management all over the globe. Availability and easy accessibility of internet and smart phones became very danger at the same time we cannot justify our life even a single day. We cannot say for certain what new advances the internet will give us, what new art forms, social classes, or subcultures it will engender. In this stage it is very important to be one step ahead by making ourselves aware about the positive and negative aspect and advancement of technology and protect ourselves from any hi-tech crime.

Some recommendations;

- ❖ Laws against cyber crime must be updated in regular basis
- ❖ Assurance from the govt. side that, Implementation of laws.
- ❖ Backup system of Government or other firms must be focused on backup system of e-data and security of the websites more protected to avoid the much harm, if anything goes wrong.
- ❖ A model approaches is required.
- ❖ Making general people aware is very important.

One thing here I would like to mention that, "if anybody of firm assuring 100% security against cyber crime will the biggest myth of the world"

Acknowledgement

I would like to thanks Satija Research Foundation for Library and Information Science (SRFLISindia), Tecnia Institute of Advanced Studies for providing such a educated and innovative platform and the most important to mention here Dr. K. P. Singh DLIS, DU, for his timely and constructive guidance.

- ***References***

- *Answers.com (s.d.) Define data diddling? Retrieved from http://www.answers.com/Q/Define_data_diddling.*
- *Benedikt, Michael. (1991). Introduction to Cyberspace: First Step. Massachusetts: MIT Press.*
- *Beza (s.d.). History of Cybercrime. Retrieved from http://www.bezaspeaks.com/cybercrime/history.htm*
- *Bhansali, S. R. (2014). The Information Technology Act2000. Jaipur: University Book House.*
- *Criminal Lawyer Group. (2015). Criminal Defense >> The evolution of cybercrime from past to the present. Retrived from http://www.criminallawyergroup.com/criminal-defense/the-evolution-of-cybercrime-from-past-to-the-present.php.*
- *Cyber Crime Lawyer V.K.Singh. (2013). Tampering with computer source documents: section 65 of IT Act 2000. Retrieved from https://cybercrimelawyer.wordpress.com/2013/05/16/section-65-of-it-act-2000-tampering-with-computer-source-documents/*
- *Cyberlawsindia.net. (2007). Cyber Law Introduction. Retrieved from http://www.cyberlawsindia.net/index1.html.*
- *Dasgupta, M. (2009). Cyber crime in India: A comparative Study. Kolkata: Eastern Law House.*
- *Encyclopadia Britannica. (2015). You searched for Cyber defamation. Retrieved from http://www.britannica.com/search?query=Cyber+defamation*
- *Garner, B. A, & Black, H. (2009). Black's law dictionary. St. Paul, Minn: West Group.*
- *Government of Canada (2015). Criminal Code (R.S.C., 1985, c. C-46). Retrieved from http://laws-lois.justice.gc.ca/eng/acts/C-46/section-163.1.html.*
- *IBN Live (2014). Hyderabad: Man arrested for mailing obscene pics morphed on boss' wife. Retrieved from http://ibnlive.in.com/news/hyderabad-man-arrested-for-mailing-obscene-pics-morphed-on-boss-wife/519681-62-270.html*
- *Kadish, S. H. (1983). Encyclopedia of crime and criminals. New York: Free Press.*
- *Khan, Nadia. (2012). Insight to Cybercrime. Retrieved from http://www.hanyang.ac.kr/home_news/H5EAFA/0002/101/2012/29-3.pdf*
- *Kumar, Arun B. R. (2012). Issues of Cyber Laws and IPR in Software Industry and Software Process Model. International Journal of Computer Application, 44 (16), 1-6.*
- *Oxford. (2010). Oxford advanced learners dictionary. UK: Oxford University Press.*
- *Tandon, Rajesh (2010). Lecture on the workshop on Cyber Law Cyber Law & Adjudication Issues in India. New Delhi. Retrieved from http://catindia.gov.in/writereaddata/ln_bgKMZv1_17_2012.pdf.*

A Study of Consumers Perception And Attitude In Life Insurance Industry

Bhoopendra Bharti [1], **Dr. SS Sharma** [2]

[1]Research Scholar (Commerce) MJP Rohilkhand University, Bareilly
E-mail: bhoopendrabharti@yahoo.co.in Mob. No. 9350464601

[2]Reader Department of Commerce, Bareilly College, Bareilly

ABSTRACT

The Indian insurance market offers many opportunities in the form of a huge market which is growing at a fast pace. The present article tries to capture the prevailing market conditions in the Indian insurance industry. It explains the reasons for why India is such an ideal place for insurance industry keeping in sight the growth trend of the industry over last few years.

KEYWORDS: Insurance, Consumer perception, Bareilly division.

1. INTRODUCTION

The Indian population is second only to China. Hence the demand for insurance is likely to be on higher side. Apart from population the other reasons that make this insurance sector to be an advantageous position. Increase in literacy rate, growing awareness of insurance, increase in income, role of agents, and newer and transparent regulations by IRDA has boosted the insurance industry.

The Indian life insurance industry has witnessed a long journey. Life Insurance in its current form was introduced in 1818 when Oriental Life Insurance Company began its operations in India. General Insurance was however a comparatively late entrant in 1850 when Triton Insurance company set up its base in Kolkata.

History of life Insurance in India can be broadly bifurcated into three eras: a) Pre Nationalization b) Nationalization and c) Post Nationalization. Life Insurance was the first to be nationalized in 1956. Life Insurance Corporation of India was formed by consolidating the operations of various insurance companies. General Insurance followed suit and was nationalized in 1973.

General Insurance Corporation of India was set up as the controlling body with New India, United India, National and Oriental as its subsidiaries. The process of opening up the insurance sector was initiated against the background of Economic Reform process which commenced from 1991. For this purpose Malhotra Committee was formed during this year who submitted their report in 1994 and Insurance Regulatory Development Act (IRDA) was passed in 1999. Resultantly Indian Insurance was opened for private companies and Private Insurance Company effectively started operations from 2001.

The insurance sector was opened up for private participation four years ago. For years now, the private players are active in the liberalized environment. The insurance market have witnessed dynamic changes which includes presence of a fairly large number of insurers both life and non-life segment. Most of the private insurance companies have formed joint venture partnering well recognized foreign players across the globe.

There are now 29 insurance companies operating in the Indian market – 14 private life insurers, nine private non-life insurers and six public sector companies. With many more joint ventures in the offing, the insurance industry in India today stands at a crossroads as competition intensifies and companies prepare survival strategies in a detariffed scenario.

There is pressure from both within the country and outside on the Government to increase the foreign direct investment (FDI) limit from the current 26% to 49%, which would help JV partners to bring in funds for expansion.

There are opportunities in the pensions sector where regulations are being framed. Less than 10 % of Indians above the age of 60 receive pensions. The IRDA has issued the first license for a standalone health company in the country as many more players wait to enter. The health insurance sector has tremendous growth potential, and as it matures and new players enter, product innovation and enhancement will increase. The deepening of the health database over time will also allow players to develop and price products for larger segments of society.

OBJECTIVES OF THE STUDY

1. To study about the important players in the Indian insurance industry.
2. To analyze the aspects of consumers decision process for insurance.
3. To suggest suitable measures for players in Indian insurance industry.

RESEARCH METHODOLOGY

In this research the primary data has been collected from consumers in the district of Bareilly. 250 questionnaires were served to consumers out of which response came from 186 consumers. 6 questionnaires were found to be partially filled so only 180 questionnaires were considered for final analysis.

Secondary data has also been used wherever necessary. It has been collected from newspapers, journals, reference books & internet. Descriptive technique like table has been used to show the research analysis. The analysis has been done in a very simple to understand manner. The use of jargons in the analysis has been kept to a very minimum level. A five-point **Likert scale** was used for measuring the items of this study.

FINDINGS

According to report from researchandmarkets.com, the insurance industry is likely to show the following trend:

- Total life insurance premium in India is projected to grow Rs 1,230,000 Crore by 2010-11
- Total non-life insurance premium is expected to increase at a CAGR of 25% for the period spanning from 2008-09 to 2010-11.
- With the entry of several low-cost airlines, along with fleet expansion by existing ones and increasing corporate aircraft ownership, the Indian aviation insurance market is all set to boom in a big way in coming years.
- Home insurance segment is set to achieve a 100% growth as financial institutions have made home insurance obligatory for housing loan approvals.
- Health insurance is poised to become the second largest business for non-life insurers after motor insurance in next three years.
- -A booming life insurance market has propelled the Indian life insurance agents into the 'top 10 country list' in terms of membership to the Million Dollar Round Table (MDRT) — an exclusive club for the highest performing life insurance agents.

Types of insurance purchased

Keeping in mind the trend of insurance sector for the country, the focus of this study was to find the pattern of purchase of insurance products in Bareilly. The finding is shown in table 1:

Segment	Share %
General	41.83
Life	58.17

Table1: Share % of insurance types purchased in Bareilly Division

It is seen that the Indian insurance market is dominated by the gents' segment which is in contradiction to the global trend where the ladies' segment has the dominant share. India is fast experiencing a change in this scenario. In the coming years this ratio is set to change. There are going to be many opportunities in the child plans and the female plan insurance.

The rising awareness about health and fitness is going to play a major role in increase of the insurance sector. Many foreign players have already shown increased interest in this segment. They have also come up with innovative marketing strategies to promote heavily their products. Indian insurance market is set to experience a phenomenal growth in the coming years. India is witnessing a fast changing retail landscape. So there is still a plethora of opportunities in the insurance industry.

Following is the list of some of the major life insurance company granted permission by IRDA that were covered as part of this research.

1. Bajaj Allianz Life Insurance Company Limited
2. Birla Sun Life Insurance Co. Ltd
3. HDFC Standard Life Insurance Co. Ltd
4. ICICI Prudential Life Insurance Co. Ltd.
5. ING Vysya Life Insurance Company Ltd.
6. Life Insurance Corporation of India
7. Max New York Life Insurance Co. Ltd
8. Met Life India Insurance Company Ltd.
9. Kotak Mahindra Old Mutual Life Insurance Limited
10. SBI Life Insurance Co. Ltd
11. Tata AIG Life Insurance Company Limited
12. Reliance Life Insurance Company Limited.
13. Aviva Life Insurance Co. India Pvt. Ltd.
14. Sahara India Life Insurance Co, Ltd.

15. Shriram Life Insurance Co, Ltd.
16. Bharti AXA Life Insurance Company Ltd.
17. Future Generali Life Insurance Company Ltd.
18. IDBI Fortis Life Insurance Company Ltd.
19. Canara HSBC Oriental Bank of Commerce Life Insurance Co. Ltd
20. AEGON Religare Life Insurance Company Limited.
21. DLF Pramerica Life Insurance Co. Ltd.
22. Star Union Dai-ichi Life Insurance Comp. Ltd

Types of life insurance purchased

At the present time the usage pattern in Bareilly is as shown in table 2:

S. No	Type of Life Insurance	Share%
1	Term life insurance	26.60
2	Money back policies	21.53
3	Endowment policies	18.52
4	Permanent life insurance	09.63
5	Annuity / pension policies / funds	23.72

Table 2 : Share % of life insurance types purchased in Bareilly

Monthly income of respondents

133 respondents i.e. 74% had a monthly income exceeding Rs 20,000, 38 had an income between Rs. 10,0000 & 20,0000. Rest of the 9 respondents had a monthly income less than Rs 10,000. The monthly incomes of the respondents are as follows (Chart 1):

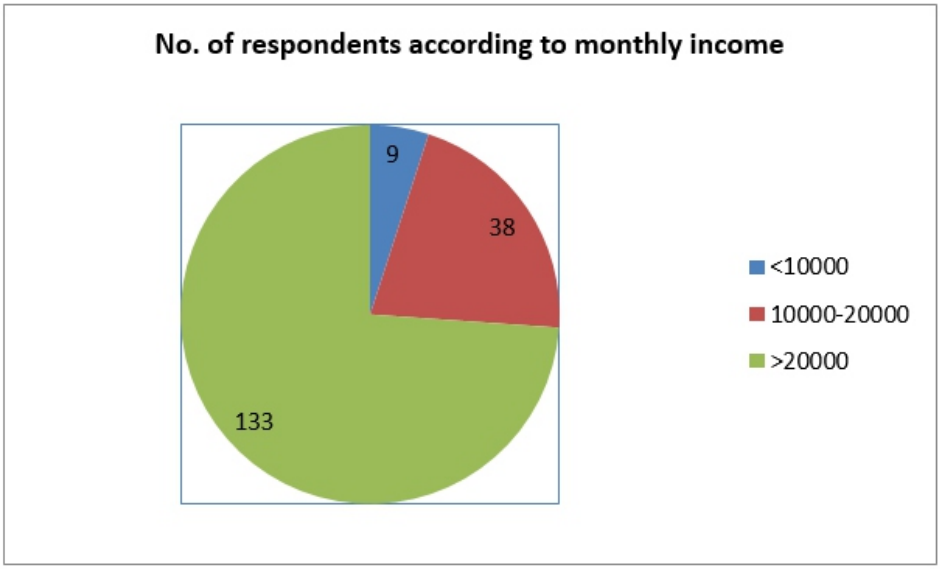


Chart 1: No. of respondents according to monthly income

Consumer preference for different insurance companies

The customers were asked to mark the company from which they have sought insurance product. The findings are shown in the Chart 2.

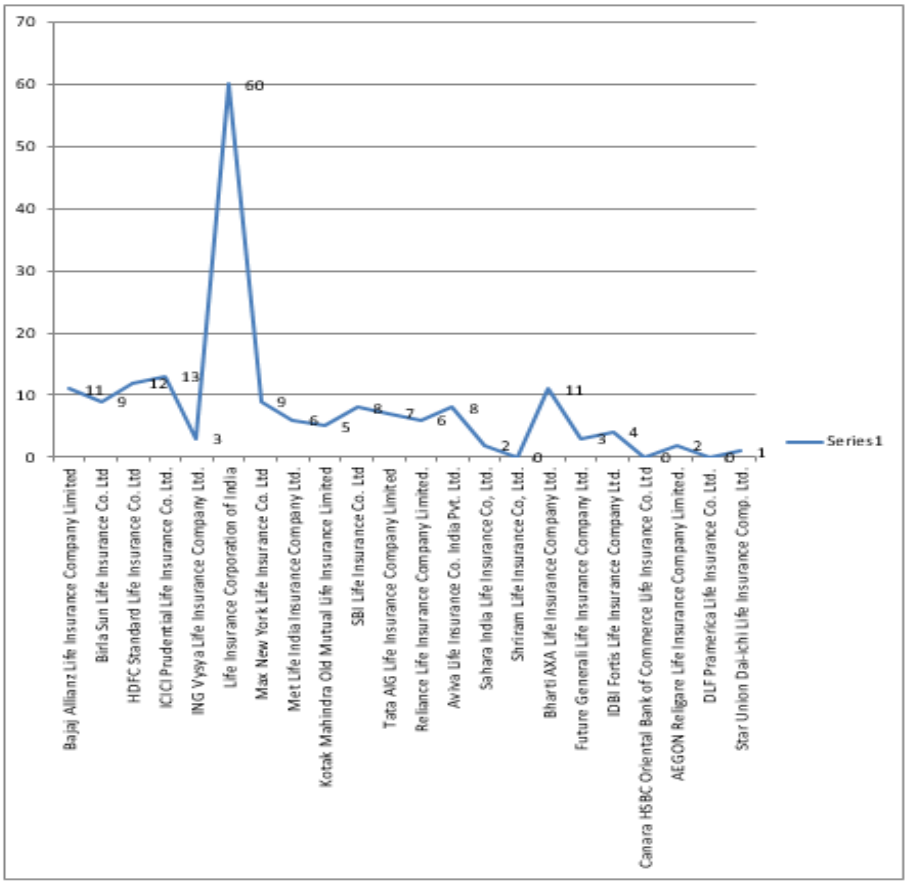


Chart 2: Consumer preference for different insurance companies

Consumer perception of significant differences among different insurance companies

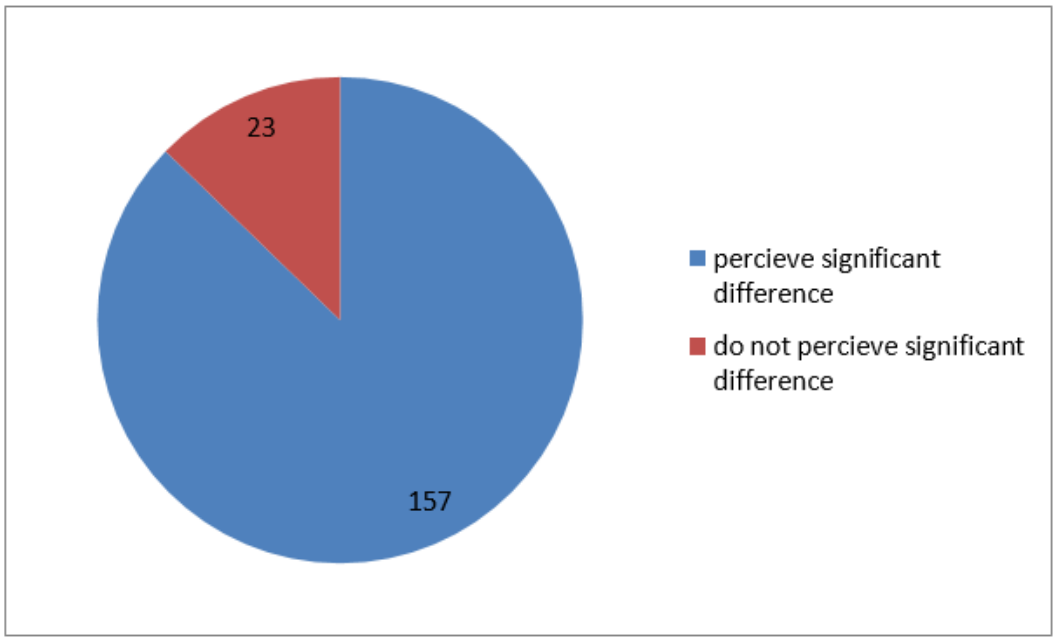


Chart 3: Consumer perception of significant differences among different insurance companies

Respondents feel there are significant differences in brand categorizing. 157 consumers out of 180 said that they perceived significant differences among different insurance companies. Only 23 consumers said that they did not perceive significant differences among different insurance brands. This shows that an insurance company is in the area of complex decision making for majority of consumers. It is a high involvement product.

Basis of selection of insurance products among customers

A five-point Likert scale rating from 5=strongly agree to 1= strongly disagree was used for measuring the items of this study. The responses were then tabulated. As can be seen from the table 6 the factors have been enlisted under the heading criterion. They have been assigned weights 1, 2, 3, 4 & 5 respectively for responses Strongly Disagree, Disagree, Neutral, Agree, and Strongly Agree. Then weighted average has been calculated by dividing the product of weights and number of responses by total number of responses.

Factors having a weighted average of more than 3 have been then taken as important. It means these factors are considered important by respondents for selection of insurance products. Out of the five factors considered three factors fall in this category.

Criterion	No. of responses	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree	Weighted Average
Weights assigned	-	5	4	3	2	1	
Cost is important for selection of insurance products	180	63	86	1	22	8	3.97
Features of the product are important for selection	180	59	80	14	21	6	3.92
Brand loyalty is important factor for selection of insurance product	180	14	29	3	93	41	2.34
Advertisement is an important element of selection of insurance product	180	34	73	10	46	17	3.38
Other factors like innovation in riders, ease of payment mode, and variety of plans available are important factors in purchase of insurance products	180	0	41	5	73	61	2.14

Table 3: Basis of selection of insurance products among customers

The consumers attach highest importance to cost and features of the insurance products. Advertisement was a lesser important factor for selecting insurance product.

Cost and features were the most important aspects for selection of insurance product for consumers. Out of the 180 consumers, 149 (63+86) consumers either strongly agree or agree that cost is an important aspect. This was followed by features, to which 139 (59+80) consumers either strongly or agreed is an important factor. 107 (34+73) consumers chose to agree that advertisement is an important factor for selection of insurance product

Brand loyalty scored low on this aspect which was selected by only 43 (14+29) consumers as important factor. Some of the other aspects like innovation in riders, ease of payments and variety of options available within a brand were also found as scoring low.

Influencer in purchase of Insurance

The consumer himself was found to be the final decision maker in purchase of insurance products. Most of the times with 85% consumers i.e. 153 out of 180 saying that they made the final decision. Spouse, children, friends and others played were rarely the final decision makers. 11 said friends, 5 said children, 4 said spouse and 7 said that others made the final purchase decisions.

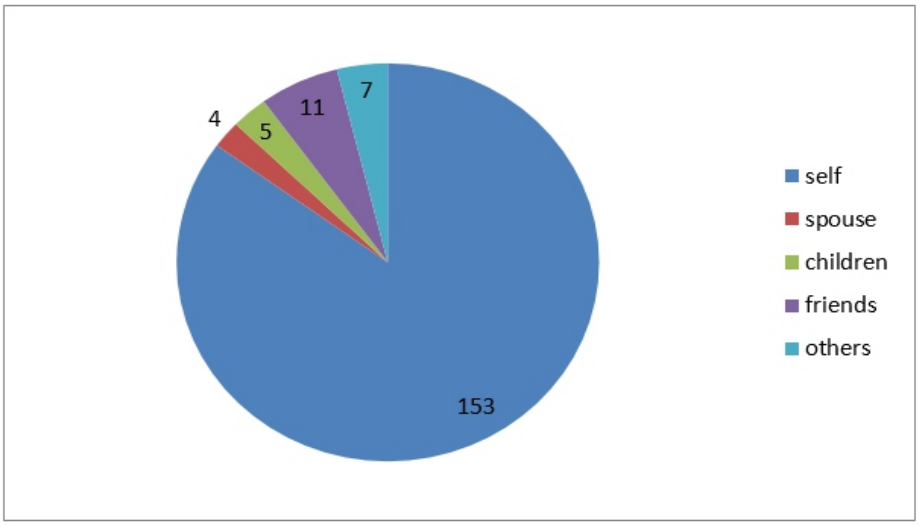


Chart 4: Influencer in purchase of Insurance

CONCLUSIONS AND SUGGESTIONS

The study led to knowledge about the important players in the Indian life insurance industry. The major aspects analyzed aspects in consumer decision process for life insurance sector. Major conclusions and suggestions of the research are:

The life insurance industry in India is mainly in the organized sector. The Indian life insurance industry is provided with infrastructure support through premier institutions like TRAI, in the areas of technological development, design and product development and human resources development and care for customer rights.

The research reveals that majority of consumers feel there are significant differences in brand categorizing. It is in the area of complex decision making and is a high involvement product. Therefore branding is a major decision for insurance companies. Brand building should be given high importance by manufacturers.

The consumers attach highest importance to cost and features of the life insurance product. Therefore affordable life insurance product with good features has a high potential in the industry.

According to this research the consumer himself was found to be the final decision maker in purchase of life insurance product most of the times. Therefore efforts should be made to target the final consumer like advertisement directed towards them.

The Indian life insurance industry is yet to witness changes in product mix, market structure and strategies of key players. The market has huge untapped potential. Like in all the other industries, technology will play a major role in reshaping of this industry in India.

REFRERENCES

- *Annual Report of the Ministry of Finance (Section 3, Insurance Division, http://finmin.nic.in/the_ministry/dept_eco_affairs/budget/annual_report/9596ea3.PDF).*
- *Bhattacharya, Saugata and Urjit R. Patel, "Reform Strategies in the Indian Financial Sector," Paper presented at the Conference on India's and China's Experience with Reform and Growth, November 2003.*
- *Cummins, David, Mary Weiss and Hongmin Zi, "Organizational Form and Efficiency," Financial Institutions Center, Working Paper No. 97-2, 1997, Wharton School, University of Pennsylvania.*
- *Farrell, M, 1957, "The Measurement of Productive Efficiency," Journal of the Royal Statistical Society, Series A, 120, 253-281.*
- *Gazette of India Extraordinary Part III Section 4. Insurance Regulatory and Development Authority (Investment) Regulations, 2000.*
- *General Insurance Corporation, Annual Reports, various years.*
- *Guerrero, Victor and Tapen Sinha, 2004, "Statistical Analysis of Market Penetration in a Mandatory Privatized Pension Market Using Generalized Logistic Curves," Journal of Data Science, 2, 196-211.*
- *Indian Insurance Commissioner's Report, 1929, Her Majesty's Stationary Office, London.*
- *IRDA Journal, 2004, "Market share for premiums: life market (March 2003-February 2004)," April, 38-39.*
- *IRDA Journal, 2004, "Gross Premium Underwritten by General Insurance Companies,"(April 2003-February 2004), April, 40.*
- *Life Insurance Corporation Annual Reports, various years.*
- *Malavya, H. D. "Insurance in India." Undated.*
- *Malhotra Committee Report on Reforms in the Insurance Sector, 1994. Government of India, Ministry of Finance, New Delhi.*
- *OECD, 2003. OECD Handbook on Insurance, Paris.*
- *Press Trust of India, 2004. "India leads the world in road accident deaths," Wire Report, January 3.*
- *Rajagopalan, R., 2004, "Valuing the Term Insurance Products in the Indian Market," Paper presented at the Fifth Global Conference of the Actuaries, January 25, New Delhi.*
- *Rao, G. V., 2003, "Playing It Safe," IRDA Journal, November, 14-16.*
- *Rodrik, Dani and Arvind Subramanian, 2003, "Why India can grow at Seven Percent," Economic and Political Weekly, April 17.*
- *Sigma, 2003, "World insurance in 2002." Swiss Re.*
- *Srinivasan, K. K. 2003, "Transition from Tariff Model of Pricing Non-life Insurance in Emerging Markets: Issues & Prospects" Paper presented at the Seventh Conference of the Asia Pacific Risk an Insurance Association Conference, Bangkok, 23 July.*
- *Swain, Shitanshu, 2004, "LIC Refusing To See The Writing On The Wall," Financial Express, April 19.*
- *Swiss Reinsurance Company database.*
- *Tripathi, Dwijendra, 2004, The Oxford History of Indian Business (Oxford University Press, Oxford). Vaidyanathan, L. S., 1934, "Mortality Experience of Assured Lives in India, 1905-1925," Journal of the Institute of Actuaries, 60, 5-66.*
- *Vaidyanathan, L. S., 1939, "Mortality Experience of Assured Lives in India, 1925-1935," Journal of the Institute of Actuaries, 70, 42-71.*
- *Wilson, Dominic and Rupa Purushothaman, 2003, "Dreaming with BRICs: the Path to 2050," Goldman and Sachs, Global Economics Paper No. 99, October.*

Impact of Social Media on Society and Cyber Law

Vipul Partap [1], Rahul Mittal[2]

[1]Assistant Professor, Tecnia Institute of Advanced Studies,
Email: vipulpartap@rediffmail.com Mobile: 9013494334

[2]Associate Professor, Tecnia Institute of Advanced Studies
Email: rahul.rahlmus@gmail.com Mobile: 9891351127

A B S T R A C T

The number of Twitter followers, Face book likes and J.R.P. (John Robert Powers) ratings are being rarely used as proxies for popularity and approved ratings. It threatens to cultivate an unfettered noisy and sometimes meaningless discourse culture with "famous" personalities pontificating on everything, so as to be seen as "speaking out."An IGO character (iGO Navigation - Global Navigation Software) communication medium available to all is a wonderful tool to rare issues but it leaves little room for a healthy debate and drawing meaningful solutions. Important issues are capsule down with rhetoric, wit and spin to make a point. Social media is powerful but can also encourage and reward a shallow posturing culture in society. Long gone are the days when a computer took up an entire room. Now we have computers at home, laptops that travel just about anywhere, and data networks that allow us to transmit information from virtually any location in a timely and efficient manner. Computers and the Internet can offer great benefits to society. However they can also present opportunities for crime, much of it just traditional crime using new technology tools.

Keywords: Cyber Crime, Media, Face book, Cyber Law

1. INTRODUCTION

Today the Internet is connected to nearly 200 countries. The very nature of a globally connected network has made it painfully clear that cyber criminal activity cannot be effectively addressed by individual nations or even a group of industrialized countries, whether it requires a concerted effort between industry, government officials, law enforcement, and citizens of all countries. Things can go wrong in cyberspace. There's fraud, stalking, viruses, outright theft, and more. And while the online world is still not nearly as dangerous as the physical realm, it pays to take precautions against victimization. Cyber crime manifests itself as pornography on the web, online harassment and stalking, e-mail security violation, data security violation, virus implantation, fraud, unauthorized credit card access, and more.

"Flavor of our times" likes it or not, social media is fast becoming the feedstock for mainstream media. It has become an intrinsic part of the information system. It manifests the true spirit of participative democracy, a collaboration of a million minds, who give and receive in the engagement of ideas. People are increasing using social media to evaluate and counter-check competing claims by politicians and business.

The Face book user base in India rare by 50 percent since last year, to touch 78 million users as of March 31, 2013, according to the data furnished by the U.S. Securities and Exchange Commission. India currently has nearly 20 million Twitter users, according to a joint study by market research firm IMRB. The impact of Social Media cannot be predicted. Its broadcasting also could be neither controlled nor checked. Ultimate democracy of expression is to large extent be biased. With social media, the rule of Communication is not in constitutional framework. The checkpoint is also very slow and confusing. We live in a world where a Wik Leaks whistleblower is challenging the depth and reach of intelligence agencies; where a social network called Face book has become the third largest country. It can undoubtedly topple regimes but can it build new, more democratic ones? A majority of chief ministers and senior political leaders agreed with Prime Minister Dr. Manmohan Singh's concern at misuse of social media and urged the centre to device a mechanism to deal with this new phenomenon, while some demanded stricter cyber laws to deal with mischief mongers. In 16th national integration council meeting which is held in Delhi in Sept., 2013, many speakers said that the clause in the information technology act, section 66A, should be suitable modified so that this clause is not misused to suppress views and dissenting opinions.

The view of Data Security Council of India's C.H.O. Kamlesh Bajaj is that the critical internet resources like domain name serves, global routers, and the control of ICANN for internet governance give a natural advantage to the U.S. in global cyber surveillance. These platforms are used by all countries, and their traffic largely passes through the U.S., thereby exposing it to surveillance. Your seemingly innocuous ports on Face book or Twitter may not be free from the surveillance programme of the United States' National security Agency. So vast is the web of information through and monitored by the U.S. that there is a reason to worry, says Neville Roy Singham, founder and Chairman of global software network thought works.

Why Social Media is a Nightmare for Parents

> Archana Satpathy: The amount of time youngsters are wasting on social media is one of the most worrying factors; This is the most crucial period of their life - they learn not just from books but also from their environment. The virtual world of Internet can hardly teach them the realities of life.

Prachi: With both parents working nowadays, children spend more time online. At this vulnerable age, they are unable to distinguish between right and wrong and thus fall prey to antisocial elements.

Sarbjeet: Children are becoming vulnerable to attacks from peers and bullies. There are a large number of people with forged identities who can often exploit and take advantage of lonely teenagers; most of whole parents are busy at work for the greater part of the day.

A teenage school girl Jaspreet receives regular Face book messages from a class boy. Through words and images, he mocks her appearance. Earlier this month, a Delhi, Bangalore, based two schools asked parents of class 1 to 10 students to have their children disable their Face book accounts, as the principals are receiving a growing number of complaints from students being bullied online. A 2012 survey on Global Online youth Behaviour found that 53 percent of eight to 17 year olds in India had been bullied online, while 50 percent admitted to have bullied online. The National Crime Records Bureau report of 2012 says that 50 offenders under the age of 18 were booked under the Information Technology Act (IT Act) in four states: Kerala, Madhya Pradesh, Rajasthan and Maharashtra. Delhi-based cyber lawyer Paran Duggal says that he has dealt with about 150 cases of cyber bullying, more than half of which involved children, over the last three years. Lawyers say that bullying can be considered an offence under the controversial section 66A of the IT Act. Under this, one can be booked for "grossly offence" messages and for "causing inconvenience.»

The research by Rui Fan and colleagues at Beihang Univerity in China compared the way that tweets labelled with specific emotions influence other people on the network. The results clearly show that anger is more influential than other emotions such as joy or sadness.

Face book confession groups - a recent trend of pages with anonymous posts - is a common hunting ground for cyber bullies. Recent high profile victims of online abuse and threats include British M.P. Stella Creasy, feminist writer campaigner Caroline Criado-Perez, The Guardian's Hadley Freenan, and Time magazine's Catherine Mayeb. She was subjected to abuse, rape and death threats on Twitter, several commentators blamed the phenomenon on the shortcomings of social media. Same situation has been occurred in Malala, Taslima, Damini, Guwahati rape case etc. Hundreds of British children have been blackmailed into indulging in online sex acts and consequently making several of them ill themselves. Britain's child exploitation and Online Protection (CHOP) has revealed. According to figures from the police forces in the U.K. and abroad, 424 children have been a victimized and have being forced to submit to online sexual blackmail in some form. Among them, 184 belonged to the U.K. Once the child has sent the images, the offenders begin blackmailing them either for more of such

indecent images or, in few cases even for cash. Mindful of the privacy fears that NSA whistleblower Edward Snowden's renelations about government snooping have raised, Face book has again assured its monthly global users that their personal information had not been compromised.

The Twitterati attacked the Akhilesh government for its inability to anticipate and control the flare up. A (a) faking news tweet said: "UP government has blamed social media for UP riots, never knew people check Facebook updates and tweets during mahapanchayat." This was retweeted 100 times. (a) 1 The Ace tweeted,"A video can provoke communal riots? Some accounts allegedly tried to pass images of violence from Syria as Muzaffarnagar. (a) Joydas tweeted, "U knows how bad Akhilesh Yadav has been for UP from the fact that people remembers Mayawati govt. fondly as the 'Good old days.' In report, Google claims consumers are more likely to find pirated material from friends of social networks than by using its search engines.

Psychological Aspects

Several studies are now bringing out the narcissistic effect of social media. Apparently, there is a rise of narcissism amongst the generation born in the 1980s and 1990s, controversially dubbed as "Generation Me" by Professor Jean M. Twenge in 2007. In fact, over the last couple of years, extensive research has shown positive connections between Face book and narcissism. This may stem from the way people use Face book to look important, look special, gain attention, status and self-esteem, thus presenting an unrealistic portrait of themselves. These people can be identified easily as the ones who post numerous attractive looking photos of themselves, then tag themselves and others in the photo to gain attention likes and comments, and also update their statuses more frequently. This aspect gives rise to voyevtism. Recently, a psychology paper (published in the Journal Personality and Individual Differences) found increasing evidence that young people are becoming increasingly narcissistic, and obsessed with self image and shallow friendships. Frequent networking on sites like Face book could also sites like Face book could also generate negative feelings like inadequacy, envy, jealousy or even aggressive behaviour due to constant comparison with their own colleagues / friends or peers who always "appear" to be better off. Face book is flooded with photos of people looking very happy with life, parting with their long lost friends or families, travelling to exotic destinations, or simply showing off their riches in the form of pictures of their flashy cars, stylish homes or yachts etc. Women, who are slim and know they, look good, post pictures of themselves in stunning outfits. All these facts are bound to have some kind of psychological impact on others who feel that they are "lesser" or inadequate in some manner or other. These comparisons can make our successes feel diminished and our failures amplified. Among the naysayers is American Author Nicholas Carr, who in his book, "The shallows, what the Internet is

Doing to our Brains?" argues the while Internet improves our cognitive ability to skim and scan; it diminishes our intellectual capacity to concentrate and contemplate. Internet gradually makes us incapable of long form reading and long hours of intellectual focus. Cyber space is on the frontline of the battle between freedom and control in the 21st century. If the government, companies, others wish to use cyberspace they need to be willing to accept the attendant risks and costs, just like they are for road or sea transit. Transfer loss and copyright theft are all part of this. It is critical that the information age does not turn into an age of 'digital imperialism.'

The Vice President of Observer Research Foundation Samif Saran says: If governments and corporate don't decide the rule, which does? The reality is that no corporate house or government has the organizational nimbleness to lay the rules here - technology's moving for fast for that. Technology is both the problem and the solution. It is an intensely personal extension of one's deepest thoughts and secrets. An extension of the mind, this moves it both private property as well as an outlet of expression, while at the same time being a global common open to everyone. Counterpoising national security and cyberspace or making international cooperation department on cyber security is both pompous and misplaced. It is a free-wheeling mind space at the cutting edge of innovation precisely because of the absence of sovereignty and artificial barriers. The rate of adoption of internet has exceeded most mass communication technologies making it almost indispensible for the modern consumer. The growing popularity of social media has coincided with the decline of the use of traditional media which has resulted in a shift from the concept of traditional one way communication to mode where people interact with each other.

Unfortunately, at present in India, there has been an over reliance and focus on Twitter, which by very nature is a low depth medium. A greater reliance on text or video blogs can be far more beneficial for deeper disclosures, which can then be discussed through a more instant medium like twitter. Aristotle, one of the pioneers on the idea of persuasion has talked about logos (logic), pathos (emotion) and ethos (credibility) as three does of persuasion. Persuasion through emotion is one area where social media empowers leaders as opposed to the traditional discourse. Instant replies (reciprocity to personal queries and thoughts of people make social media a relevant and a powerful tool for any leader. It also leads to a discourse that gives citizens a great understanding of the leader and the party. An important aspect of the Indian social media is that it has a high representation of youth. Approximately 72% of Indian social networking site users fall into the Gen Next Category (19-24 years).

The authors of 'The New Digital Age,' Eric Schmidt Executive Chairman of Google and Jared Cohen, Director, Google Ideas, told that 'the Internet is among the few things humans have built that they don's

truly understand.' The New Digital Age carries a full chapter dealing with terrorism. It says: "As we have made clear, technology is an equal-opportunity enabler, providing powerful tools for people to use for their own ends, sometimes wonderfully constructive ends, but sometimes unimaginably destructive ones.

Cyber Law

India has enacted the first I.T.Act, 2000 based on the UNCIRAL model recommended by the general assembly of the United Nations. Chapter XI of this Act deals with offences/crimes along with certain other provisions scattered in this Acts .The various offences which are provided under this chapter are shown in the following table: -

Offence	Section under IT Act
Tampering with Computer source documents	Sec.65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

NOTE: Sec.78 of I.T.Act empowers Deputy Superintendent of Police to investigate cases falling under this Act.

Computer Related Crimes Covered Under IPC and Special Laws

Offence	Section
Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499 IPC
Forgery of electronic records	Sec 463 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Emailspoofing	Sec463 IPC
W eb-Jacking	Sec.383 IPC
E-M ailA buse	Sec.500 IPC
Online sale of Drugs	NDPS Act
Online sale of Arms	Arms Act

Elementary Problem Associated with Cyber

One of the greatest lacunae in the field of Cyber Crime is the absence of comprehensive law any where in the World. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of I.T. Act and amendments made to Indian Penal Code, problems associated with cyber crimes continue to persist.

™ Jurisdiction is the highly debatable issue as to the maintainability of any suits, which has been filed. Today with the growing arms of cyber space the territorial boundaries seem to vanish. Thus the concept of territorial jurisdiction as envisaged under S.16 of Cr.P.C. and S.2.of the I.P.C. will have to give way to alternative method of dispute resolution.

™ Loss of evidence is a very common & expected problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses the system of crime investigation.

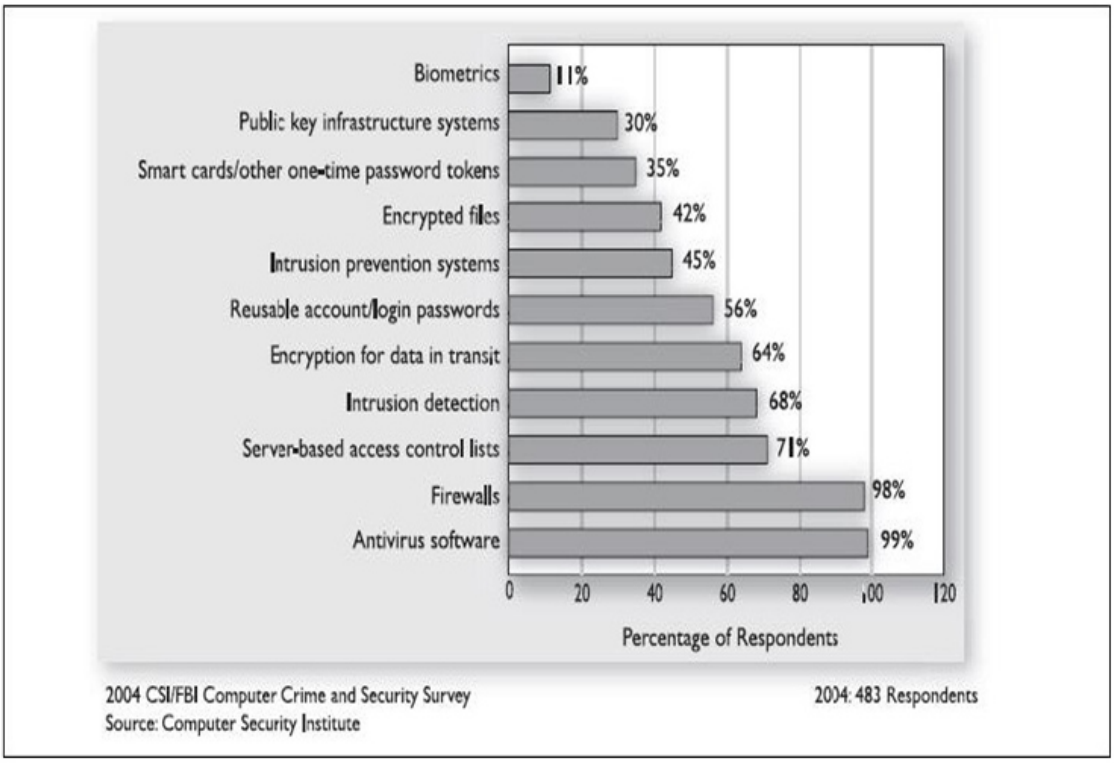
™ Cyber Army: There is also an imperative need to build a high technology crime & investigation infrastructure, with highly technical staff at the other end.

™ A law regulating the cyber-space, which India has done?

™ Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provision recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

™ Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such case, which needs appreciation, is the P.I.L. (Public Interest Litigation), which the Kerala High Court has accepted through an email.

'Perfect' is a relative term. Nothing in this world is perfect. The persons who legislate the laws and by-laws also are not perfect. The laws therefore enacted by them cannot be perfect. The cyber law has emerged from the womb of globalization. It is at the threshold of development. In due course of exposure through varied and complicated issues it will grow to be a piece of its time legislation.



The Information Technology Act 2000

An At to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "Electronic Commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends, inter alia, that all States give favorable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records

Cyber Crime Laws Vary

This article provides examples of countries with laws that deter and/or punish particular cyber crimes. Many countries still don't effectively deter, stop, limit or punish cyber crime. A cyber crime is either any crime that requires the use of a computer system to complete the crime or a crime where the computer system is the target of the crime. Here are examples of a few countries with laws related to particular cyber crimes. This is not a complete list of every country with laws related to cyber crime.

1. In Australia, forgery, fraud, hacking and theft related to a computer system can be cyber crimes.
2. In Belgium, electronic sabotage, forgery, fraud and hacking related to a computer system can be cyber crimes.
3. In Canada, the courts seem to update the law to include cyber crime by using existing laws related to electronic sabotage, forgery, fraud, intrusion and theft.
4. In Chile, the courts seem to be considered competent to hear cases of any cyber crime involving child pornography as long as the website involved can be visited from Chile.
5. In the Czech Republic, hacking doesn't seem to be a cyber crime but what you do with the accessed information can be.
6. In Ireland, theft and fraud related to a computer system can be cyber crimes.
7. In Japan, electronic sabotage, forgery, fraud, hacking and intrusion related to a computer system can be cyber crimes.
8. In Peru, electronic sabotage, forgery and intrusion related to a computer system can be cyber crimes.
9. In Spain, fraud and theft related to a computer system can be cyber crimes.
10. In the United Arab Emirates, it seems that forgery, fraud, hacking and theft related to a computer system can be cyber crimes in addition to the use of electronics to insult any religion.
11. In the United States of America, creating and operating a bot-network is now a Federal cyber crime. In addition, electronic sabotage, forgery, fraud, hacking, identity theft and intrusion related to a computer system can be cyber crimes.

Conclusion

Capacity of human mind is unfathomable. It is not possible to eliminate cyber crime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime. Undoubtedly the Act is a historical step in the cyber world.

Further I all together do not deny that there is a need to bring changes in the Information Technology Act to make it more effective to combat cyber crime. I would conclude with a word of caution for the pro-legislation school that it should be kept in mind that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive. Different media were used to create awareness and knowledge regarding the same. And this gave birth to the concept of Social awareness communication. Social awareness communication can be defined as a key strategy to inform the public about social concerns and to maintain important social issues on the public agenda. The use of the mass and multi media and other technological innovations to disseminate useful Social awareness information to the public, increases awareness of specific aspects of individual and collective issues as well as importance of Social awareness in development. Where there are so many positive aspects to the social media, there are bound to be negative aspects as well. It is fact that it cannot be controlled and therefore it goes without saying that it consequences can also be dangerous and uncontrollable for all those who use it recklessly and in an irresponsible manner. It is said that, "unless you take control of social media, you risk social media taking control of you."

References

Computer and Intellectual Property Section–Criminal Division. (2002). Searching and seizing computers and obtaining electronic evidence in criminal investigations. Washington DC: U.S. Department of Justice.
Cue´llar, M., et al. (2001).The transnational dimension of cyber crime and terrorism. Abraham D. Sofaer and Seymour E. Goodman (Eds). Palo Alto, CA: Leland Stan-ford Junior University, Hoover Institution Press.
Girasa, R. J. (2002). Cyberlaw: National and international perspectives. Upper Saddle River, NJ: Prentice-Hall.
Goetz, E., & Shenoi, S. (Eds.). (2007). Critical infrastructure protection (IFIP International Federation for Information Processing). New York: Springer.
Himanen, P. (2001). The hacker ethic and the spirit of the information age. New York: Random House, Inc.
Hugh, S. A. (2006). Computer and intellectual property crime: Federal and state law. Arlington, VA: BNA Books.
Levy, S. (1984). Hackers: Heroes of the computer revolution. New York: Doubleday.
Lewis, T. G. (2006). Critical infrastructure protection in homeland security: Defending a networked nation.
New York: Wiley-Interscience.
McCue, C. (2007). Data mining and predictive analysis: Intelligence gathering and crime analysis. Boston,
MA: Butterworth-Heinemann.
McQuade, S. (2006) Understanding and managing cyber crime. Boston, MA: Allyn and Bacon.
The Hindu, 23 Sept. 2013

The Hindu, 05 Sept., 2013
The Indian Express, 11 Aug., 2013
Schmidt, Eric & Cohen Jared, The New Digital Age.
Times of India, 10 Sept., 2013
Times of India, 12 Sept., 2013
Economic & Political Weekly, June, 2012.
Mainstream, Sept., 2012.
Yojna, May, 2013.
The Statesman, 4th Nov., 2012
The Times, 3rd Feb., 2013.
The Guardian, 1st Aug., 2012.
Langer, Ellem, The Power of Mindful Learning.
Carr, Nicholas, The Shallows: What the Internet is doing to our Brains?
www.scbatch.mit.edu
Frozen planet - http://www.open.edu/open learn

Remedies for Corruption in Authoritarian Countries under Democracy Reforms: Reexamining Anti-Corruption Agencies (Acas) For Alternatives an Analysis of Vietnam and Mainland China

Sang Thi Thu Bui
Kyushu University, Graduate School of Law
Comparative Studies of Politics and Public Administration in Asia
s.t.t.bui0504@gmail.com

ABSTRACT

In the countries where authoritarian regimes still exist, corruption is so systematic that justice is missing in most of the time. There is almost no hope for anti-corruption activities in strongly authoritarian regimes because under these "states of the bully" (Monteith, 2009), corruption is a matter of fact. However, in those under democracy reforms like Vietnam and Mainland China, the governments have been undertaking anti-corruption reforms. Although the governments' anti-corruption initiatives show little effectiveness, there may still be ways out. This paper aims at a remedy for widespread corruption in the countries. It argues that their current anti-corruption approaches which focus on anti-corruption enforcement through ACAs will not be able to reduce corruption that endorsed by not only their own institutional designs but also cultural and social values. To support the argument, the paper reexamines the possibility of ACAs under the current contexts of Vietnam and Mainland China by checking the existence of the conditions for successful ACAs provided by Meagher (2004) and Helbrunn (2004).The paper then proposes a reinforcing circle approach that combines the ethnographic approach with the democratic legitimacy approach as the remedy for their widespread corruption in consideration of all causes of corruption as well as the limitations of their capacity. Through contextual analysis, the paper identifies the different roles of intellectuals, civil societies and transnational networks in changing corrupt acts domestically considered as cultural and social practice, at the same time, points outspecific areas that each country should prioritize as more significant anti-corruption reforms.

Keywords Authoritarian Regimes, Widespread Corruption, ACAs, Ethnographic Approach, Democratic Legitimacy Approach

1. INTRODUCTION

Corruption is well-known as abuse of public power for private gains. Transparency International's 2012 Corruption Perception Index (CPI) that ranks 176 countries in terms of their corruption perception in public sectors shows that no country has a perfect score and two-thirds of countries score below 50, which indicates a serious corruption problem.

Corruption is more prevalent in developing countries than developed countries. And the most corrupt countries are strongly authoritarian. Why is corruption worse in those countries? According to Jain (2011), there are many conditions for corruption to arise. However, its survival depends upon three conditions. First of all, imperfect capital markets allow corruption to survive. Foellmi and Oechslin's (2007) argument cited by Jain implies that unlike in competitive markets, there are rents associated with a government's regulatory powers in imperfect capital ones, which is seen as the condition for corruption to emerge. Secondly, the system checking the bureaucracy within the administrative system or that by the society neither exists nor functions. The third condition is the ineffectiveness of the public institutions that are supposed to control corruption. Civic groups are not strong enough to exert moral pressures, opposition political parties are not allowed, the media is not free to expose wrong doings, and the legal system does not have the authority to prosecute and punish the guilty. In developing countries, especially those under authoritarian regimes, all three conditions co-exist, which creates a convenient environment for corruption to take place. Moreover, Segon and Booth (2010) and He (2000) who studied corruption in Vietnam and Mainland China pointed out two more reasons apart from the three conditions mentioned above. They are the motivation for monetary gain usually accentuated by poverty, low public sector salaries and the existence of cultural and social values endorsing corruption.

In term of forms of corruption, like in other countries, corruption in Vietnam and Mainland China often takes forms of bribery that can be both petty and grand, and fraud. Apart from that, cronyism and gift-giving were reported as forms of corruption often seen in Asia. (Khantri, Johnson and Ahmed, 2011 and Nojonen, 2011) According to the authors, cronyism has deep cultural roots. The authors developed a two-stage model of cronyism from a cultural perspective. The first stage describes how Confucian values, lack of trust, collectivism and paternalism lead to strong loyalty to superiors and emphasis on personal relationship and the second stage describes how these social behavior lead to the immediate antecedents of cronyism which are formation of strong in-groups, over-emphasis on relations and over-emphasis on loyalty. The author also pointed out that in China, gift-giving is regarded as a legitimate and traditional pattern of the subject's establishing a personal relationship with the official. In China, gifts are categorized as “ordinary business gift”-non-expensive small things, “hand-grenades and machine guns”-brand-name liqueur and cigarettes and “guided missiles”- highly appreciated items and personal favors. As a result, serious consequences of corruption in Vietnam and Mainland China were reported. The consequences are loss of state assets, reduction in business opportunities and competitiveness; reduce foreign investor confidence, under-utilization and loss of competent civil servants and officials, increase social inequality and environmental degradation, political instability and legitimacy crisis. (Gainsborough, 2006 and He, 2000)

Among anti-corruption mechanisms, ACAs are often seen as the only way to reduce widespread corruption because existing institutions are considered too weak for the task. The success stories about reducing corruption through ACAs in Singapore and Hong Kong set foundation to the establishment of ACAs to combat and prevent corruption. In 2005, the United Nations Convention against Corruption (UNCAC) came into force as the first legally binding anti-corruption framework to deal with the international problem of corruption crimes. UNCAC requires the existence of the two types of anti-corruption institutions: one to prevent corruption and one to combat corruption through law enforcement. (UNCAC, article 6 & 36) According to Meagher (2005), ACAs are "centers on separate, permanent agencies whose primary function is to provide centralized leadership in core areas of anti-corruption activity". (p.70)ACAs are diverse in terms of form and effectiveness because they reflect different contexts. Some have made great strides toward accomplishing their goals while others have fallen back. Some are national while others are local. Some are well integrated with other government agencies and interact well with other anti-corruption stakeholders, while others operate in isolation. While the number of ACAs worldwide is growing, 2008 OECD review of ACAs indicates more failures than successes. Why do states adopt ACAs though it is unlikely to succeed in reducing corruption? Helbrunn (2004) found out some reasons behind states' motivation to establish ACAs. First of all, states lack a real political intention to reform because government officers can gain greater economic benefits from systematic corruption. So establishing ACAs is to placate domestic calls for reform. Secondly, states need international investors and donors for their economic development. And since investors and donors require governments' greater effort to reduce corruption, governments establish ACAs to satisfy them. Helbrunn also reported that in the worst cases, ACAs were used as a tool to repress political rivals and members of the opposition or previous governments. In fact, empirical studies by Meagher (2004) and Helbrunn (2004) implied that there are certain conditions for ACAs to be successful. They are the momentum created by scandal and crisis; political, legal, and socio-economic conditions for good governance; legal tools to go after venal officials; independence from interference by the political leadership, resources (well-trained personnel and budget funding), reporting hierarchy, the presence of oversight committees; and the small size of a country.

Both in Vietnam and China, the governments have recognized corruption as a threat to their regimes and talked about their determination to reduce it. As a result, they have been taking a few initiatives to tackle corruption. In Vietnam, the anti-corruption legal framework has improved significantly over the past few years. Vietnam adopted the Anti-Corruption Law in 2005 focusing on corruption in public sectors and the National Strategy on Anti-Corruption to 2020 in 2009.Other corruption related regulations are 1999 Penal Code, 2003 Criminal Procedure Code, 2004 Law on Inspection, 2005 Law on Practicing Thrift and Fighting Waste, 2009 amended Law on Procurement.

The government is working on law on public investment, revising Law on Thrift Practices and Anti-Wastefulness and Land Law.(Le, 2012) Vietnam also ratified UNCAC in 2009. In terms of legal enforcement, there is no such an independent ACA in charge but several institutions have an anti-corruption mandate. The Central Steering Committee against Corruption was created by the 2005 Law on Anti-Corruption and previously chaired directly by the Prime Minister. However, it was brought back under the Communist Party in 2012. (Le, 2012) It is mandated to guide, coordinate, and oversee the Government's anticorruption efforts. In 2008, Steering Committees were created at the local level. The Government Inspectorate was created in 1956 but only began to have a clear corruption mandate in 2005. It functions as an Ombudsman and has an Anti-Corruption Bureau that is responsible for the investigation of corruption complaints. The People's Procuracy is in charge of prosecuting cases of corruption. The State Audit of Vietnam (SAV) is responsible for verifying the accuracy and legality of the state budget. Furthermore, Vietnam has had some institutional reforms aiming at combating corruption such as ratification of the International Covenant on Civil and Political Rights in 1982, renovation policy (DoiMoi) in 1986, the 1992 constitution amendment, public administration reform and the Grassroots Democracy Decree in 1998.

In China, the government has been trying to improve transparency in its system. Its corruption related regulations are Criminal Law focusing corruption in public sectors,1993 Unfair Competition Law dealing with corruption in private sectors, Article 41 of the Constitution protecting whistle-blowers, 2002 Government Procurement Law, 2003 Regulations on Combating Money Laundering by Financial Institutions, 2007 Regulations on Open Government Information, 2008 Tangible Construction Market - Anti-Corruption in Public Procurement, and 2010 new ethics code. (Trust Law, 2013)China also ratified the UNCAC in 2006. And it has been the host of the International Association of Anti-Corruption Authorities (IAACA) that supports the implementation of UNCAC. According to Manion (2004), The Chinese procuracy and the Committees of Discipline Inspection (CDI) are the agencies that enforce China’s anti-corruption laws. They have offices at all levels of China’s government. Formally, the Chinese procuracy that is accountable for the people’s congresses is in charge of investigation and prosecution of corruption. CDI under the communist party is in charge of corruption within the government. On the other hand, National Bureau of Corruption Prevention (NBCP) established in 2007 under the Ministry of Supervision is mandated to guide anti-corruption work in both the public and private sector. The Ministry of Supervision with both a national organ and local organs functions like an Ombudsman. National Audit Office (NAO) has used open auditing to investigate and expose cases of corruption. (Trust Law, 2013) Furthermore, China implemented e-governance to increase efficiency and accountability. It has websites for both national and local governments. And it also has special websites as well as 24-hour hotlines for the people to report

corruption. (Trust Law, 2013) Moreover, He (2000) reported reforms in many aspects initiated by the government to deal with corruption such as economic reform, political reform toward democracy, and administrative reform. China also implemented anti-corruption campaigns at both national and local level. (He, 2000) Finally, as an anti-corruption initiative by the new leaders, China is going to implement its first local integrated ACA in Hengqin New Area. (China Daily, 2012)

In spite of all the efforts by the governments and the communist parties, corruption in the countries was assessed to be serious with anti-corruption to be ineffective. According to the Vietnam Chamber of Commerce and Industry, 77 percent of businesses in Hanoi (highest percentage) and 12 percent of businesses in Binh Duong provinces (lowest percentage) bribed government officials. (Cited as Global Integrity, 2006) Vietnam's integrity scored 44 out of 100 for the effectiveness of national-level anti-corruption system, in which legal framework scored 52 and actual implementation scored 31, implementation gap scored 21. (Global Integrity, 2011) In 2012, Transparency International ranked Vietnam as the 123th out of 176 countries at the score of 3.1. According to Global Integrity Report (2011), China's integrity scored 64 out of 100 for the effectiveness of national-level anti-corruption system, in which legal framework scored 78 and actual implementation scored 47, implementation gap scored 31. In 2012, Transparency International ranked China as the 80th at the score of 3.9.

The above discussions show that the serious problems of corruption in Vietnam and Mainland China are caused by their communist institutional designs that are neither transparent enough nor properly checked and by their cultural and social values that endorse corruption. The discussions also point out that their current approaches to corruption that focus on enforcement through ACAs are ineffective. Why will the ACA model not work in the countries? What can the countries' leaders do to reduce corruption effectively? The paper argues that the ACA model is not suitable in the contexts of Vietnam and Mainland China because of a lack of the conditions for a successful implementation and that to deal with their specific corruption problems, the leaders can take a comprehensive approach that combines the ethnographic approach with the democratic legitimacy approach. The combination approach not only helps the countries reduce all kinds of corruptions but also takes into account the limitation of their communist political systems. Moreover, the two components of the combination approach can reinforce each other for more effectiveness. It is well known that transparency is the key for anti-corruption. Therefore, there is a hope for anti-corruption in authoritarian countries like Vietnam and Mainland China who are trying to be more transparent through democratic reforms. Moreover, this paper studies ACAs because it is the most popular anti-corruption mechanism to be preferred by systematically corrupted states including Vietnam and Mainland China. (McCusker, 2006) Finally, it is necessary to study Vietnam and Mainland China together because their similarities in politics, cultural and social values often make their leaders refer to each other.

Literature Review

Studies on remedies for corruption in Vietnam and Mainland China can be divided into four camps. However, it is important to notify that studies on Vietnam's anti-corruption are very limited. The first one approaches corruption from a moral perspective. The second camp calls for fundamental changes towards democratic governance in the countries. The third camp suggests converting economic special zones into special governance zones (SGZs) with a well-structured checking system within institutions and then spreading the model all over the countries. The forth camp argues that reducing corruption in the countries is very difficult because the leaders are not interested in making a grand institutional change; so, there is no hope for anti-corruption there. However, among the three possible remedies, the moral approach is not appropriate to deal with the multi-dimensional problem of corruption and the two other approaches directly challenge the sole rule of the communist parties, so, they are not accepted by the governments.

The representative of the first camp is Ma (2008). He studied on ACAs in China and found corruption happening within the agencies. Looking at the causes, the author concluded that "plenty of temptations coupled with a lack of supervision has made corruption a big issue in anti-corruption agencies, including law-enforcement, the legal system, and the judiciary." (p.158) He pointed out that the institutional design that guarantees the Party's absolute rule at the expense of the other institutions' autonomy and capacity allowed that happen. According to Ma, "the improper political interference also led to disappointment among anticorruption fighters and even their degeneration". (p.159) Therefore, it is important to promote and preserve adequate sense of personal integrity in anti-corruption agencies by further understanding ACAs.

In the second camp, Fritzen (2003) and Fu (2011) can be regarded as leading scholars. Fritzen assessed Vietnam's 2005 anti-corruption law by an institution approach. The author reviewed the studies that explain why contexts are so important to anti-corruption. The literature review showed three propositions. First, struggles over institutional redesign are characterized by conflict between powerful institutional actors. Second, these calculations of interest include both short- and long-term considerations, which may diverge. Finally, existing institutions and governance characteristics have a profound influence on reform efforts. Fritzen employed these propositions to explore the institutional context of anti-corruption in Vietnam. The author argued that organizational network decentralization, executive dominance and state-centrism structure the interests of the various political and bureaucratic actors and strongly influence the channels through which they will engage with the anti-corruption strategy. Fritzen found out that "Vietnam's authoritarian institutions affected the feasibility and sustainability of the country's anticorruption strategy". (p.93) The propositions gleaned from rational

choice institutionalism have helped to clarify the institutional constraints on the implementation of the anti-corruption strategy. On the other hand, Fu examined the two schools of corruption in China: the "trap" school and the "gap" school from a perspective of investigation. The "trap" school argues that there will be no remedy for corruption in China until fundamental political changes happen. On the other hand, the "gap" school argues that there is a wide gap between law and enforcement but this gap can be narrowed through enhanced disciplinary action and institutional innovation. Fu found that corruption is out of control at local level but central authorities are prepared and ready to change. However, according to Fu, options for China's future corruption are open. The author said that if China wants to combat corruption, supervision from other political parties and civil society, a large degree of freedom of the press and expression and an independent judiciary are necessary**.**

As the only scholar in the third camp, Wei (2000) suggested establishing SGZs as "a geographically limited area within a country, in which a comprehensive package of civil service reform, redefined role of government in the economy, enhanced rule of law, and enhanced citizen's voice, will take place". (p.1) From there, governments can spread the model all over the country. The model requires that in order to run a SGZ efficiently; some conditions have to be established. At the initial stage of the program, first of all, "political and fiscal support from the central government and international organization (the World Bank) is crucial". (p.1) Secondly, "a fair market mechanism should be used to allocate resources, to produce and procure public goods, to cut red tapes, to reduce requirement on permits and licenses on economic activities". (p.2) Thirdly, "the top officials of a SGZ should be chosen (by the central government or local election) from those with high caliber and integrity and civil servants should be recruited and promoted based on merit". (p.2) Fourthly, "civil servants are properly paid (close to their best private sector opportunity cost)". (p.2) Finally, auditing and investigation are performed on the efficiency and integrity of the civil servants and violations of law (including taking bribes) will be prosecuted after a due process. In the long run, it is required that "the improved tax base (through reduced arbitrary tax exemption by bribe taking officials and through increased investment and output in the zone) will generate more revenues to help pay the initial cost of raising civil servants' salaries". (p.2) Considering all these condition, Wei suggested that China should convert some of the existing special economic zones into SGZs.

Lastly, Manion (2004) is among those who see no hope in the possibility of anti-corruption in China. She argued that it is impossible for China to transform from a widespread-corruption system to a clean government like Hong Kong. To support her argument, she used a "Schelling-type tipping model" to create a theoretical framework in which clean government and widespread corruption are equilibria. That means once these equilibria are reached, it is very difficult for states to move from one equilibrium

to the other. From there, the author introduced implications for anti-corruption reforms in widespread-corruption countries. The first implication is to reduce corrupt payoffs through three strategies so-called enforcement, institutional design and moral education. The second implication is to change shared expectation by "coordinating expectations about cleaner government" and "boosting anti-corruption enforcement with reports from ordinary citizens" (p.22). However, the last implication tells about the problems when implementing these strategies in widespread-corruption countries, which reinforces the author's argument of the difficulty of anti-corruption in the countries. The problem with enforcement is that there are too many corrupt officers and even enforcers are also corrupted. Institutional design presents a problem of officials not wanting to change fundamentally. Moreover, it is very difficult to change expectation about corruption because there is always a doubt of government credibility. Next, the author discussed anti-corruption in Hong Kong to find out what made Hong Kong succeed in the transformation. Then she moved on discussing China's corruption and the problems of its anti-corruption enforcement. First of all, there are problems of organization and coordination among China's ACAs. According to the author, China's CDI prevents many communist party members from criminal punishment because CDI has the authority to decide what to do with wrongdoing officials, which often leads to less punishment. Another problem is the criminal justice system.

That is, the system allows official to face lower criminal standard than ordinary people for the same crimes. Moreover, the author also found that anti-corruption campaigns used as enforcement mechanisms are highly politicalized and in fact, could neither deter corruption nor enhance the rule of law. To reinforce her argument, finally, the author discussed the main differences between China and Hong Kong making anti-corruption reforms in China so difficult. They are the nature of ACAs, incentive structures that allows opportunities for corrupt acts and the possibility of significant institutional design.

Since the current approaches to corruption in the countries are neither appropriate to tackle corruption nor acceptable to the authoritarian regimes, any proposal for anti-corruption in the countries has to take all causes of corruption in the countries as well as the capacity of the governments into consideration to create a comprehensive and practical approach. At the same time, it has to help enhance political commitment to anti-corruption in the countries.

Theoretical Framework

This paper employs both the ethnographic approach and the democratic legitimacy approach to create a theoretical framework of a combining approach. It argues that combining the two approaches are necessary in order to tackle corruption in the countries comprehensively and practically.

The ethnographic approach provides a remedy for petty corruption endorsed by cultural and social values while the democratic legitimacy approach deals with grand corruption taking place in the environment where public institutions are not transparent enough or properly checked though institutional reforms based on consensus between the governments and their people. Therefore, the combining approach presents a comprehensive remedy that is more likely to work and be accepted by the countries' current leaders. Moreover, the ethnographic approach's means of human capacity development can create better domestic pressure for anti-corruption reforms which helps reinforce the effectiveness of the democratic legitimacy approach for more significant changes. On the other hand, more significant anti-corruption reforms through the democratic approach can result in more trust in government credibility among the people that encourages the people to change their expectation and social practice. In that sense, the combining approach creates a reinforcing circle known as the remedy for widespread corruption. Furthermore, in this theoretical framework, this paper identifies external pressure as an important factor that can help enhance political commitment to anti-corruption in the countries. The following discussion presents the details of the ethnographic approach and the democratic legitimacy approach.

Corruption from the ethnographic approach is seen as a part of a social interaction. From ethnographers' point of view, “social norms support interactions that outsiders see as corrupt but that the participants view as acceptable or even moral.” (Ackerman, 2010, p.4) It is often seen that “ordinary people condemn corruption at the elite level, but they themselves participate in networks that socially reproduce corruption.” (Ackerman, 2010, p.5) However, ethnographers argued that “social norms may be deeply embedded and self-reinforcing, but they do sometimes change…if a society is ever to build a legitimate democracy, they must change.” (Ackerman, 2010, p.6) The ethnographers also suggested that “more public awareness of the costs of payments whether labeled gifts or bribes could change behavior and increase support for reform.” (Ackerman, 2010, p.6)

Ackerman (2010) proposed the democratic legitimacy approach base on the argument that “one needs to have a realistic appreciation of the strains facing modern democracies that seek to justify their legitimacy. Corruption can undermine governments even if it aids market participants and supports traditional cultures. However, aggressive and punitive anticorruption campaigns can also undermine governments' ability to tap into the loyalty and good will of their populations and can poison the business environment.” (p.10) She suggests that “as long as political leaders have some interest in reform, anti-corruption policy can start with these areas of agreement and later confront the more contested dimensions of the problem.” (p.10) She also proposed some areas as following.

- Publication and easy public access to the constitution and to legal codes and statutes, regulations and decrees with the force of law, legal guidelines and practice manuals, and judicial opinions

- Standardized and transparent public accounting for funds by the government under the control of both an internal audit office and an independent external audit body

- Foster effective oversight of government activity by removing press restrictions and sponsor training in investigative journalism, making it easy to establish and finance civil society organizations

- Transparent and competitive processes for large scale procurement that take realistic account of the occasional need for sole-source procurement (the negotiations should be transparent with the focus on the government obtaining a high quality result at a good price. Purchase as much as possible by shopping in private markets in competition with private buyers rather than using special purpose orders. Support international efforts to provide benchmark prices for common procurement needs)

- Enforcement of bribery laws against major offenders both in and outside of government. Special efforts to apprehend those involved in corruption connected with organized crime. Opportunities for individuals and businesses to lodge complaints about demands for bribes or other favors and to have these complaints are expeditiously dealt with through an independent and well-funded Ombudsman.

- A diagnostic study of the rules, regulations, and licensing requirements facing individuals and businesses to isolate reforms including repeal that might both improve government functioning and reduce corruption.

- Improvements in the pay, recruitment and working conditions of civil servants and the judiciary combined with strengthened conflict-of-interest rules and internal monitoring of public service delivery.

- Outlaw the buying of individual votes, and clarify the system of campaign finance, the role of lobbyists, and the private financial interests of politicians to limit conflicts of interest.

- (Pp.12-13)

The author also emphasized that any reform agenda must be consistent with the goal of strengthening state capacity and accountability.

Can the ACA Model Function Effectively in Vietnam and Mainland China?

This section is devoted to analyze the status of the conditions for the anti-corruption mechanisms to be successful. To test the applicability of ACAs, the momentum created by scandal and crisis; political, legal, and socio-economic conditions for effective governance; legal tools to go after venal officials; independence from interference by the political leadership, resources (well-trained personnel and budget funding), reporting hierarchy, the presence of oversight committees; and the size of a country will be checked under the countries' contexts. Recently land-related corruption scandals have been dominated in Vietnam's public scene. This year in April, a land-related protest took place in Hung Yen province. Witnesses reported about 1000 policemen tear gas to 3000 farmers. A similar protest happened in Nam Dinh province. It is said that most of recent complaints are related to land management. Experts have been calling for a land reform to deal with the land management crisis. However, the government announced that there would not be any major change to Vietnam's land policy in the coming revised constitution. Although Vietnamese leaders recognized corruption as the most serious problem that Vietnam is facing and expressed their determination to combat it by all means, the first move taken was to put the Anti-corruption Committee under the control of the Communist Party. It can be seen that the government has no will to establish an independent agency to deal with the corruption problem. Moreover, researches on corruption in Vietnam have been almost avoided. On the top of all, Vietnam does not have political, legal, and socio-economic conditions for effective governance. Governance is a new concept in Vietnam. In Vietnam, governance is known as state-management that does not include citizens, firms, civil society organizations, professional associations, etc. On the other hand, Vietnam has 63 provinces that have different level of development and corruption; a central anti-corruption agency will have difficulty to manage them all. All in all, the conditions for a successful ACA do not seem to exist in the current context of Vietnam.

Like Vietnam, China has a perfect momentum to step for a big innovation in anti-corruption. This momentum is created by violent protests over corrupted officers and corruption scandals related to top officers. Chung, Lai and Xia (2006) reported the incidents of collective protest have dramatically increased in the past twelve years. The protests were also said to become more violent in recent years. And violent incidents appear to be growing nationwide. Urban workers have participated in collective protests for at least four different reasons, including economic difficulties caused by unemployment or bankruptcy, delayed salary payments, excessive taxation and surcharges, and illegal financial scams.

For rural participants in collective protests, the most important reasons have been disputes over land division and appropriation, followed by excessive taxation and irrigation rights. Moreover, recently Bo Xi Lai's corruption scandal that is on trial, Bloomberg News's report on Xi Jinping's family wealth and The New York Times's investigation report on Wen JiaBao's family wealth that are rejected by the Chinese government have put huge pressure on China's new leaders. In term of legal tools to go after officers, in China, both the central and local government, as well as the Disciplinary Commission of the Chinese Communist Party, has set up anti-corruption whistle blowing hotlines in the last few years. Both the Administrative Supervision Law and the CCP Internal Supervision Rules set out rules for whistle blowing. According to official data disclosed in 2008, more than 70% of the criminal abuses of public power offenses committed by governmental officials have been prosecuted based on whistle blowing tips. (Cited as Mysong, Bing and Boeringer, 2011) Rewards may be granted to whistleblowers, as provided under the relevant law and regulations such as the Administrative Supervision Law and its Implementing Regulations. In accordance with the relevant laws and regulations, whistleblowers are to be strictly protected and retaliation is prohibited. In reality, however, protection of whistleblowers is reportedly weak and retaliation not uncommon. According to the Supreme People's Procuratorate, more than 70% of whistleblowers are retaliated against, of which the majority cannot find any effective remedy from the government or judicial authority. The methods of retaliation range from de facto demotion and illegal detention to assassination. Moreover, China's political, legal, and socio-economic conditions for good governance are far from enough. In China, governance is known as state-management that does not include citizens, firms, civil society organizations, professional associations, etc. though China's civil society has achieved significant developments. Currently, several agencies are in charge of anti-corruption in China but China's politicians dominate them. Ma discussed why ACAs in China are corrupted as above. However, Ma's reasons are not enough to explain the failure of ACAs in China. Su (2007) pointed out that China's ACAs have overlapping jurisdictions and an unclear division of labor. At the same time, anticorruption goals are subject to other goals (such as short-term economic growth rate) and mild party punishments substitute harsh legal penalty. In term of anti-corruption strategy, leadership in Mainland China only realizes the importance of a wholesome anticorruption strategy in recent years. The rapid economic growth raised serious problems in terms of moral standard and weak institutions. Without having paid timely and sufficient attention to education and reorganization of procedures, Mainland China's anticorruption reform has been largely regarded as "failed". Moreover, there is no independency from the political leadership. The central Commission for Discipline Inspection is staffed by eight deputies and 120 senior members and headed by a Politburo Standing Committee member. (Cited as Thornten, 2008) Last of all, China is a huge country with 23 provinces, 5 autonomous regions and 4 municipalities, which makes it very difficult for central ACAs to manage.

Remedies for Corruption in Vietnam and Mainland China

Combining the ethnographic approach and democratic legitimacy approach, this paper suggests that through human capacity building, the governments and anti-corruption activists can make the people realize the costs of pay-offs and then discourage them to involve in networks that socially reproduce corruption. Especially, offering a chance for the people to better understand administrative procedures and laws will make it possible for them to avoid and report corruption acts. As a result, tension against corruption will be higher and the people's demand for reform will be greater. If the governments do not want to lose popular support, it will have to initiate deeper reforms. In order to further enhance the governments' political will; this paper suggests that international donors and investors can play an important role. Wei (2000) pointed out two kinds of international pressure that can be brought to bear on the corruption problem. First, international organizations such as the United Nations Development Program, the World Bank, the International Monetary Fund, the Asian Development Bank, and the like, can provide persistent moral persuasion as well as technical assistance to induce or help countries in their fight against corruption. Various conferences on good governance and corruption organized by the UNDP, the World Bank and so on are useful. Cutting off loans or threatening to cut off loans by the IMF or World Bank on the ground of corruption in recipient countries may be even more effective on the margin in some cases. The second channel is concerted international effort to criminalize the offering of bribes by multinational firms to host countries' officials. However, corruption-prone foreign officials do not feel enough pressure to change their behavior even if they are genuinely interested in attracting foreign investment into their countries. Moreover, they are more likely resist demand of bribes if they can be confident that they will not lose business to their competitors as a result. Today Vietnam faces business opportunity competition with Myanmar as well as the problem in Spartly Islands and when Mainland China demands high economic development rate to protect its legitimacy, foreign actors can make greater contribution in anti-corruption in the countries. International pressure for anti-corruption activities is not the driving factor to the governments but together with the people's attitude change to corruption, it will be important to make the leaders commit to anti-corruption more.

In terms of corruption in the private sector, it has not yet been prioritized in Mainland China and Vietnam. In Vietnam, private corruption is still excluded in all anti-corruption regulations. In China, it is criminalized but the thing like gift-giving in business or in other areas that is considered as a corrupt act in other countries has not yet been regulated. Therefore, it is important to make the governments and individuals recognize the negative impacts, irrationality and un-ethnicity of private corruption. For that, NGOs can advocate for better corporate governance and corporate social responsibility. This also reflects the combining approach.

Conclusion

The conditions for ACAs to be successful under the current contexts of Vietnam and Mainland China are too weak or even missing; so ACAs are unlikely to be successful there. The approach combining ethnographic and democratic legitimacy elements can on one hand, reduce petty corruption and gift-giving by raising public awareness on the cost of bribery through research publication and human capacity development activities by civil society and transnational networks and on the other hand, reduce grand corruption through domestic and international pressure. Since Vietnam and China are different in terms of economic and social development, they should start with different areas of change.

The originality of this paper lies in its combining approach and academic and practical analysis stand. Anti-corruption scholars proposed different approaches from various perspectives but so far no one combines different approaches to create a more comprehensive one to deal with corruption. On the other hand, most scholars studying remedies for corruption in Vietnam and Mainland China did not look for possibilities under the current political and social contexts in the countries but go beyond what the communist parties are expected to make consensus on. This paper takes a more practical stand to find out which approach to corruption suits best the current contexts in the countries in a rational manner; so; the combining approach is more likely to be accepted by the governments. However, the arguments are not tested with primary data, which is the limitation of this paper. For a future research, an empirical study on the combining approach is highly recommended.

References

Ackerman R. S. (2010),Corruption: Greed, Culture and the State, Yale Law Journal Online, 120, pp. 125-140. Yale Law & Economics Research Paper No. 409. Retrieved on July, 17th, 2012 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1648859.

ChinaDaily(2012),Offices to Unite in Fight against Graft, Retrieved on January 28th, 2013 from http://www.chinadaily.com.cn/china/2012-09/11/content_15748648.html.

Chung J. H., Lai H. and Xia M. (2006), Mounting Challenges to Governance in China: Surveying Collective Protestors, Religious Sects and Criminal Organizations, The China Journey, 56, pp. 1-31.

Gainsborough, M. (2006), National Integrity System Country Study, Transparency International, Berlin.

Global Integrity (2006), Retrieved on June, 3rd, 2011 from http://back.globalintegrity.org/reports/2006/vietnam/notebook.cfm.

Global Integrity (2011), Retrieved on January 27, 2013 from http://www.globalintegrity.org/report/findings.

He, Z. (2000), Corruption and anti-corruption in reform China, Communist and Post-Communist Studies, 33, pp. 243–270.

Heilbrunn J. (2004) Anti-Corruption Commissions Panacea or Real Medicine to Fight Corruption?, World Bank Institute Retrieved on November, 6th, 2011 from http://siteresources.worldbank.org/WBI/Resources/wbi37234Heilbrunn.pdf.

Fu, H. (2011), The Upward and Downward Spirals in China's Anti-corruption Enforcement. Retrieved on July, 17th, 2012 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1883348.

Fritzen, S. (2006), Beyond 'political will': How institutional context shapes the implementation of anti-corruption policies, Policy & Society, 24(3), pp. 79-96.
Jain A. K. (2011), Corruption: Theory, Evidence and Policy, CESifo DICE Report.
Khantri N., Johnson J. P. and Ahmed Z. (2003), A Two Stage Model of Cronyism in Organizations: A Cultural View of Governance, Corruption and Governance in Asia, New York: Palgrave Macmillan, pp.61-81.
Le H.H (2012), Vietnam's Fight against Corruption: a Self-defeating Effort?, East Asia Forum, Retrieved on January 28th, 2013 from ***http://www.eastasiaforum.org/2012/11/06/vietnams-fight-against-corruption-a-self-defeating-effort/****.*
Ma, S. K. (2008), The dual nature of anti-corruption agencies in China, Crime Law Soc Change, 49, pp. 153–165.
Manion M. (2004), Corruption by Design: Building Clean Government in Mainland China and Hong Kong, Harvard University Press, Cambridge, Massachusetts and London, England.
Meagher P. (2005), "Anti-corruption Agencies: Rhetoric versus Reality", The Journal of Policy Reform, 8(1) pp. 69–103.
Monteith, B. (2009), The Bully State: The End of Tolerance, The Free Society.
Mysong W., Bing Y. and Boeringer C. H. (2011), Blowing the Whistle on Corruption in the U.S. and China, Corporate Compliance Insights, Retrieved November 27, 2012 from http://www.corporatecomplianceinsights.com/blowing-the-whistle-on-corruption-in-the-u-s-and-china/.
Nojonen M. (2003), The Competitive Advantage with Chinese Characteristics-The Sophisticated Choreography of Gift-Giving, Corruption and Governance in Asia, New York: Palgrave Macmillan, pp.107-129.
OECD (2008),Specialized Anti-corruption Institutions: Review of Models– ISBN-978-92-64-03979-7
Segon M. and Booth C. (2010),Managerial Perspectives of Bribery and Corruption in Vietnam, International Review of Business Research Papers, 6(1), Pp.574-589.
Su, L. (2007), "Corruption by design? A comparative study of Singapore, Hong Kong and mainland China", Discussion Papers, The Policy and Governance Program, the Crawford School of Economics and Government.
Transparency International (2012), Corruption Perception Index, Retrieved on January 26, 2013 from http://www.transparency.org/cpi2012/results.
Thornten J. L, 2008, Long Time Coming The Prospects for Democracy in China, Foreign Affairs, 87 (1), pp. 2-22.
Trust Law (2013), Anti-corruption Profile-China, Retrieved on January 28th, 2013 from http://www.trust.org/trustlaw/country-profiles/good-governance.dot?id=f6914514-db9d-437c-b7a6-2a4c88453881.
United Nations Convention against Corruption (2005), Retrievedon June, 3rd, 2011 from http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf
Wei, S. J. (2000), Special Governance Zone: A Practical Entry-Point for a Winnable Anti-Corruption Program. Retrieved on July, 17th, 2012 from http://www.brookings.edu/~/media/research/files/papers/2000/9/24development%20wei/20000924.pdf

Author's Profile

Bui Thi Thu Sang

Bui Thi Thu Sang is currently a master candidate at Graduate School of Law, Kyushu University. She specializes in comparative politics and public administration in Asia. Coming from Vietnam where the problem of corruption is serious, she always has a strong interest in anti-corruption. At undergraduate level, she wrote a graduation thesis entitled "The Status and Future Direction of the Fight against Transnational Bribery Crime under International Law and Soft Law: Vietnam as a case study". Recognizing the limitations of her own undergraduate research, she decided to continue doing research on corruption in Vietnam and even broadened her research scale to corruption in authoritarian countries. Besides, she is also doing research on Japanese politics and EU governance. She had chances to present her papers at several international academic conferences on human security, Asia Pacific, Asian governance, EU in Japan, Hong Kong, China, Vietnam and the Philippines. She got an honorable mention at Asia Pacific EU Center Graduate Students Conference. She hopes to continue researching and working to reduce corruption in Vietnam and other countries after graduation.

Towards Fighting Corruption: The Role of Corporations

Mohammad Rafiqul Islam Talukdar
Center for Decentralization and Governance Society (CDG)
Agargaon, Dhaka-Bangladesh
rafiqul.talukdar@gmail.com

ABSTRACT

*The study calls attention to the importance of corporate explicit movement for combating corruption given the fact that corruption undermines fair competition, increases business operational costs, discards corporate reputation, diverts essential public resources away from their coherent uses. Certainly, this challenging posture requires a vision-driven strategic framework allowing the corporate leaders to see the problem on a system perspective, and so to stress equally on supply side, demand side and social side of the problem. Importantly, the study follows here focused synthesis method in an opportune fashion, while it uses SWOT analysis as a supportive technique. And it responds to the concerns - why is the current paradigm of CSR (*2.0*) aligned with the fighting corruption? - And how can corporates go robustly so as to make here difference?*

Keywords Corporate, Social, Responsibility, Corruption, Ant-corruption, Fighting, Combating, Focused-Synthesis, SWOT

1. INTRODUCTION

Corruption poses a serious governance, corporate and development challenge. In general, corruption erodes the institutional capacity of governments and destabilizes the democratic values, discourages investment, undermines fair competition, increases business operational costs, discards corporate reputation, diverts essential public resources away from their rational uses and damages development efforts, all of which together imposes direct costs on society and tailors the sufferings of the mass-people. In addition, studies - for instance, the HDR 2009 - support that our world is extremely unequal that makes obvious the huge differences in human development, while corruption and unfair distribution[1] of resources, public services and opportunities across and within countries are the basic ingredients of the disparity in human development.

[1]Unfair distribution of resources, public services and opportunities is also resultant from corruption.

There are, however, growing recognitions in governments all over the world to integrate fighting corruption into their governance agenda. Unlike the corporate sectors, the development partners, basically multilateral and bilateral donors, seek to enhance equity, transparency and accountability in the development works. Hills et al.(2009) identifies that NGOs such as Transparency International (TI) and Global Witness exert influence through advocacy efforts, corruption indices, and broad awareness building, while bilateral and multilateral efforts like the U.N. Convention Against Corruption, the Organization for Economic Cooperation and Development (OECD), and the World Bank Institute (WBI) have heightened global commitment to anti-corruption work.

The 2009 study also reveals that corporations are a significant part of the problem as the typical source of bribes, and they could benefit measurably from progress toward solutions - particularly in terms of reduced costs, greater operational efficiency, and improved reputation. Although some companies seek tighter controls on bribery to ensure compliance with existing anti-corruption laws, proactive and effective approaches to addressing the overall problem of corruption are not widespread.The study, however, argues that the anti-corruption field offers a major opportunity for strategic corporate social responsibility (CSR) programs to tackle an issue that is inherently linked with both corporate and societal interests.

This study strengthens the Hills et al. (2009) study, and emphasizes the importance of corporations to be inclusively move toward combating corruption. The current study focuses explicitly on the triangulation approach of anti-corruption given the call for supply and demand sides enforcements and social pressure. The study follows here focused synthesis method[3] in an opportune fashion, while it uses SWOT analysis as a supportive technique. And it responds to the concerns - why is the current paradigm of CSR (2.0) aligned with the fighting corruption? - and how can corporates go robustly so as to make here difference?

CSR 2.0 and Fighting Corruption

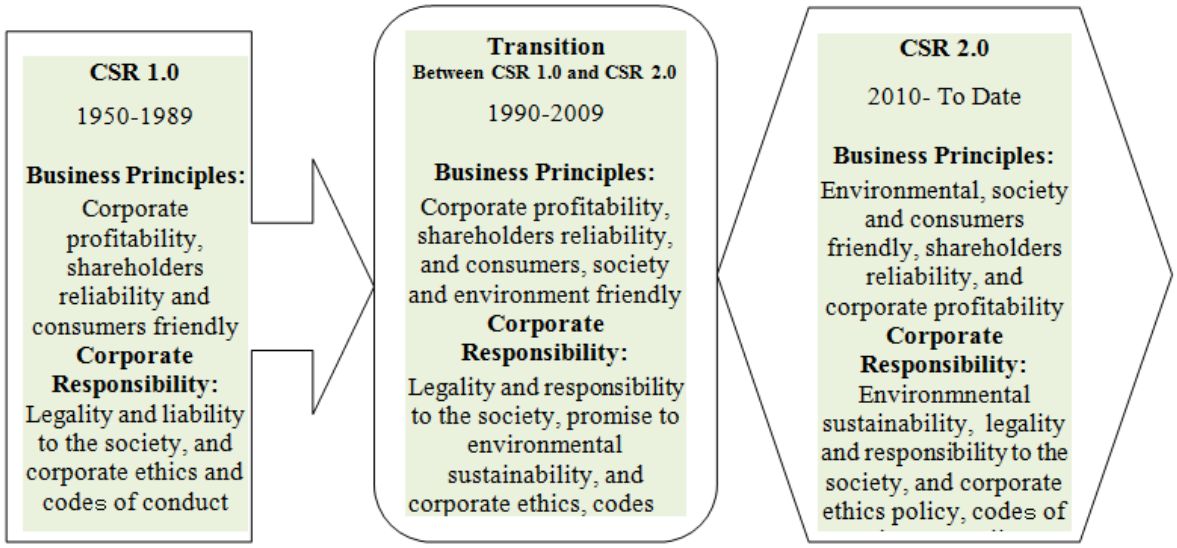
A 2010 write-up of Visser points out that defensive, minimalist responses to social and environmental issues are replaced with proactive strategies and investment in growing responsibility markets, such as clean technology.

[2]The study produced a splendid document title "Strategic CSR: A call to action for corporations" published in May 2009 - authored by Greg Hills, Leigh Fiske, Adeeb Mahmud –under FSG Social Impact Advisors at Boston, Geneva, San Francisco and Seattle with the support from Merck Company Foundation and in collaboration with Ethics Resource Center.

[3]Focused Synthesis allows collecting and documenting information as well as data from a range of sources as diverse literature review, researcher's personal experience, web and media evidence, legislative hearing, court verdict, staff memorandum, unpublished project or study document, anecdotal evidence and story, citation or discussion with experts, practitioners and stakeholders (Talukdar, 2012).

Reputation-conscious public-relation approaches to CSR are no longer credible, and so companies are judged on actual social, environmental and ethical performance. Now the ultimate purpose of business is to serve society, through the provision of safe, high quality products and services that enhance our well-being, without eroding our ecological and community life-support systems.

As such, making a positive contribution to society is the essence of CSR 2.0[4] – not just as a marginal afterthought, but as a way of doing business. In fact, CSR 2.0 is about designing and adopting an inherently sustainable and responsible business model, supported by a reformed financial and economic system that makes creating a better world. Figure1 shows the transformation of CSR 1.0 to CSR 2.0.



Source: © the Author

Figure 1. Transformation of CSR Paradigm

As CSR 2.0 is concerned about sustainability and responsibility, it must comply with the global concern about corruption. According to Hills et al.(2009), corruption is estimated to cost $2.6 trillion annually, an amount equal to more than 5 percent of global GDP. Each year, over $1 trillion is paid in bribes; not only do these payments undermine fair competition and affect the profitability of businesses operating globally, but they also divert crucial public resources away from their legitimate uses, denying citizens essential public services such as education, clean water, and health care. United Nations (2010) witnesses that corruption may take in many forms with varying degree of intentions from the minor use of influence to institutional bribery, and it may not be confined just into financial gain, rather leads to non-financial advantages as well. Transparency International (2010) denotes corruption as the abuse of entrusted power for private gain - demand side - where corporations play a vital role as supply side.

[4]According to Visser (2010) there are five principles that make up the DNA of CSR 2.0: Creativity , Scalability, Responsiveness , Glocality and Circularity.

Mehra and Agbool (2011) points out that company compliance programs should not simply be seen as a means of reducing liability and risk; they are also critical components of a company's CSR Policy. The reality is that corruption should and does have its costs, and not just in situations where companies get caught. Bribery distorts competition and rewards those who cannot compete in an open and fair market.

Greg Andres, Department of Justice (DOJ) representative, gave a statement before the recent House Judiciary Committee hearing on the Foreign Corrupt Practices Act (FCPA)**:** "Corruption undermines the democratic process, distorts markets, and frustrates competition. When government officials, whether at home or abroad, trade contracts for bribes, communities, businesses and governments lose; and when corporations and their executives bribe foreign officials in order to obtain or retain business, they perpetuate a culture of corruption that we are working hard to change."

According to United Nations Global Compact, "Corruption is now recognized to be one of the world's greatest challenges." An analysis of the Corruption Perceptions Index 2012 argues, "Corruption is a major threat facing humanity. Corruption destroys lives and communities, and undermines countries and institutions. It generates popular anger that threatens to further destabilize societies and exacerbate violent conflicts".

The concerns for ethics and standards in public life, and strategies to control corruption are now almost global and central to democratic governance and management of public services (OECD, 1999 & 2000; Hoddes et al., 2001). Citizens and service users expect public officials, whether elected, appointed or employed, to serve the public interest with fairness, and to manage public resources properly on a daily basis (Larbi, 2007). Therefore, a systematic focus of corporations on combating corruption with inclusion, cohesion and accountability can improve the coherence, quality and effectiveness of the new paradigm of CSR. As shown in figure-1 corporate ethics policy, codes of conduct, compliance monitoring and fighting corruption are now to be inbuilt with the corporate responsibility, while these have seen as converging interest with the sustainability of human development and exclusion from poverty and rights. In today's world, there are crucial links between corruption and human rights violation, poverty, exclusion, environmental degradation, vulnerability and conflict.

Fighting Corruption as Corporate Strategy

Porter and Kramer (2006) argue strategic CSR efforts should target issues that are of high importance to a company's core business strategy and operations and also have a meaningful benefit to society. While traditional CSR efforts focus on the tension between business and society, fighting corruption

presents an opportunity to focus instead on their interdependence in order to create shared value.

Importantly, global movements against corruption - Global Witnesses (GW)'s campaign against corruption[5], Transparency International (TI)'s National Integrity System framework, World Bank Institute (WBI)'s Business Fighting Corruption portal, U.N. Convention Against Corruption (UNCAC), the United Nations Global Compact (UNGC), the Organization for Economic Cooperation and Development (OECD), World Economic Forum (WEF)'s Partnering Against Corruption Initiative (PACI), the Extractive Industries Transparency Initiative (EITI), Merck Company Foundation's initiative with the Ethics Resource Center (ERC), and a joint publication of Transparency International, International Business Leaders Forum, and the United Nations Global Compact title Business against Corruption: A Framework for Action - have made almost all countries and a number of corporations agreed on to fighting corruption collaboratively, more strategically and systematically.

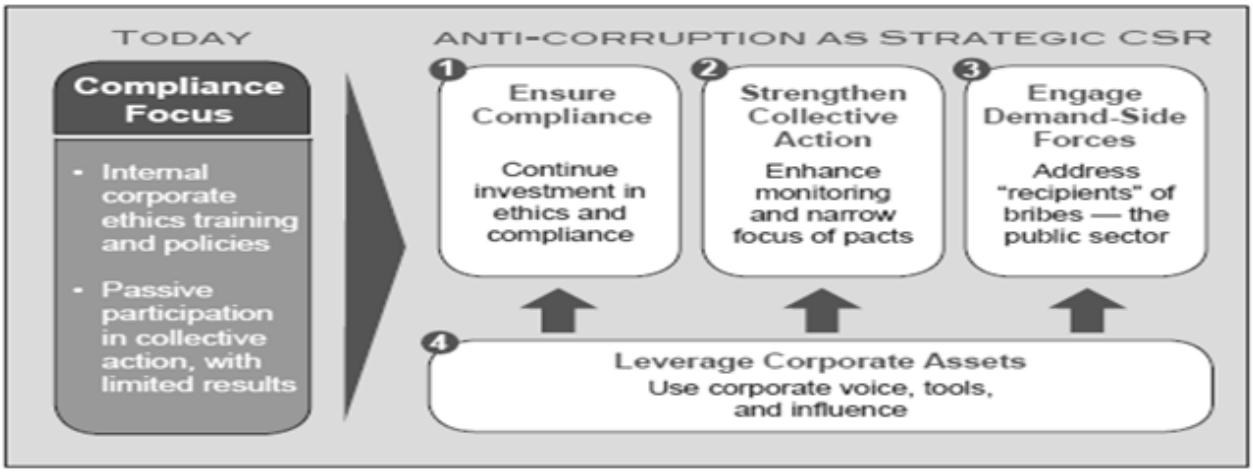
Yet many of the corporations see corruption as a legal, political and risk-management problem and limit their efforts to corporate ethics training, codes of conduct – a tailor-made document for staff integrity, and a minimal compliance-driven approach - just adaptation to the global compliance. Unlike other philanthropic, social and environmental concerns, corruption that costs business and society much through direct and indirect way has got less attention to the corporate culture, and so the corporate-wide anti-corruption drives are insufficient in-terms of scale and visibility.

Hills et al.(2009) acknowledge that corruption has unique qualities that distinguish it from other social problems. The paradox of corruption is that while it is happening everywhere, it is rarely seen. The act of bribery itself is not directly damaging to lives or the environment, but the resulting outcomes can have devastating effects on competition and human development. Because of the unique and substantial threat that corruption poses to both business and society, corporations should begin viewing the issue through the lens of strategic corporate social responsibility. Certainly, a comprehensive approach to fighting corruption requires a focus on the demand side as well[6]. However, corporations typically shy away from this approach, as it implies being critical of a government that is often a key customer or stakeholder in its business activity.

Hills et al. further argue that despite the salient differences between corruption and other social issues, multinational corporations need to be sophisticated players in the anti-corruption movement, where

[6]One corporate representative, however, says, “I have my doubts about how effective companies can be on the demand side. There are certainly limitations in terms of time and resources and the acceptability of such activities. The best way to cut demand from the public sector is to make it clear that there will be no supply. Making sure that we don't pay bribes is how we deal with the problem.”

companies are likely to work hand in hand with leading anti-corruption players and governments to help ensure that bribery remains an exception that is harshly regulated rather than a rule. Collective action agreements will be focused, effective, and routine. Corporate anti-corruption departments will be commonplace and staffed with experts familiar with external, multi-stakeholder initiatives. To catalyze this movement, authors call for corporations to embrace anti-corruption work as strategic CSR. Here, a step change is needed, with corporations moving from narrow compliance-focused approaches to broader roles that maintain an emphasis on compliance as well as increased proactive, external, and more comprehensive efforts as documented in the figure-2.



Source: Hills et al., 2009:39

Figure 2 Four Paths to Fighting Corruption

The current round study on combating corruption suggests that corporations' involvement for tackling corruption requires a vision-driven strategic framework allowing them to see the problem as a system perspective, and so to stress equally on supply side, demand side and social side given the SWOT analysis[7]. The study reveals that corporations need to set out forums so as to frame enhanced understanding and consensus among themselves on why and how to work more strategically and coherently on the integration of combating corruption in the strategic CSR. In addition, the research gives emphasis to the linking context – collaboration across private, public and civil society – of combating corruption so as to generate more effective and durable results.

[7]Strengths and weaknesses analysis of internal environment and opportunities and threats analysis of external environment.

Table 1. SWOT Analysis

Internal Analysis	Strengths	Weaknesses
Corporations	1. Resources 2. Corporate willingness 3. Ethics policy, codes of conduct and compliance monitoring are already inaction	1. Fighting corruption against key government actors, while maintaining a strong business presence is perceived to be risky 2. To date, corporations have paid much attention to labor, stakeholders and environmental issues but less attention to anti-corruption agenda
External Analysis	**Opportunities**	**Threats**
Social, Economical, Political and Institutional Perspectives	1. The current paradigms of CSR 2.0 and capitalism as well as leadership 3.0 are aligned with combating corruption 2. The concerns for corporate ethics and strategies to control corruption are now almost global 3. The cost of corruption outweighs the investment for fighting corruption 4. Existence of strong civil society movement 5. Presence of strong civic response	1. Limited corporate-wide movements till to date 2. The paradox of corruption is critical: It is happening frequently but it is rarely seen or punished

Source: © the Author

Table1 shows that strengths outweigh the weaknesses, while opportunities prevail over the threats. So the SWOT perspective for crafting the corporate strategic framework with strategic CSR lens for fighting corruption demonstrates virtual strengths of corporations and clear-cut opportunities in external environment.

Table 2. Corporate Strategic Framework for Fighting Corruption

Leverage Corporate Resources		
Supply side	**Demand side**	**Social side**
• Corporate ethics policy or guidelines, and codes of conduct • Compliance monitoring and enforcement, and transparency and accountability • Change management that requires capacity to think (reflexiveness or critical thinking) at both organizational or individual levels rather than just ability to follow rules (Collins, 2006) • Professional training, knowledge building and sharing • Best practices and lessons learned • Making it clear that there will be no supply for bribes	• Help build anti-corruption corporate forums and collective actions and consensus • Influencing legislation – help build up anti-bribery policy and guidelines, advance compliance monitoring and enforcement mechanisms globally, regionally and locally • Help promote global, regional and local institutional arrangement for fighting corruption • Help governments develop public management ethics policy or guidelines, codes of conduct • Help governments reinforcement of public accountability and transparency mechanisms, for instance, disclosure of public office holders' assets, liabilities and conflict of interest, and ensuring free press and electronic media and people's access to public information • Help governments sustain quality professional training for public officials, and knowledge building and sharing initiatives for elected officials • Help goverments build up public performance measurement and reporting system with *Key Performance Indicators (Taylor, 2007)* • Help governments adapt best practices and lessons learned	• Help build up strategic public, private and civil partnership for fighting corruption • Policy Advocacy- organizing local, regional, or global workshops and seminars with engagement of academics, practitioners, civil society, government officials, politicians and private sector • Help keep up research and publication on local, regional, or global good governance and anti-corruption issues with increased engagement of youth researchers • Support global movements against corruption • Help advance global, regional and local bridging youth leadership programmes • Help civic virtue progrmmes at school and civic awareness on anti-corruption programmes • Help mentor local companies on anti-corruption efforts by bringing financial management, legal compliance, and technical-assistance skills

Source: © the Author

Conclusion

Corruptions not only erodes trust in democratic governance and institutions but also discourages investment, destabilizes corporate governance and ethics and forces cut back development – the result of which together pulls down the human and civilization progress. Notwithstanding a 1998 study of

Florini observed governments would increasingly answer to the call for transparent governance and easy public access to all kinds of official government information. Besides, this study notices, over the span of last decade, Transparency International, Global Witnesses, Ethics Resource Center, the World Bank Institute, the U.N. Convention Against Corruption, the United Nations Global Compact, the Organization for Economic Cooperation and Development, World Economic Forum, International Business Leaders Forum, and Merck Company Foundation all together have made significant progress in getting corporations agreed for fighting corruption explicitly. Yet corporate leaders cannot solve the problem alone as corruption is a multidimensional and sophisticated problem. Therefore, the anti-corruption movement has tended to be considered part of corporate governance agenda (supply side response) as well as political governance reform process (demand side response) and social governance initiatives (development partners and civil society response).

Notwithstanding this study notices that there is now time to shift from reserved demand side response to explicit and strategic corporate social responsibility towards fighting corruption as stated in figure-2 and table-2. Importantly, corporations need to get on forums and strategic public, private and civic society partnerships so as to frame enhanced understanding and consensus among themselves and with other key players or stakeholders on why and how to work more strategically and coherently for combating corruption. Finally, in order to overcome the challenges inherent in this type of responsibility[8], they must share and analyze their experiences, build and share knowledge, and help grow up intellectual avenues like International Conference on Corporate Social Responsibility and Sustainable Development.

References

Collins, P. (Guest ed.) (2006). Symposium on Bridging Public and Private Ethics at Work. Public Administration and Development, Vol.26. Pp. 93-98.
Florini, A. (1998). The End of Secrecy. Foreign Policy, Vol.111, Pp.50-63.
Hills, G., Fiske, L., & Mahmud, A. (2009). Strategic CSR: A call to action for corporations. Boston, Geneva, San Francisco and Seattle: FSG Social Impact Advisors.
Hoddes, R., Banfield, J., & Wolfe, T. (eds.) (2001). Global Corruption Report 2001. Berlin:TI.
Larbi, G. (2007). Between Spin and Reality: Examining Disclosure Practices in Three African Countries. Public Administration and Development, Vol.27. Pp. 205-214.
Mehra, A., & Agbool, A. (2011, July 1). The Corporate Responsibility to Prevent Corruption. Forbes.com.
OECD (1999). Public Sector Corruption: An International Suvey of Prevention Measures. Peris :OECD.
OECD (2000). Trust in Government: ethics Measures in OECD Countries. Peris :OECD.
Porter, M., & Kramer, M. (2006, December). Strategy and Society: The Link between Competitive Advantage and Corporate Social Responsibility. Harvard Business Review.

[8]Responsibility is literally what it says – our ability to respond. To be responsible is to be proactive in the world, to be sensitive to the interconnections, and to be willing to do something constructive as a way of giving back. Responsibility is the footprints we leave in the sand, the mark of our passage. What tracks will you leave? - Wayne Visser)2005) in his book Business Frontiers .

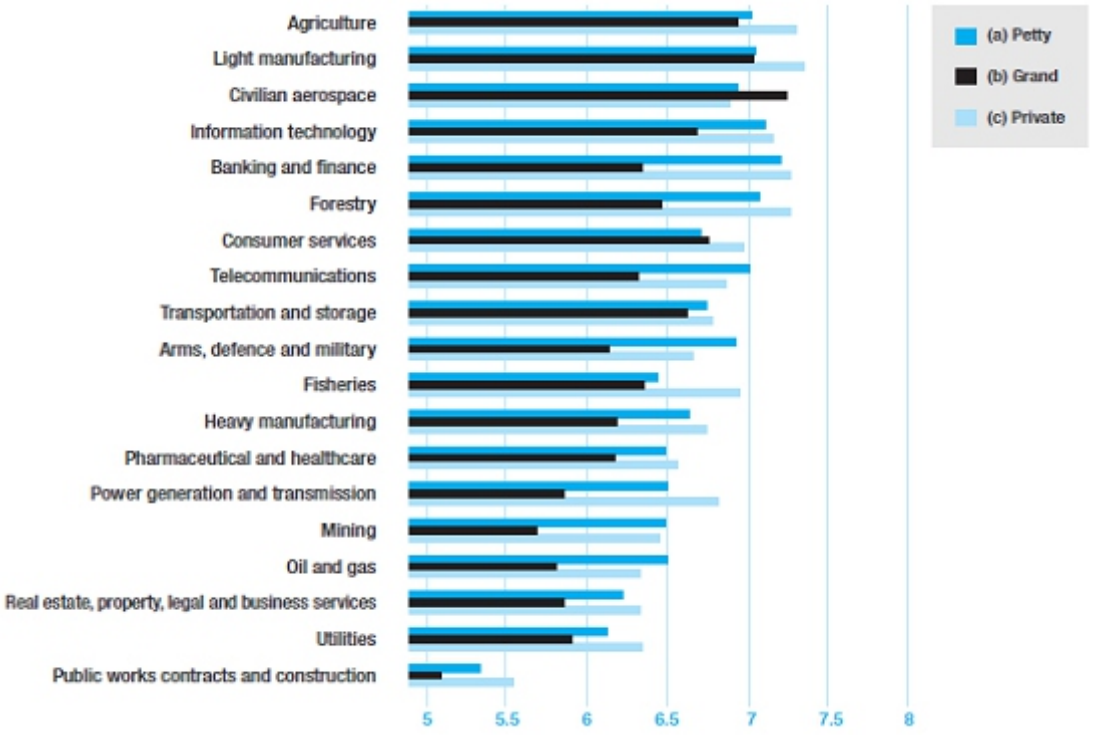
Talukdar, M.R.I. (2012). Mobile Communications and Fighting Corruption. *M4D 2012 International Conference Proceedings.* Karlstad :Karlstad University Studies.
Taylor, J. (2007). The Usefulness of Key Performance Indicators to Public Accountability Authorities in East Asia. *Public Administration and Development,* Vol.27. Pp. 341-352.
Transparency International (2012). *Corruption Perceptions Index Report 2012.* Berlin:TI.
Transparency International (2011). *Bribe Payers Index 2011***.** Berlin:TI.
Transparency International (2010). *Corruption Perceptions Index Report 2010.* Berlin:TI.
Transparency International (2009). *Global Corruption Report 2009:Corruption and the Private Sector.* Cambridge: Cambridge University Press.
Transparency International (2008). *Bribe Payers Index 2008*. Berlin:TI.
United Nations Development Programme (2009). *Human Development Report 2009* title "Overcoming barriers: Human mobility and development". New York :UNDP.
United Nations (2010). *United Nations Global Compact. Principle10*.
United Nations Global Compact, Transparency International, & International Business Leaders Forum (2005). *Business Against Corruption: A Framework for Action.*
Visser, W. (2010). From the Age of Greed to the Age of Responsibility, In William Sun, et al. (eds)*Re-framing Corporate Social Responsibility: Lessons from the Global Financial Crisis*. Emerald, & Wiley.
Visser, W. (2005). *Business Frontiers: Social Responsibility, Sustainable Development and Economic Justice.* ICFAI University Press.

Exhibits

Exhibit 1 Forms of Bribery by Sector

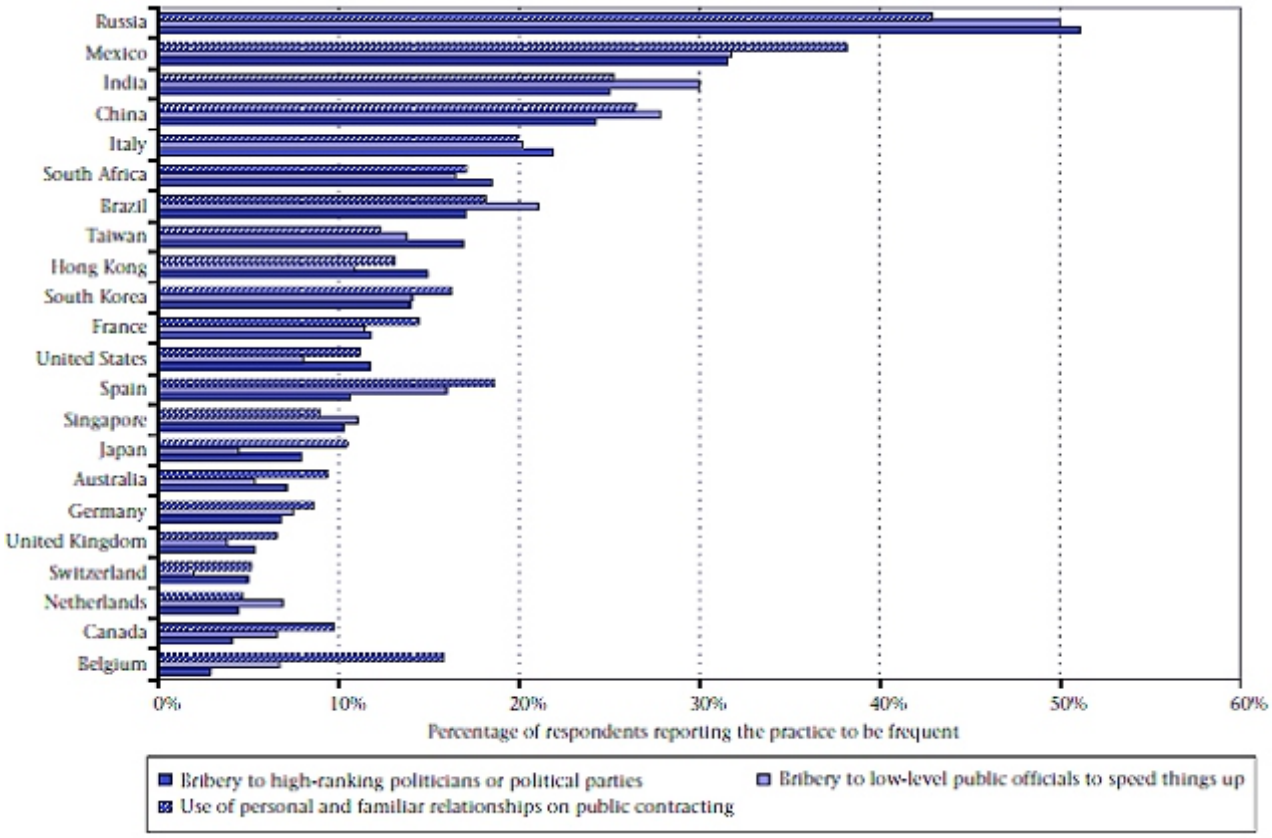
According to the 2011 Bribe Payers Survey - "Business people in 30 countries around the world were asked, based on their business relationships (for example as a supplier, client, partner or competitor): How often do firms in each sector: a) engage in bribery of low-level public officials **(petty corruption),** for example to speed up administrative processes and/or facilitate the granting of licenses?; b) use improper contributions to high- ranking politicians or political parties to achieve influence **(grand corruption)**?; and c) pay or receive bribes from other private firms **(private-to-private corruption)**?"

Note: Sectors are scored on a scale of 0-10, where a maximum score of 10 corresponds with the view that companies in that sector never engage in that form of bribery and a 0 corresponds with the view that they always do.



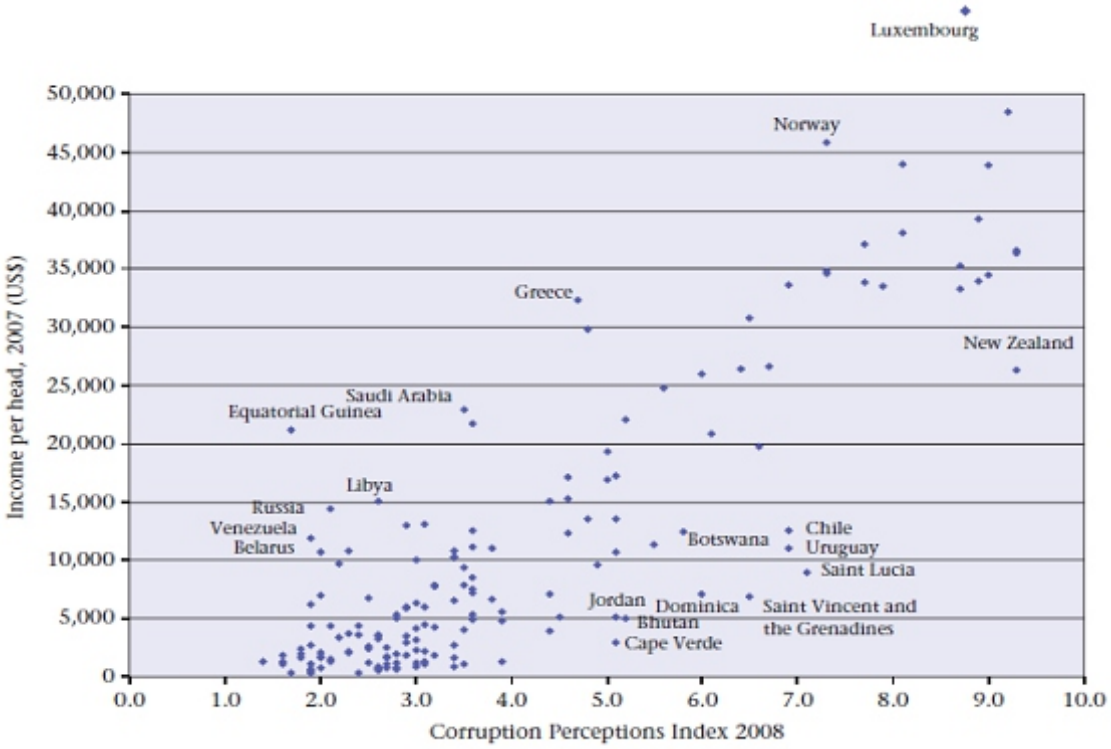
Source: TI Bribe Payers Index 2011

Exhibit 2. Types of foreign bribery



Source: TI Bribe Payers Index 2008

Exhibit 3. Corruption and poverty



Source: World Bank and Transparency International as documented in TI's Global Corruption Report 2009

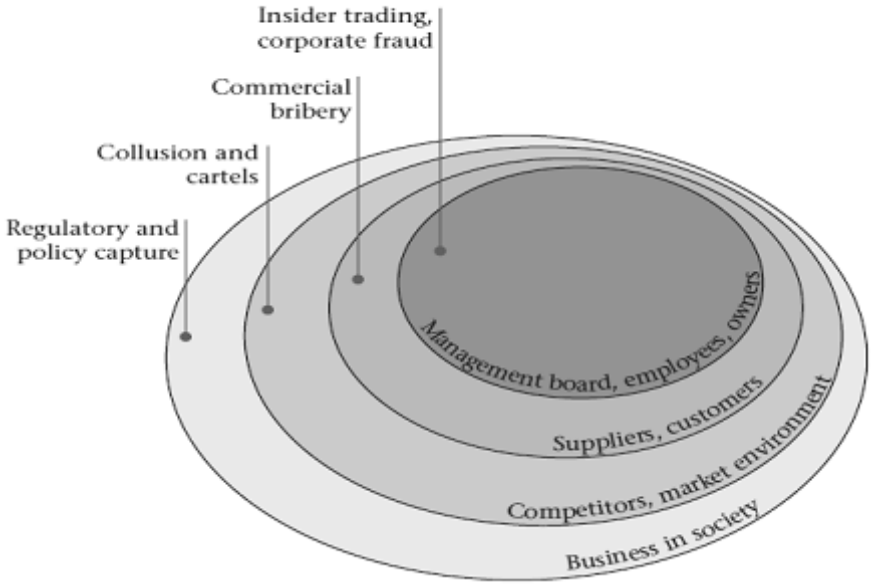
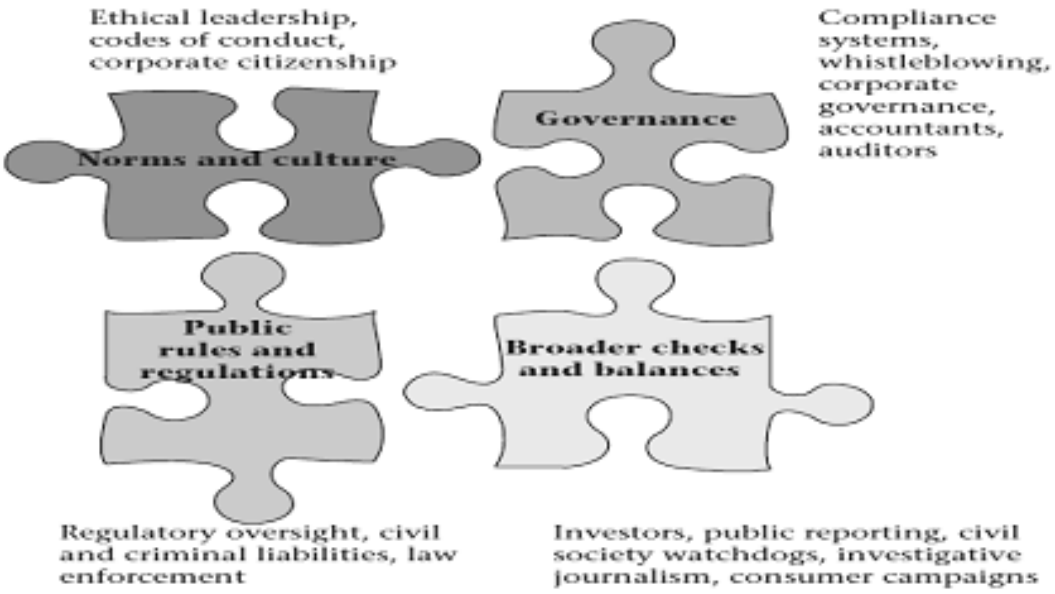


Exhibit 4. Corruption Risks within the Spheres of Corporate Activity

Source: Transparency International, 2009:8

Exhibit 5. From Corporate Integrity to Corporate Integrity System

Source: Transparency International, 2009:9



Author's Profile

Mohammad Talukdar

Mohammad Talukdar holds a Master of Social Sciences Degree in Public Administration specializing in Public Administration in South and South-East Asia from Dhaka University, Dhaka. He also received an international Master's Degree in Development Management from Asian Institute of Management (AIM), Manila. He is a development activist, researcher and management consultant. He was Center for Development Management Fellow at Asian Institute of Management, Manila. He is currently the Voluntary Chairman at Center for Decentralization and Governance Society (CDG), Dhaka. Importantly, he has authored three books and a number of national and international scholarly journal articles on decentralization and local governance, and governance and development. He also writes in English dailies. And he loves to present papers at national and international seminars and conferences.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

-

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005

Notes: