Ethical issue on the internet

Sociology, Ethics

Ethical issues relating to the use of the Internet and the implications for managers and business practice. by Mihai C. Orzan Abstract When we address the topic of ethical issues on the Internet we are generally referring at two different matters: privacy and intellectual property. Each has been examined extensively in the last five years, since the Internet explosive intrusion in everyday life activities, each has an important number of sub fields that require special attention from managers and other business professionals.

The purpose of this paper is to to make a short presentation of most relevant developments pertaining Internet ethical issues in direct connection with the business world. The Privacy debate is centered on the arguments regarding citizens' right to privacy granted or implied by laws on one hand and companies approach on " customer data, considered an asset to sell for profits" (Choi, 2000, p. 317) on the other hand. Privacy on the Internet is exploding as a topic of public concern these days. A recent Internet survey showed that 4 out of 5 users have major concerns regarding various privacy threats when they're online.

Yet only 6% of them have actually experienced privacy abuses. Those who are not yet on the Net cite privacy as the main reason they have chosen not to become Internet users. If electronic commerce is going to thrive, this fear is going to have to be dealt with by laws and by industry practices and this paper attempts to give a thorough description of the major computer ethics trends of the moment. The other major source of concern for business world as well as the majority of Internet users is copyright control.

Serious question come from both approaches on this matter: what information available on the Internet can I freely use and how can one protect the hardly earned information that he posts on a website. In fact, “ The Internet has been characterized as the largest threat to copyright since its inception. It is awash in information, much of it with varying degrees of copyright protection. ” (O’Mahoney, 2001). Copyrighted issue constitutes an important part of this paper and it details most of the present concerns of intellectual property. 1 Privacy Everyone has the right to know what information is collected and how it will be used and to accept or decline the collection or dissemination of this information– particularly financial and medical information. " President George W. Bush. Privacy has become a major concern on the Internet. According to (Ferrell, Leclair & Fraedrich, 1997), “ the extraordinary growth of the Internet has created a number of privacy issues that society has never encountered before and therefore has been slow to address. ” Opinions have been expressed and actions were taken in order to resolve these matters in one way or another.

In aninterviewearlier this year United States President George W. Bush (Miller, 2001) expressed numerous and informed concerns regarding privacy issues, including access, security, and use of personal information. He promised to ensure actions that will meet consumer demands for privacy protection and advocated " opt- in" policies for mailing lists. He concluded the interview by stating: " I share many people's concerns that, with the advent of the Internet, personal privacy is increasingly at risk, and I am committed to protecting personal privacy for everyone. Privacy issues on the Internet relate to two major concerns. The first concern is users’ ability to

control the rate, type, and sequence of the information they view. Spam, or unsolicited commercial e- mail, is a control concern because it violates privacy and steals resources. A second concern relates to the ability of users to address and understand how organizations collect and use personal information on the Internet. Many 2 Web sites require visitors to identify themselves and provide information about their wants and needs.

Some Web sites track visitors' " footsteps" through the site by storing a cookie, or identifying string of text, on their computers. The use of cookies can be an ethical issue, especially because many users have no idea that this transfer of information is even occurring. Internet privacy is an important ethical issue because most organizations engaging in e- commerce have not yet developed policies and codes of conduct to encourage responsible behavior. Spamming " Junk e- mail and spam are both terms for advertising and e- mail sent to you which you did not ask for and which you do not want", (Elbel, 2001).

However, spam is a more generic term that includes broadcast posting to newsgroups as well as individuals. And spamming is very costly for the end users: recent surveys showed that various forms of spam consume up to 15% of Internet bandwidth. According to a recent European Union study " junk email costs all of us some 9. 4 billion (US) dollars per year, and many major ISPs say that spam adds 20% of the cost of their service", (Elbel, 2001). As you can see spamming is a very profitable endeavor and have grown over the years to assume a number of different forms.

Thus, we can distinguish: v Unsolicited e- mail is any email message received where the recipient did not specifically ask to receive it. It might not be

always an abuse. v Bulk e- mail is any group of messages sent via e- mail, with substantially identical content, to a large number of addresses at once. Many ISPs specify a threshold for bulk e- mail to be 25 or more recipients within a 24- hour period. Once again, bulk e- mail itself is not necessarily abuse of the e- mail system. 3 Unsolicited Commercial E- mail (UCE) is a form of e- mail containing commercial information that has been sent to a recipient who did not ask to receive it. Several ISPs specify that sending even one UCE is a violation of privacy. v MakeMoneyFast (MMF) are e- mail messages that " guarantee immediate, incredible profits! ", including such schemes as chain letters. v Multi-Level Marketing (MLM) are e- mail messages that " guarantee incredible profits! ", right after you send them an " initial investment" and recruit others. v Mailbomb is probably the most harmful type of spamming.

It takes the form of email packages delivered repeatedly to the same address until the mailbox is overloaded, or perhaps even the system that hosts the mailbox crashes. Mailbombs generally take one of two forms. A mailbox might be targeted to receive hundreds or thousands of messages, making it difficult or impossible for the victim to use their own mailbox, possibly subjects them to additional charges for storage space, and might cause them to miss messages entirely due to overflow. This is seen as a denial- of- service attack, perhaps also harassment.

Another form of mailbombing is to forge subscription requests to many mailing lists, all for one recipient. The result is a huge barrage of email arriving in the victim's e- mail box, all of it unwanted, but " legitimate". There are several ways to escape spamming, but none will guarantee 100 percent

reliability. First, a complaint to the ISPs that originated and forwarded the spam is required. It is also recommended to switch to an ISP that uses one or all of the anti- spam databases available (RBL, RSS, and DUL). About 40% of the Internet is using these services, with good success.

Also, it is important that you never, under any circumstance, reply to junk e-mail, even if it is to send a " remove" request. Most spammers ignore such 4 responses, or worse, add you to their list of validated e- mail addresses that they sell. Also, getting removed doesn't keep you from being added the next time they mine for addresses, nor will it get you off other copies of the list that have been sold or traded to others. Finally, we should note that there are voices that argue that spamming is a legitimate form of expression and restricting it would be a First Amendment infringement.

Even more, has been suggested that “ junk e- mail (also called " bulk" e-mail and " spam") should be legally protected”, (D’Ambrosio, 2000). Tracking a user on the Internet Data about individuals is collected in a wide variety of ways, including information provided on application forms, credit/debit card transactions, and cookies. Many users expect that such activities are anonymous, but unfortunately they are far from being so. It is possible to record many online activities, including which newsgroups or files a subscriber has accessed and which web sites a subscriber has visited.

This information can be collected both by a subscriber's own service provider (available in the request headers of browsers) and by agents of remote sites which a subscriber visits. But the most popular form of collecting data about web surfers is the cookie. These are short pieces of data used by web servers to help identify web users. The cookie is stored on the user's

computer, but contrary to popular belief it is not an executable program and cannot do anything harmful to the machine. Cookies are used by Internet shopping sites to keep track of users and their shopping carts.

When someone first visits an Internet shopping site, they are sent a cookie containing the name (ID number) of a shopping cart and other useful tags. Another use of cookies is to create customized home 5 pages. A cookie is sent to the user’s browser for each of the items they expect to see on their custom home page. One of the less admirable uses of cookies, and the one that is causing all the controversy, is its use as a device for tracking the browsing and buying habits of individual web users.

On a single web site or a group of web sites within a single subdomain, cookies can be used to see what web pages you visit and how often you visit them. However, such concerns can be easily addressed by setting the browser to not accept cookies or use one of the new cookie blocking packages that offer selective cookie access. Note that blocking all cookies prevents some online services from working. Also, preventing the browser from accepting cookies does not confer anonymity; it just makes it more difficult to be tracked on the Web. Related to cookies, but more damaging is the activity known as “ prying”.

Many of the commercial online services will automatically download graphics and program upgrades to the user's home computer. News reports have documented the fact that certain online services have admitted to both accidental and intentional prying into the memory of home computers signing on to the service. In some cases, personal files have been copied and collected by the online services. Use of Personal Information You can find out

simple directory information about people on a variety of web sites, like Switchboard, Whowhere, Four11, Bigfoot.

These contain information retrieved from telephone books. And most of these sites allow someone who doesn’t want to be listed in their databases to have his/her information removed. But beyond the free services there are the fee- based services where one can find out a great deal about 6 individuals on the Internet. There are services like as KnowX, Informus, Infotel, CDB, Infotek, Information America, and Lexis- Nexis that offer subscription based services and give access either through the Internet or through their own telephone networks.

The information they provide is primarily from public records like records of court cases, both civil and criminal (not the full text, not yet anyway, but an index of cases), bankruptcies, judgments and liens, property records, such as county tax assessors files, professional license information, if regulated by the state, Dept of Motor Vehicle data from many states, voter registration data from many states, stock investments, if you own 15% or more of a company’s stock, and many more other sources.

Data warehouses built with this kind of sensitive personal information (including " browsing patterns," also known as " transaction- generated information") are the lifeblood of many enterprises that need to locate their customers with direct mailing (or e- mailing) campaigns. It may also create the potential for " junk e- mail" and other marketing uses. Additionally, this information may be embarrassing for users who have accessed sensitive or controversial materials online. In theory, individuals (data subjects) are

routinely asked if they would permit their information to be used by the information collector.

Application forms usually include a clause stating that personal information provided may be used for marketing and other purposes. This is the principle of informed consent, meaning that if the individual does not so request that his/her data not to be used for such purposes, it is assumed that he/she had given permission. The alternative principle, of affirmative consent, where an individual is required to give permission for each and every occasion on which a data user wishes to make use of an individual’s data, becomes extremely expensive and complex and is seldom practiced.

The Federal Trade Commission is urging commercial web site operators to make public their information collection practices in privacy policies posted on web sites. 7 Many web sites now post information about their information-collection practices. You can look for a privacy " seal of approval," such as TRUSTe, Council of Better Business Bureaus (BBB), American Institute of Certified Public Accountants, WebTrust, and others on the first page of the web site. Those that participate in such programs agree to post their privacy policies and submit to audits of their privacy practices in order to display the logo.

There are several technologies that help online users protect their privacy. v Encryption is a method of scrambling an e- mail message or file so that it is unintelligible to anyone who does not know how to unscramble it. Thus, private information may be encrypted, and then transmitted, stored or distributed without fear that outsiders will have access to its content. Various

strong encryption programs, such as PGP (Pretty Good Privacy) and RSA (RSA Data Security) are available online.

Because encryption prevents unauthorized access, law enforcement agencies have expressed concerns over the use of thistechnology, and Congress has considered legislation to create a " back door" to allow law enforcement officials to decipher encrypted messages. Federal law limits exporting certain types of encryption code or descriptive information to other countries and file them under the same ammo type as nuclear weapons. v Anonymous remailers. Because it is relatively easy to determine the name and email address of anyone who posts messages or sends e- mail, the practice of using anonymous remailing programs has become more common.

These programs receive e- mail, strip off all identifying information, and then forward the mail to the appropriate address. v Memory protection software. Software security programs are now available which help prevent unauthorized access to files on the home computer. For 8 example, one program encrypts every directory with a different password so that to access any directory you must log in first. Then, if an online service provider tries to read any private files, it would be denied access. These programs may include an " audit trail" that records all activity on the computer's drives.

Censorshipand Blocking Software “ With its recent explosive growth, the Internet now faces a problem inherent in all media that serve diverse audiences: not all materials are appropriate for every audience” (Resnick & Miller, 1996). Any rules or laws about distribution, however, will be too restrictive from some perspectives, yet not restrictive enough from others. Apparently it might be easier to meet diverse needs by controlling reception

rather than distribution. In the TV industry, this realization has led to the V-chip, a system for blocking reception based on labels embedded in the broadcast stream.

On the Internet, the solution might be considered even better, with richer labels that reflect diverse viewpoints, and more flexible selection criteria. Not everyone needs to block reception of the same materials. Parents may not wish to expose their children to sexual or violent images, businesses may want to prevent their employees from visiting recreational sites during hours of peak network usage, and governments may want to restrict reception of materials that are legal in other countries but not in their own.

The blocking solution with the largest acceptance at this moment is PICS (Platform for Internet Content Selection). Its labels are supposed to be able to describe any aspect of a document or a Web site. As was natural to be expected, PICS labels started out as an attempt to block web pages that were not compliant with indecency 9 laws. As one of its initiators said, “ the original impetus for PICS was to allow parents and teachers to screen materials they felt were inappropriate for children using the Net”, (Weinberger, 1997).

At this moment, Microsoft, Netscape, SurfWatch, CyberPatrol, and other software vendors have PICS- compatible products, while AOL, AT WorldNet, CompuServe, and Prodigy provide free blocking software that is PICS-compliant. Intellectual Property Intellectual Property concerns the protection of “ all products created or designed by human intellect – book, songs, poems, trademarks, blueprints...and software” (Davidson, 2000, p. 9). The copying of software programs, although nominally protected by copyright

laws, is certainly widespread. Much of the argument about IP lies in the deontological dichotomy between rights and duties", (Davidson, 2000, p. 12). Software producers claim that they have the right to protect the fruit of their endeavors, and have the right to be compensated for the resources spend in the development process, while consumers claim that they have the right to use a product for which they have paid and expect that the product will be free of defects. This should lead to competitively priced products with superior quality, providing value for money. 10 Copyright, Patents, and Trademarks

According to prof. Johnson (2000) " as computing resources become more and more prevalent, computer software becomes easier and easier to access, and as such, easier and easier to copy", (p. 124). Protection for one's work, from a legal point of view, requires copyright, patents, and trademarks for sensible and strategic information. The best approach is to have a combination of trade secret protection, copyright laws, and trademark laws for the product in question because these are cheap, effective, and fast ways of protecting a software product from being pirated.

Copyright Issues Copyrighted works on the net include news stories, software, novels, screenplays, graphics, pictures, Usenet messages and even e- mail. " In fact, the frightening reality is that almost everything on the Net is protected by copyright law" (O'Mahoney, 2001). Software and manuals, as novels and other literary works, are protected under copyright laws. In simple terms, this guarantees the copyright owner, the author in most cases, the exclusive rights to the reproduction and distribution of his intellectual property.

Thus, copyright law guarantees the owner of the intellectual property the same types of rights that patent law guarantees the owner of an invention or other piece of seemingly more tangible physical property. Computer software and data are intellectual property, and as such are covered by copyright law. The problems start when people cannot, or will not, make the mental transition from physical to intellectual property. While most people would not steal books from a bookstore or a software package from a dealer's showroom, 11 ven if they knew they would not be caught, many of the same people would not hesitate copying a computer program from a demo or from their friends and colleagues. The only free software is the one places in the public domain, also known as freeware. For the rest of the software products the user must abide by the license agreements which usually come with a program and places restrictions upon reproducing and distributing the software, including such things as loaning the software to a friend or colleague and making duplicates for classroom or network use. Some licenses even go so far as to restrict use to a specific computer.

In most cases, however, the user does have the right to make a backup copy of the software for archival purposes. In theory, any use of a software package which falls outside of the limits of the license agreement renders the user, and quite often the user's company or institution, liable to prosecution. A computer program is defined in the copyright law as " a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result. " Copyright protection begins at the time a work is created in fixed form; no act other than creation of the work is required to obtain a copyright for the work.

According to (Yoches and Levine, 1989) “ the scope of copyright protection for a computer program's expression may extend beyond its literal code to the structure, sequence and organization of the program. ” Another debated and important aspect of software copyright involves the use of databases, data warehouses, and other forms of data collections. Under traditional concepts of literary copyright, the data contained in a compilation, and the selection of the data, may sometimes not be protected from copying. Only the coordination and arrangement of the database may be protected, and even then there must be some originality to the collection and arrangement for it to be protected”, (Losey, 1995). 12 There are essentially three ways to legally protect computer databases: copyright, trade secret and contract. Raw facts in a database may not be protected by copyright, regardless of the time or expense that went into locating them. However, in many databases the data itself, or the particular expressions of the facts, may have been created by the author. In such cases the data has originality and can be protected.

Even if the contents are raw facts, not new materials created by the author, the compilation aspects of the database (selection, coordination and arrangement) may still receive copyright protection. A trade secret is “ knowledge which a person or company acquires through its own efforts and which has some value to it” (Losey, 1995). Typically, this knowledge is kept secret from competitors because it is felt that this information provides some type of competitive advantage. Since a computer database is a compilation that derives economic value, it is a type of intellectual property that has frequently received trade secrecy protection.

Finally, the owner of a database can require that any purchaser enter into a written contract as a condition of purchase of the database. That written agreement could expressly provide that the purchaser will not disclose the content to anyone but authorized users, nor make any copies or unauthorized use of the information. Typically this takes the form of a License Agreement between the owner/licensor of the database and the user/licensee of the database. Protect your site against theft It might be useful to know that a link is a URL, a fact not unlike a street address, and is therefore not copyrightable.

However, a URL list may be copyrightable under a 13 compilation copyright if it contains some originality. The Internet was created on the basis of being able to attach hypertext links to any other location on the Web. Consequently, by putting yourself on the Internet, " you have given implied permission to others to link to your Web page, and everyone else on the Web is deemed to have given you implied permission to link to their Web pages" (O'Mahoney, 2001). The two primary methods of protection are technical countermeasures and legal protection.

Technical countermeasures include strategies such as digital watermarking and spiders that search the Internet for copies of your pages or graphics. These strategies tend to be difficult, expensive, and user- unfriendly. The primary vehicle for legal protection is copyright. This is by far the easiest and most popular form of protection in use today. In implementing a copyright strategy, there are three items that you should consider: v Ownership: before trying to copyright your website, a clear understanding of what exactly it is considered to be copyrighted is required.

There are many elements to a website, including text, graphics, scripts, data, and code. If everything was created from scratch for the website, ownership is not an issue. However, if someone else created text, or some clip art was downloaded from another website, or scanned photographs from archives were used, or a web design firm was hired to load all informational content into an attractive package, then ownership of the respective elements is shared with the original creators, unless otherwise stated in contracts and licenses. Copyright notice: it is generally a good idea to put a copyright notice on your website. It used to be that in order to be afforded any copyright protection whatsoever, one needed to put the world on notice by attaching a copyright notice to the work. While this is no longer the case, it is still customary to attach a 14 copyright notice on copyrighted works in order to be eligible for certain types of damages. The copyright notice consists of at least elements that include the copyright symbol and/or the term " Copyright", the year of copyright, and the name of the copyright holder. Registration: register your copyright with the Copyright Office. Although the Copyright Act gives protection just for creating your work and reducing it to a tangible form, that protection proved somewhat illusory in some cases when registration was overlooked. Patents and Trademarks “ A recognized brand name or trademark represents the goodwill that has been built into the product or service”, (Eldenbrock & Borwankar, 1996). Consumers tend to associate the recognized brand name or trademark with certain characteristics that are specific to that name or mark.

Therefore, companies often spend millions of dollars annually for safeguarding the investment in the related intellectual property rights.

Trademark laws protect the name of the software, not the software itself. Some examples include: " Lotus 1- 2- 3", " Apple ", " D- BASE", " WordPerfect", and many others. Copyright protection protects the expression of an idea, not the idea itself. A patent protects the idea itself. There are two major drawbacks to patents. They take a lot of money and a lot of time (usually two or more years).

Computer games are rarely patent protected because the shelf life for a game is usually no more than six months. 15 Fair Use “ When the fair use doctrine applies to a specific use of a work, the person making fair use of the work does not need to seek permission from the copyright owner or to compensate the copyright owner for the use of the work”, (Lehman, 1998). The fair use is a form of limitation of the exclusive rights of copyright owners for purposes such as criticism, comments, news reporting, teaching (including the possibility to make multiple copies of a copyrighted work for classroom use), scholarships, or research.

In order to determine whether the use made of a work in any particular case is not a copyright infringement, Smith’s (2001) Copyright Implementation Manual offers the following guidelines: 1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; 2. the nature of the copyrighted work; 3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and 4. the effect of the use upon the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors. Those

creators and authors who wish to dedicate their works to the public domain may, of course, do so notwithstanding the availability of protection under the Copyright Act. 16 Libel and Defamation " We know that as the Internet grows, there will be more and more lawsuits involving libel and defamation. " said attorney David H. Donaldson, editor of Legal Bytes, " The only question is if the number of cases will grow steadily or if there will be an explosion of lawsuits all at once. The Internet has been used to harass, slander, threat and these online activities led to arrests, successful sues (because have used netnews to slander and for delivering inappropriate screen saver images) and other forms of legal punishments. The most frequent form of libel on the Internet is flaming, defined as " the practice of sending extremely critical, derogatory, and often vulgar e- mail messages, or newsgroup postings to other users on the Internet or online services" (O'Brien, 2002, pp. 326).

Famous cases ofracismor defamation have turned the attention at the gaps in legislation regarding Internet crime. Sexual explicit web pages are responsible for another stir in social awareness regarding Internet- related legal void. Sometimes even a " link to another's page could be defamatory and may subject someone to legal liability", (INET Legal Networks, 2001), if it links to a page where offensive or illegal content is present and if you do not give strong warning to the web surfer about the consequences of his/her " click".

There are a number of features unique to the Internet that distinguish it from any other medium and have " led to the current re- examination of existing libel laws to allow for their possible evolution and ultimately their application in the cyberspace", (Potts & Harris, 1996). These features include its global

nature (more than 125 countries are linked via Internet), which raised questions about jurisdiction, repeated publication every time a 17 page is updated/viewed, and the possibility to enforce judgments.

Another Internet specific aspect is its highly interactive nature, which decreases the effectiveness of later corrections, but empowers the ability to reply, which might be considered more gratifying, immediate and potent than launching a libel action. Accessibility is another feature of the Internet, which distinguishes it from traditional print or broadcast media. The relatively low cost of connecting to the Internet and even of establishing one's own website means that the opportunity for defamation has increased exponentially. Now, on the Internet everyone can be a publisher and can be sued as a publisher.

Internet anonymity means that users do not have to reveal their true identity in order to send email or post messages on bulletin boards. This feature, coupled with the ability to access the Internet in the privacy and seclusion of one's own home or office and the interactive, responsive nature of communications on the Internet, has resulted in users being far less inhibited about the contents of their messages than in any other form of media. Computer Crime One of the biggest threats for the online community comes from various ways in which a computers network in general and the Internet in special might be used to support computer crime.

The list of such actions is vast as “ criminals are doing everything from stealing intellectual property and committing fraud to unleashing viruses and committing acts of cyberterrorism” (Sager, Hamm, Gross, Carey & Hoff, 2000) and a few of the most dangerous and common ones have already

entered the general IT folklore. The Association of Information Technology Professionals defined computer crime as including “ unauthorized use, access, modification, and destruction of hardware, software, data, or network resources; unauthorized release of information; unauthorized copying of 18 oftware; denying an end user access to his or her own hardware, software, data, or network resources; using or conspiring to use computer or network resources to illegally obtain information or tangible property. ” Software piracy Software piracy is the illegal copying of computer software. It is also considered the computer industry's worst problem and, according to the specialists, has become a household crime. “ People who wouldn't think of sneaking merchandise out of a store or burgling a house regularly obtain copies of computer programs that they haven't paid for”, (Hard- Davis, 2001).

Software piracy is fought by legal means (licenses, copyright, trademarks and patents, and lawsuits, when all else fails). According to Zwass (1997), “ deterrent controls (legal sanctions) and preventive controls (increasing the cost of piracy by technological means) can be used to combat software piracy. ” Information technology is a key driver in theglobalizationand growth of the world economy. In a recent study of worldwide software market (International Data Corporation, 1999) the total worldwide package software market has been stimated at $135 billion. Worldwide expenditures on software are expected to increase to about $220 billion by the year 2002. The U. S. software industry is reaping the benefits of this hyper growth, having captured 70% of global software sales. According to (Software Publishers Association, 1998), the worldwide revenues of business- based PC

applications was $17. 2 billion, but global revenue losses due to piracy in the business application software market were calculated at $11. 4 billion.

This is very similar to the report of (International Research and Planning, 2001)’s Business Software Alliance (BSA), a watchdog group representing the world’s leading software manufacturers, which announced the results of 19 its sixth annual benchmark survey on global software piracy. The independent study highlights the serious impact of copyright infringement with piracy losses nearing $11. 8 billion worldwide in 2000. Figure 1 shows an interesting correlation between the national piracy rates compiled by the SPA with the per capita GNP for 65 countries in the year 1997.

Higher software piracy rates are heavily skewed towards countries with low per capita GNP. The effect of GNP is much more pronounced for the countries with GNPs less than $6, 000, as shown in Figure 2. Each $1, 000 increase in per capita GNP is associated with a nearly 6% decrease in the piracy rate. These results indicate a significant income effect on the global piracy rates, particularly in the poorer segments of the world. The different ways of illegally copying computer software can be broken down into five basic ways of pirating. Counterfeiting is duplicating and selling unauthorized copies of software in such a manner as to try to pass off the illegal copy as if it were a legitimate copy produced by or authorized by the publisher. v Softlifting is the purchasing of a single licensed copy of software and loading it on several machines, contrary to the terms of the license agreement. This includes sharing software with friends and co- workers. v Hard- disk loading is selling computers pre- loaded with illegal software. v Bulletin-board piracy is putting software on a bulletin- board service for nyone to copy or copying software

from a bullet in- board service that is not shareware or freeware. v Software rental is the renting of software for temporary use. An interesting study regarding software piracy inacademicenvironmentwas conducted at the Faculty of Business at the City University of Hong Kong (Moores & 20 Dhillon, 2000). A total of 243 usable responses were received, of which 122 were female and 121 were male. As shown in Figure 3, 81% of the respondents report they buy pirated software on a regular basis, with a significant minority (29%) buying every month, and 3% even reporting they buy several times a week.

The most popular pirated software bought was spreadsheets, followed by programming languages, databases, word processors, and statistical packages. Other software mentioned included e- mail, graphics, and game software. Only 7% claim to have never bought pirated software. Illegal Information The Internet was designed as an inherently insecure communications vehicle. This allowed an impressive number of security gaps that led to numerous hacking techniques. Probably the most famous one at this moment is the denial of service attack, that led to the shutdown of many famous Internet sites, including Yahoo! , eBay, Amazon, and CNN.

Other hacking tactics include spoofing (faking an web page to trick users into giving away critical information), Trojan horses (programs that are planted on user’s machine without his knowledge), logic bombs (instructions in computer programs that triggers malicious acts), and password crackers. According to Givens (2001), “ Identity thieves are able to shop online anonymously using the identities of others. Web- based information brokers sell sensitive personal data, including Social Security numbers, relatively

cheaply. ” In December 1999 300, 000 credit card numbers were stolen from the onlinemusicretailer CD Universe database.

That’s way it is considered a federal crime to possess 15 ore more access devices like cellular activation codes, account passwords, and credit card numbers. 21 Beside the theft that these kinds of devices enable, such actions lead to loss of trust from customers to such services that have been the target of hacking. It is also illegal in many states to have pornographic related material on your machine, and in some cases mere possession of child pornography is punishable by many years in jail. As mentioned before, possession or export of certain types of cryptographic techniques is a very serious federal crime.

AMA Code of Ethics of Marketing on the Internet “ All professionals find a code of ethics is useful to guide them through the sometimes thorny issues that confront them” (Klampert, 1998). Codes of ethics are an organized, written set of rules that describe expected behaviors. There are many such codes in Information Systems (ACM, IEEE, British Computer Society), but none of them has overall recognition. Most institutions that provide Internet access have formulated policies and procedures regarding the fair use of their facilities.

The most frequent policies are grouped under the following categories: a Code for Ethical Computer Use (usually a written policy an institution has developed to describe ethical use of their computer system), an E- mail Privacy Policy, and an Internet Access Policy. One of the most representative such codes for the Internet community is the one that has been imposed by the American Marketing Association for its members. Below there are a few

of the most interesting requirements, as they can be found in the latest edition of (AMA, 2001) Code of Ethics for Marketing on the Internet: 2 Adherence to all applicable laws and regulations with no use of Internet marketing that would be illegal, if conducted by mail, telephone, fax or other media. Organizational commitment to ethical Internet practices communicated to employees, customers and relevant stakeholders. Information collected from customers should be confidential and used only for expressed purposes. All data, especially confidential customer data, should be safeguarded against unauthorized access. The expressed wishes of others should be respected with regard to the receipt of unsolicited e-mail messages.

Information obtained from the Internet sources should be properly authorized and documented. Marketers should treat access to accounts, passwords, and other information as confidential, and only examine or disclose content when authorized by a responsible party. The integrity of others' information systems should be respected with regard to placement of information, advertising or messages. Conclusions This R paper gives a general overview of the most debated ethical issues related to the use of Internet and their implications for managers and business practice.

However, there are several other less critical aspects that should be considered by a very thorough revision and some very interesting papers on these subjects are listed in Appendix C. These aspects include unauthorized use of computer resources at work, accessing individuals’ private e- mail and telephone conversations and computer records by the companies they work for and other forms of computer monitoring, challenges to 23 work

conditions and individuality that are brought about by computer systems, mistaken computer matching of individuals, and many, many more.

To protect themselves and the people they work with, information professionals need to be as professional as they can be and, sometimes, must decline a project if clients insist that they do something they have moral objections about. Ethical considerations are inherent for any IT professional. Moral behavior, including acting with integrity, increasing personal competence, setting high standards of personal performance, acceptingresponsibilityfor your actions, avoiding computer crime, and increasing the security of computer systems developed are just a few of many such considerations.

Overall, I believethat there is a critical need for heightened debate on professional ethics in Information Systems. 24 Appendix A Figure 1. Per capita GNP and piracy rates. Figure 2. Piracy rates and per capita GNP less than $6000 25 Figure 3. Frequency of pirated software. 26 Appendix B Cited Works 1. Choi, S. - Y. & Whinston, A. B. (2000). The Internet Economy: Technology and Practice. Austin, TX: SmartEcon Publishing. 2. D’Ambrosio, J. (2000,. January). Should “ Junk” E- mail Be Legally Protected? [online]. Available: http://www. fmew. com/archive/junk/. October 26, 2001). 3. Davidson, Robert (2000, April). Professional Ethics in Information Systems: A Personal Perspective. Communications of the AIS, Vol. 3, Article 8. 4. Elbel, F. (2001, October 23). Junk E- mail and Spam. [online]. Available: http://www. ecofuture. org/jmemail. html. (October 26, 2001). 5. Elderbrock, David and Borwankar, Nitin. (1996). Building Successful Internet Businesses: The Essential Sourcebook for Creating Businesses on the Net. Foster City, CA:

IDG Books Worldwide. 6. Ferrell, O. C. , Leclair, D. T. , & Fraedrich, J. P. (1997, October).

Integrity Management : A Guide to Managing Legal and Ethical Issues in the Workplace. O'Collins Corp. 7. Givens, Beth. (2001, March). A Review of Current Privacy Issues. [online]. Available: http://www. privacyrights. org/ar/Privacy- IssuesList. htm. (October 26, 2001). 8. Hard- Davis, G. (2001, March). Internet Piracy Exposed. Alameda, CA: Sybex. 27 9. INET Legal Networks (2001). Defamation – Law for Internet [online]. Available: http://www. lawforinternet. com/subject_defamation. php3? searchkys= defamation = topdefamation. html. (October 26, 2001). 10.

International Data Corporation (1999, February 10). Distribution of Worldwide Software Revenues Vary Dramatically [online]. Available: www. idcresearch. com/Press/default. htm. (October 26, 2001). 11. International Research and Planning. (2001, May). Sixth Annual BSA Global Software Piracy Study. [online]. Available: http://www. bsa. org/resources/200105- 21. 55. pdf. (October 26, 2001). 12. Johnson, Mark B. (2000, January). Software Piracy: Stopping It Before It Stops You. Proceedings of the sixteenth ACM SIGUCCS Conference on User Services. pp. 124- 131. 13. Klampert, Elizabeth (1998, July 13).

Business Ethics for Information Professionals. Proceedings of the AALL 1998 Conference on Independent Law Librarian Program, Anaheim, CA. 14. Lehman, B. A. , (1998). The Conference on Fair Use: final report to the commissioner on the conclusion of the Conference on Fair Use. Washington, DC: Office of Public Affairs U. S. Patent and Trademark Office. 15. Losey, Ralph C. (1995). Practical and Legal Protection of Computer Databases

[online]. Available: http://www. eff. org/Intellectual_property/database_protection. paper. (October 25, 2001). 16. Miller, M. J. (2001, February 6).

Bush’s Privacy Plan. PC Magazine, Vol. 20, No. 3. 28 17. Moores, T & Dhillon, G. (2000, December). Software Piracy: A View from Hong Kong. Communicationof the ACM, Vol. 28, No. 10, p. 88- 93. 18. O’Brien, J. A. (2002). Management Information Systems: Managing Information Technology in the E- Business Enterprise. New York, NY: McGraw- Hill. 19. O’Mahoney, B. (2001). Copyright Website [online]. Available: http://www. benedict. com/digital/digital. asp. (October 26, 2001). 20. Potts, David & Harris, S. (1996, May 16). Defamation on the Internet [online]. Available: http://owl. nglish. purdue. edu/handouts/research/r_apa. html. (October 26, 2001). 21. Resnick, P. & Miller, J. (1996). PICS: Internet Access Controls Without Censorship. Communications of the ACM, Vol. 39, No. 10, pp. 87- 93. 22. Sager, Ira, Hamm, Steve, Gross, Neil, Carey, John and Hoff, Robert. (2000, February 21). Business Week. 23. Smith, Steve. (2001, May). Copyright Implementation Manual [online]. Available: http://www. groton. k12. ct. us/mts/cimhp01. htm. (December 1, 2001). 24. Software Publishers Association (1998). SPA's Report on Global Software Piracy [online]. Available: www. pa. org/piracy/98report. htm. (October 26, 2001). 25. Weinberger, J. (1997, March). Rating the Net. Hastings Communications and Entertainment Law Journal, Vol. 19. 26. Yoches, E. Robert & Levine, Arthur J. (1989, May). Basic principles of copyright protection for computer software. Communications of the ACM Vol. 32 No. 5. pp. 544. 27. Zwass, Vladimir. (1997, Spring). Editorial Introduction. Journal of Management Information

Systems, Vol. 13, No. 4, pp. 3- 6. 29 Appendix C Bibliography 1. American Marketing Association (2001). Full Text of the AMA Code of Ethics [online].

Available: http://www. ama. org/about/ama/fulleth. asp. (October 26, 2001). 2. Berman, J. & Weitzner, D. (1995). User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media. Yale Law Journal, Vol. 104, pp. 1619. 3. BRINT Institute. (2001). Intelectual Property: Copyright, Trademarks and Patents. [online]. Available: http://www. brint. com/IntellP. htm. (October 26, 2001). 4. British Computer Society. (2000). British Computer Society Code of Practice [online]. Available: http://www. bcs. org. uk/aboutbcs/cop. htm. (November 30, 2001). 5. CETUS. (1995).

Fair Use: A Statement of Principle [online]. Available: http://www. cetus. org/fair4. html. (December 1, 2001). 6. Cheng, H. K. , Sims, R. R. , and Teegen, H. (1999, Spring). To Purchase or to Private Software: An Empirical Study. Journal of Management Information Systems Vol. 13, No. 4, p. 49- 60. 7. Gopal, R. D. , & Sanders, G. L. (1997, Spring). Preventive and Deterrent Controls for Software Piracy. Journal of Management Information Systems Vol. 13 No. 4. pp. 29- 47. 30 8. Hinman, Lawrence M. (2001, September 15). Ethic Updates [online]. Available: http://ethics. acusd. edu/index. tml. (October 25, 2001). 9. Jamison, B. , Gold, J. & Jamison, W. (1997). Electronic Selling: 23 Steps to ESelling Profits. New York, NY: McGraw Hill. 10. Lending, D. & Slaughter, S. A. (2001, April). Research in progress: the effects of ethical climate on attitudes and behaviors toward software piracy. Proceedings of the 2001 ACM SIGCPR conference on Computer personnel research. p. 198- 200. 11. Limayem, Moez, Khalifa, Mohamed , Chin, Wynne

W. (1999, January). Factors Motivating Software Piracy. Proceeding of the 20th international conference on Information Systems, p. 124- 13. 12.

Scott, Thomas J. , Kallman, Ernest A. , Lelewer, Debra. (1994 November). Ethical Issues Involving the Internet. Proceedings of the conference on Ethics in the computer age. pp. 31- 32. 13. Thong, J. Y. L. , & Yap, C. - S. (1998, Summer). Testing and Ethical DecisionMaking Theory: The Case of Softlifting. Journal of Management Information Systems Vo. 15, No. 1. pp. 213- 237. 14. U. S. Department of Energy Computer Incident Advisory Capability Information Bulletin. (1998, March 12). Internet Cookies. [online]. Available: http://ciac. llnl. gov/ciac/bulletins/i- 034. shtml. (October 26, 2001). 31