One writer sees the dilemma arising from the U.S./developed nation's viewpoint as jeopardizing the historical compromise on which the treaty is based: the sharing of revenues between OECD member countries and the reciprocity of treaty benefits. Elimination of source based taxation of income derived from telecommunication, software services, and licensing of intangibles will only improve the position of the U.S.. In the long run, developing nations will suffer from the U.S. and other developed nations' success. The OECD position in the TAG is to our advantage.

Recognizing the lack with which Philippine tax law addresses electronic commerce and the issues it raises, adoption of the guidelines by the OECD TAG and the U.S. Software Regulations for income characterization is essential. It is also necessary to determine under what circumstances a server may constitute permanent establishment as these issues are intimately related to the larger issue of income allocation under tax treaties.

A REVIEW OF STUDENT WRITTEN WORK ON E-COMMERCE AND RELATED TOPICS

As a supplement to this issue, the Editorial Board has prepared a summary of the different Notes written by students relating to E-commerce and the Internet.[1]

CLOSING IN ON COMPUTER BANDITS: A STUDY ON THE EXTENT OF THE COPYRIGHTABILITY OF COMPUTER SOFTWARES

MA. GABRIELLE ROSARIO M. YLAGAN *(1993)*

Computer scientists have little incentive to develop software for mass distribution because of blatant copyright violations. This thesis discusses whether the visual display of a computer program is protected by copyright. While current law protects computer programs, it fails to define "computer programs." Protection is crucial to the willingness of scientists to invest time and effort in creating software.

The resolution of the issue hinges on two cases decided by the American courts, namely: 1) *Broderbund v. Unison*; and 2) *Lotus v. Paperback Corporation*. The study is limited on the copyrightability of the user interface (the display screen that directly affects the user).

The author proposes a new law be enacted, considering the different facets of a computer program; but warns that the new law must not be so liberal as to allow indiscriminate copying; neither must it be so restrictive as to stifle the growth of the computer industry. As to the problem of determining the extent of infringement of the visual display, the author advocates the use of the substantial similarity test.

COMPUTERS UNDER SEIGE: CRIMINALIZING COMPUTER ABUSES

JOEL MAG-IBA VILLASECA *(1995)*

The pervasive use of computers has expanded traditional categories of criminals. "White collar crimes," denominated as the use of computer technology to steal or manipulate information, financial instruments and other misuse of computer systems of governments, financial institutions and commercial entities. The thesis studies the growth of computer crime and analyzes the responses, both legal and non-legal, that have been used to address the problem.

The adequacy of traditional criminal law doctrines is discussed along

Cite as 45 ATENEO L.J. 461 (2001).

[1] This report was prepared by Silvia Jo G. Sabio and Erlynne E. Uy.A copy of these notes are available at the circulation desk of the Ateneo Law School Library, Rockwell Campus.

with relevant developments in criminal law in the area of computer abuse. United States' response to the situation is useful where alternatives have evolved to address the issue. The role of international law is excluded.

While the freedoms to express and to experiment are recognized, the author notes that any law passed must balance such freedoms against the mindset of hackers who continue to disrupt networks and cause damage to different sectors. He recommends certain amendments to the Guingona Bill and the Rules on Evidence, education and training for the Department of Justice (on how to prosecute such crimes) and the adoption of a Code of Ethics for computer users.

OUTBREAK! AN ANALYSIS OF POSSIBLE LEGAL REMEDIES FOR THE VICTIM OF A COMPUTER VIRUS

LISSA RODRIGUEZ NUESTRO (1996)

This Note provides a working knowledge on computer viruses in general, the extent of damage that may result from infection, and the steps that the user may undertake to recover costs of damages and prevent subsequent attacks. Owing to the fact that the issue of computer viruses in the Philippines is relatively unexplored, American law and jurisprudence, as well as articles on the topic, were consulted.

The author explores the legal remedies available to a victim of a computer virus and the requisites found under the pertinent provisions of the law, both existing and proposed, which provide the aggrieved party with a remedy for the recovery of damages arising from the infection of his computer systems. Specifically, it dissects pertinent provisions on malicious mischief, quasi-delicts and human relations in order to determine whether prosecution under said provisions is feasible, and analyzes which among the available remedies afford the best recovery for the offended party. The provisions of the bill proposed by Senator Guingona relating to the introduction of a virus into a computer system is also discussed.

After a careful scrutiny of the loopholes of the existing law, this Note proposes the proper measures for the prosecution of persons who, through willful acts or through negligence, cause a computer system to be infected. The Note concludes that a case based on malicious mischief, or on the proposed computer crime law, will not cover acts of negligence. An action for quasi-delict may be instituted but recoverable amounts may be limited. A proceeding based on the human relations chapter of the Civil Code may succeed depending on the presence of the essential elements covered by the provisions.

OBSCENITY, PORNOGRAPHY AND CENSORSHIP IN CYBERSPACE: DO WE HAVE TO NET THE INTERNET?

CELSO VIRGILIO C. YLAGAN (1996)

The dramatic growth and popularity of the Internet has led to the concomitant problem of computerized pornography – or technoporn. Obscenity and pornography on this supernetwork is deemed a threat to the morality of future generations. This note seeks to explore the legal implications of the possible spread of obscenity and pornography through the Internet.

The author first discusses the working framework of the concepts involved in the field of computers. This is followed by a discussion of the relevant legal concepts involved, i.e., freedom of expression, prior restraint or censorship, freedom from punishment, and their application to the problems of obscenity and pornography in the Internet. The author then explores the different legal possibilities of regulating or censoring of the Internet.

The author concludes that outright censorship would be abhorrent on the ground that it violates freedom of expression. Enactment of legislation to regulate the Internet may be a better option, but only after a careful study to determine what law should be enacted considering the multi-jurisdictional nature of the Internet; the problems of enforcement; and the as-yet undecided determination of what kind of medium the Internet is. In the meantime, the Revised Penal Code on obscenity could be amended to include transmission through the Internet, and efforts could be made to update technology to allow filtering of information.

HTTP://WWW.INTERNET.ORG/LIBEL/PUB: ON-LINE DEFAMATION – PUNISHING INTERNET LIBEL UNDER THE REVISED PENAL CODE

CHRIS ALLAN P. ZAFRA (1996)

Stripped to its core, the Net is nothing more than a means of communication on a grander scale. Hence, the ever present possibility of "on-line" defamation. This work resolves two issues relative to Internet libel. First, considering that the Revised Penal Code was crafted in the 1930s, does it cover "On-line defamation"? In this respect, two essential requisites of Libel are discussed: (1) the writing, and (2) publication requirements. The second issue deals with the question of criminal responsibility: who are to be held liable for defamatory imputations circulated through the Internet?

The author resolves first whether libel committed through the Internet is punishable as Libel under the Revised Penal Code. The Internet as a mode or instrumentality for circulating defamatory imputations is emphasized, hence, it focuses on the elements of publication and media of communication. The issue of prosecution is limited to two basic points: (a) the issue of criminal jurisdiction as applied to on-line defamation (under these are resolutions to the question of jurisdiction over the subject, particular offense, the issue of territoriality and venue); and (b) the question of criminal liability of the author and the systems operator of the system through which the libelous material was published.

The author's conclusion is that that on-line defamation is punishable as libel under the Revised Penal Code, and, if certain conditions are met, may be prosecuted under Philippine jurisdiction. He recommends amendments to Philippine libel laws and the adoption of multilateral treaties addressing on-line defamation, but cautions that any changes must be made only after a thorough study is undertaken.

CYBERTHEFT: A STUDY ON THE EXTENT OF COPYRIGHT INFRINGEMENT IN LOCAL BULLETIN BOARD SYSTEMS AND THE CORRESPONDING LIABILITIES ARISING THEREFROM.

JEFFREY N. ONG (1997)

High quality digitized pictures, digitized music and software are all capable of being uploaded and downloaded from computer bulletin boards. Copyrighted materials are likewise made accessible by anyone without the permission of its author. This study defines the extent of copyright infringement that occurs in Philippine Bulletin Board Systems and alludes to acts constituting infringement.

The applicability of P.D. 49 (the then existing copyright law) is analyzed but does not take into account the R.A. which was then pending in Congress. Actual on-line transmission is utilized to determine the true extent of copyright infringement. Liability regimes are based on foreign journals and American jurisprudence.

While P.D. 49 identifies and resolves the incidents of bulletin board system activities the adoption of a strict liability regime as far as "sysop" or operator liability is concerned is recommended.

REGULATING INTERNET PORNOGRAPHY

FRANCIS ESPIRITU (1998)

Government regulation has become necessary due to the extent of proliferation of pornography on the Internet. The main issue in this Note is the extent which the State may regulate the Internet without violating freedom of speech.

The Note analyzes and compares Philippine and American jurisprudence regarding obscenity vis-à-vis the constitutionally guaranteed freedom of speech and expression, with emphasis on the (then) recent United States Supreme Court rulings regarding Internet pornography. The author recommends the regulation of the Internet by an administrative body implementing a program of filtering the access to Web sites containing obscene materials. The law creating this administrative body should clearly delineate the standards for obscenity that the administrative body shall follow in determining which particular web sites should be filtered.

This Note advances the discussion by incorporating the relatively recent rulings of the United States Supreme Court. These rulings which treat the issue of governmental regulation of obscenity in various media, including the Internet, provides more relevant jurisprudential basis for a rational legal framework for governmental regulation of the Internet.

CYBERLAW: PROTECTING COPYRIGHT ON THE WORLD-WIDE WEB[2]

LARISSA KRISTINA G. LAMBINO (1998)

The Internet's digital medium, known for its global network and instantaneously transmissible data, assimilates the features of a computer, a photocopier, a facsimile machine, and an electronic mailing system. This is a disturbing development to copyright advocates, who believe that traditional protection accorded to copyright may be eroded.

Reasonable protection should be accorded to intellectual property—whether existing in tangible form or in the Internet's digital code. Since the application of the copyright holder's exclusive rights has traditionally been applied to physical works, the study analyzes how this protection translates to digitized works on the Internet. In line with this, compelling reasons for excluding the application of traditional concepts in copyright law are clarified. The author demonstrates the need for uniform international copyright protection and standards of liability for copyright infringement within the framework of existing laws. Copyright protection, typical for printed, audio and video media may not be appropriate for this medium.

---

[2] 43 ATENEO L.J. 93 (1998).

PROPOSING STATUTORY MEASURES FOR THE REGULATION OF INTERNET COMMERCIAL TRANSACTIONS

ALDWIN BERNABE SALUMBIDES (1998)

One of the radical changes brought about by the Internet is the birth of commercial transactions conducted and perfected through the Internet. As business is generated, resulting liaisons are bound to be transgressed. This leads to the question that this Note seeks to answer: what then are the laws that should apply to commercial disputes arising on the Net?

The author discusses how contractual relations are formed, when a breach would occur, and the perils and security issues of payment in cyberspace. The issues of *situs*, capacity of parties, transactional jurisdiction, and personality and standing are discussed in relation to jurisdiction and litigation.

Considering the lack of local legislation governing Internet commercial transactions, the author sees a pressing need for immediate and specific legislation. Although the author does not propose any specific measure, he discusses the possible measures that may be enacted to address the need, i.e., security through exclusivity, identification through encryption, penal, sanctions, prescribing a form for internet transactions, fixing the point of perfection, and intermediary liability.

ELECTRONIC COMMERCE: A TAXATION LIMBO?

OLGA ANN N. BARRERA (1999)

As commerce grows on-line, so will concern over revenue lost by the Philippine government because of uncollected taxes on products and services sold over the Internet. This results to an erosion of the key revenue bases of the government: income and value added taxes.

The following categories of transactions occurring between and among corporations on-line are focused on: 1) sale of physical goods to business; and 2) sale from business to business of service and intangibles. Books and journals authored by foreign tax commentators, as well as existing tax regulations and rulings are analyzed.

The study concludes that traditional taxation concepts are applicable to address the taxation concerns in electronic commerce. The Internet is merely a medium through which commerce is made possible at the minimum time and should not affect the tax treatment of these transactions. The author recommends several interpretative rules on the taxation of electronic commerce.

E-MAIL MONITORING @ WORKPLACE.COM.PH: EMPLOYEE'S RIGHT TO PRIVACY IN THE INFORMATION AGE

NENITA C. CHUA (1999)

E-mail monitoring gives rise to two competing interests, namely: 1) the employer's right to maintain control and supervision over the workplace and 2) the employee's right to privacy. A review of existing laws in the Philippine jurisdiction reveals that employers do not have unbridled authority to monitor employees. Present law also affords remedies for employees whose privacy have been invaded. But these laws nevertheless fail to squarely address the issue of workplace monitoring.

American law and jurisprudence attempt to resolve the apparent conflict between the employer right to property and the employee's right to privacy. The permissible bounds in monitoring e-mail messages is discussed as well as the different levels of privacy protection afforded to public and private employees. The study resolves whether invasion of privacy in the workplace constitute a valid cause of action within the Philippine context.

Employees deserve some level of privacy in the workplace. Clear-cut policies governing workplace monitoring must be developed. A new law must be enacted to ensure the mandatory disclosure of such company policy. Such law must likewise specify the types of monitoring allowed, the duration of monitoring, and the use to be made of the collected data and penalties for the violation thereof.

SHOULD THE INTERNET TELEPHONY INDUSTRY BE REGULATED?

MA. ANTONINA M. MENDOZA (1999)

Internet telephony technology allows the placement of voice telephone calls over the Internet for the cost of regular Internet access fee and for unlimited time and distance. This technology threatens existing telephone companies.

Given the local regulatory environment of the telecomunications industry in the Philippines, the jurisdiction of the National Telecommunications Commission is doubtful since Internet telephony calls are currently not classified as telecommunications. The reaction of the international community, particularly United States and the European Community, to this technology is evaluated to the extent of the regulation policy it has adopted.

The existing regulatory structure on telecommunications is inapplicable to Internet telephony. The government must refrain from regulating the Internet and Internet telephony as this may cause the obstruction of the growth of domestic telecommunications industry on contrast to other countries that embraces and develops the Internet telephony. With the trend of deregulation and the opening of telecommunication markets to competition, it is anti-thesis to advocate increased regulation.

DETERMINING THE BOUNDARIES OF "MINIMUM CONTACTS": PERSONAL JURISDICTION IN CYBERSPACE

SHIELA T. QUIEN (1999)

With the advent of the Internet, it is now possible to be haled into a foreign court thousands of miles away even if an individual has never set foot in that State. This study discusses the various tests determining when it is proper for a forum to exercise jurisdiction over a person on s dispute arising from transactions made over the Internet.

Personal jurisdiction has two aspects, namely: 1) the long-arm statute of the State' and 2) constitutional due process considerations. American case law is heavily alluded to since there are several decided cases on the matter. The United States' federal system of government is a rich source of conflict of law cases, particularly on the issue of personal jurisdiction.

As there is no recourse for Filipinos who have been wronged by tortuous acts committed by non-residents through the Internet in Philippine legislation, guidelines are proposed to determine whether an particular on-line activity exposes the individual or entity operating such to the risk of being sued anywhere in the world. The degree of interaction, amount of promotion and solicitation and content of the site have been incorporated from American jurisprudence in shaping personal jurisdiction in cyberspace.

DOMAIN NAME DISPUTES: RESOLVING THE RIGHTS OF TRADEMARK OWNERS AND DOMAIN NAME REGISTRANTS UNDER RA 8293

CHRISTINE MARIE PALANCA QUIRINO (1999)

The distinctiveness and familiarity of domain names provide an incentive for businesses to register their trademark names as domain names. Because of this attractive feature, they may already be registered by owners of identical or similar trademarks or by speculators hoping for instant wealth. The problem stems from the fact that trademark law allows the concurrent use of domain names whereas the inter-operability of the Internet mandates that every domain name be unique.

Domain name disputes are considered in relation to the provisions of R.A. 8293 on trademarks, the Paris Convention, the TRIPS Agreement.

The study examines the five major classifications of domain name disputes: infringement, dilution, arbitrage, character string conflicts and parody and preemption. The author concludes that R.A. 8293 effectively resolves the rights of trademark owners and domain name registrants in cases of infringement but must be amended in order to address the problems of dilution and speculation. Character string conflicts are best determined under the first-come first-serve policy whereas parody and preemption are still too novel to merit any review of legislation.

E-MAIL PRIVACY: UPHOLDING THE ELECTRONIC BILL OF RIGHTS

MARIA CONCEPCION ABELLA GLORIA (2000)

The rise of cybercrimes and cybertorts have spurred the international community into a frenzy of Net regulations that seem to take "Big Brother" lengths to the utter dismay of both the Constitutionalists and the net users. This proves a monumental challenge as the Internet has neither boundaries nor physical features.

The Note deals solely with the issues of electronic mail privacy as against private individuals and the government. It illustrates the need to extend the right to privacy of correspondence granted to traditional forms of communications to electronic mail. It then identifies the problem areas in regulating e-mail privacy and proposes workable solutions. Finally, it proposes to bring the Philippines at par with current international legislation concerning electronic mail.

This Note reviews the existing laws and jurisprudence from different countries to arrive at an equitable and workable paradigm for the Philippines given our current level of technology and our Internet capacity. Most of the resource were taken from Cyberlaw websites and continuously updated by subscriptions. These web posts originate from the different Law Journals of universities like Harvard, Yale and the New York University, the latter reputedly the current leader in the field of Information Technology Law.

A BASIC CODE FOR CYBERSPACE

PETER O. KHO (2000)

The jurisdiction of a State within its own territory is necessary, exclusive and absolute. It is susceptible of no limitation not imposed by it. Its laws bind nationals and aliens, including non-residents,, and no process from a foreign government can take effect for or against them within the territory of the local

State without its permission. The purpose of Sovereignty and State Power is to maintain peace and order. There are situations where this end would be difficult to achieve through local police power or legislation alone due to the elusive nature of the medium. The same goal however, may best be attained by a concerted effort among countries that are hooked in Cyberspace.

This Note proposes to make an exception to the above rule and seeks to curtail the sovereign power of a State so far as the control over the Internet is concerned, because such an unbridled power may adversely affect rights of all citizens using the Web. It is based on a framework that there be a minimum law governing crimes and anomalies in Cyberspace. The focus, however, is limited to the general proposition of a basic international law governing cyberspace, to be agreed upon by countries linked to the Web.

The Note first covers the origin and development of cyberspace, and then explores in detail the inadequacy and major problems pervading the World Wide Web. It then reviews the attempts, perceived as futile, of some legislation to take control and dominion of cyberspace. Finally, a proposal is made that in ratifying an International Treaty that provides a minimum set of conduct online, circumvention of laws universally regarded as a menace may be avoided. These include virus explosion, child pornography, piracy, online fraud and violation of individual privacy.

ELECTRONIC CONTRACTS OF SALE AND THE STATUTE OF FRAUDS

FREDERICK R. T*AMAYO (2000)*

Commercial transactions make-up a large percentage of Internet communications. The main challenge to the law is the adoption of existing provisions of the Statute of Frauds to this new activity. The issue arises from the lack of specific legislation with respect to electronically rendered contracts and the fact that the Statute of Frauds was conceived of and designed for the physical rather than the virtual world.

Are contracts of sale executed through an electronic medium such as the Internet enforceable in light of Article 1403 (2) of the New Civil Code of the Philippines, which requires a written and signed document? This Note seeks to answer this question by first discussing the present status of the law on contracts in general, and contracts of sale in particular. It presents those contracts of sale that are covered by the Statute of Frauds and the exemptions therein. A discussion is then made of the enforceability of electronic contracts of sale vis-à-vis the written and signed requirements of the Statute of Frauds.

The author concludes that that notwithstanding the formulation of the Statute of Frauds decades before the Internet, it is still applicable to electronic contracts of sale.