ETHICAL ISSUES IN THE INFORMATION AGE

Dominique Louis, Pace University, 163 Williams Street, New York, N.Y. 10038, Tel. 212-346-1687
Email: capital402000@yahoo.com

ABSTRACT

The technological revolution with its concomitant technologies is accompanied by an accelerating shift in work relations that focuses on connectivity, interdependence and dynamism. Along with this change in relations, new ethical cultures and responsibilities are evolving at different levels: individual, corporate and governmental. This paper examines the importance of the ethical issues that stem from the adoption of Information Technology in the digital economy, as shaped by the five ethical aspects in the Information Age, highlights the effective strategies of Information Technology related opportunities, challenges and solutions, and concludes by offering some possible research questions and hypotheses for future study.

INTRODUCTION

With the explosive growth of Information Technology over the last decades, contemporary organizations adopt the efficacy of information systems in their strategy as one of the avenues to achieve competitive advantage and differentiate themselves in the marketplace. Yet, the evolution of information systems necessitates changes that disrupt the existing equilibrium of rights and obligations and force previous practices become obsolete. The objectives of this paper are to powerfully illustrate the ethical aspects of information systems: Privacy Rights, Intellectual Property Rights, Liability and Authority to Command, Information Systems Standards, and Quality of Life, further discuss the Value of Information Technology, and eventually highlight the Opportunities, Challenges and Solution*s* that can effectively inhibit and subvert unethical behavior. The research type is purely descriptive.

BACKGROUND

The term **ethic**s derives from the Greek word "**ethik**e" meaning **character** precisely because the ancient Greeks conceived an excellent character by the impacts of individual behavior upon it, as portrayed by Aristotle in 350 B.C. [9, chap. I] Consequently, ethics refer to the moral values of right or wrong that dictate and direct individual behavior. [6, p. 148] In the digital regime, the introduction of IT as a vehicle to achieve optimal performance produces *opportunities for development as well as threatening risks* in every societal level. Therefore, in an **ethical analysis**, ethical conduct is created by the approaches and interactions of three contributors: The *IT professional* is an ethically driven decision-maker. The *real world* reflects an enormously perplexing environment of constant changes incurred by individuals, cultures, products, or events. The r*esources for ethics valuation* embrace moral values, laws, codes of ethics, and core principles, as fundamentally established and solidified by ethicists. [1]

Acknowledgement: Dr. Jennifer D.E. Thomas, Professor of Information Systems, Pace University, who guided the development of the paper.

FIVE ETHICAL ASPECTS IN THE INFORMATION AGE

Growing at an astounding rate, IT enhancements permeate individual, social and political levels, thereby entailing concerns that espouse five ethical aspects: [6, p. 150]

- *Privacy rights*. What information rights are individuals and organizations entitled to?
- *Intellectual property rights*. How can intellectual property rights be safeguarded in a fluid environment where technological advancements facilitate bogus reproduction?
- *Liability and authority to command*. Who is liable when information or property rights are desecrated?
- *Information systems standards*. What system standards should we adopt to protect individual and collective rights?
- *Quality of life*. What principles should guide us in a digitally driven society? How do we ensure the appropriate level of trust that contributes into societal prosperity? [6, p. 150]

Privacy Rights

Privacy is the condition of individual freedom from *unauthorized observations*, or legislatively the right to control how collected information is used. [10, p 7] Thus, privacy reflects the claim to remain *unobserved* from individuals or organizations, including the state. [6, p. 155] On that basis, ethicists assessing the impact of IT on privacy focus their attention on "*the key issue of whether there indeed exists a morally legitimate sphere of privacy within the public domain – one that extends beyond matters of governmental oversight and surveillance – that should be recognized and protected"*. [4] In actuality, the constant challenge for the protection of individual privacy stems from the Internet technology and its architectural ramifications, where data transmission traverses through a vast network of networks - each capable of capturing and storing data traversing it - before it reaches its ultimate destination. In the same domain, web retailers use various sophisticated techniques to monitor individual web behavior and align their marketing directions accordingly. Within this context, **cookies** are small text strings that the website owner can place on a client computer, aiming to identify the visitor's web browser to track visits to the web site. [7, p. 342] **Web bugs** are also tiny graphic files in the form of hyperlinks that are built in e-mail messages or web pages to surreptitiously capture the reader of the e-mail messages or web pages, and report this information to another computer. [6, p. 159] Conversely, **spyware** can install itself on an Internet user's computer, inviting various web sites to transmit unsolicited material - including banner ads - to the user, while possibly reporting the user's Internet activity to other networks. [6, p. 159] IT advancements make it increasingly feasible for firms to engage in **employee workplace monitoring**, *involving the monitoring of employee web surfing and e-mail activity, in addition to the examination of files on an employee's office PC*, driven by a variety of incentives. [7, p. 449] **Loss of productivity** pertains to employee exceeding the allowable time for personal web surfing and e-mail use, whereas **harassment** targets to contain the offensive e-mail circulation, and the access of unacceptable content web sites, thus enforcing employee protection, while avoiding potential lawsuits. [7, p. 451] **Viruses** and other **malware** refer to security threats associated with the employee use of malicious software. **Trade secrets** and **commercially damaging behavior** might also imperil a firm's image since receiving confidential information concerning other companies can bestow legal penalties against a company, whereas disclosing trade secrets out of a company can cause even more irreparable harm. [7, p. 452]

Intellectual Property Rights

Intellectual property refers to the *intangible assets* created by individuals and organizations in their labor, and is legally protected under three domains: *trade secrets, copyrights* and *patents.* [6, p. 161]
Trade secret is the artifact of an intellectual effort that is used for business advantage, but, remains *confidential* and *publicly inaccessible*, and encompasses a variety of products including devices, formulas, and patents, or integrated procedures, such as computer programs with innovative features of functionality. In fact, trade secret law confers monopoly on the incentive idea in a work product, yet, with limitations, precisely because when a uniquely designed computer application becomes available to the public, from there on its uniqueness ceases to exist. [6, p. 161] **Copyright** is the legal right granted to intellectual property authors or creators to protect their effort from being variably *copied* during the author's life plus 70 more years after death, whereas corporate ownership copyright grant extends to 95 years after work initiation. [6, p. 161]] **Patent** is the exclusive invention right that the state confers to an inventor for 20 years. Fundamental considerations involve the *invention* idea and its *usefulness*, since the intent behind the law is to ensure that inventors enjoy the fruits of their labor, while making their work product available to the public, yet, only after users obtain license from the patent's owner. [6, p. 162]

Liability and Authority for Command

Top managers are particularly accountable for the coordination of activities between IT personnel and users to surmount conflicts, and assure that all parts of the enterprise entwine properly, thus working in unison. [9, chap. III] Additionally, upper management should be constantly vigilant on the information security governance across the organizational boundaries, since the most frequently reported security breaches in all sectors are virus attacks and insider abuses of about 75% and 50% respectively. [5]

Information Systems Standards

The ethical confrontation over accountability for unintentional consequences versus accountability for foreseeable implications invokes the legitimate question of *what constitutes an acceptable information system configuration*. As assessed, ineffective system performance derives from three basic elements: **software flaws**, **hardware** or **facility failures**, and **low input data quality**. Considering the fact that achieving a computer program with no flaws is almost unattainable, the implicit ethical concern that emerges here is *at what point of defectiveness a product should be released by a manufacturer.* [6, p. 166] Conversely, when program flaws are identifiable, yet, rectifiable only at a high cost, programs should be considered unaffordable and virtually worthless. Far worse hardware or facility failures are caused by natural or other causes. To prepare for these eventualities, top management should make a sizable investment in a quality information retrieval plan with an alternative facility operation location, that is continually updated and properly disseminated, fostering an atmosphere of watchfulness across the enterprise. With respect to the input data quality in the overall efficacy of systems, when input data is of low quality, contentious issues are invited that vouch for incidents with grave implications. [6, p. 166]

Quality of Life

IT effectiveness revolves around four significant characteristics: *processing power*, *storage capacity*, *ubiquity*, and *reproduction capability.* Yet, these unprecedented capabilities create equivocal challenges, such as: *How do unprivileged individuals establish trustworthiness in paperless operations*? [9, chap. X] Hence, IT innovative mechanisms illuminate the path for people with malicious intents to discover

system vulnerabilities as real incentives for damaging others. **Computer crime** is the illegal activity implemented using a computer or against a computer system, versus a **computer abuse** which is an illicit activity, yet, not illegal. **Spamming** is the popular abuse of sending unsolicited e-mail to a large number of Internet users with the impetus to promote products through the inexpensive digital dissemination. [6, p. 169] **Poising power** involves the decentralized decision-making to lower corporate level employees, who are given the authority to make low-impact decisions, yet only within their turf, while critical decisions remain still centralized. [6, p. 168] Leveraging IT to create competitive advantage induces **job loss.** Implicitly, *since empowerment is tantamount to bypassing middle management*, incompetent middle managers are inclined to lose their employment, while freshly educated workers for reengineered jobs enter the workforce. [6, p. 170] The ubiquity of IT also provides the fulcrum for the realization of **outsourcing** as a concept of exporting jobs to lower wage countries using the dynamic presence of IT at global distances. [9, chap. VII] This trend enables employee and overhead corporate control, while assisting agency managers to achieve desired aims in their search for qualified staff. [2] Unfortunately, growing economic inequalities stemming from social and cultural diversities provide the climate for the **digital divide**, a phenomenon that divides society into two parts: The uneducated, socially isolated and with no computer access workers, versus their digital counterparts of high computer literacy, exposure, and social existence. [6 p. 172] **Supporting balances** refers to the inescapable computing capability that assures reliable communications across vast distances, yet, erodes the traditional work versus family balances, coercing individuals into extended working hours rather than connecting with family and friends. [6, p. 168] Computing entails *health risks.* **Repetitive stress injury** - in particular the **carpal tunnel syndrome** - occurs when numerous muscle actions are repeated in the delivery of electronic transactions. **Computer vision syndrome** refers to the eye strain condition related to computer screen display, and lastly, the **technostress** is stress induced by computer use. [6, p. 172]

THE VALUE OF INFORMATION TECHNOLOGY

In some organizations IT adds tremendous value to their effectiveness empowering their capabilities in the achievement of high quality operations that subsequently increase customer loyalty and reliability in their respective fields. However, IT does not always provide benefits for a firm, since some IT projects can fail, thus yielding only negative impacts on organizational performance and reputation. [9, chap. XI] Therefore, IT impacts managerial decision making, precisely because novel technologies trigger rampant experimentation until they become fruitful. But, when they realize value, the yielded profits fuel the engine that enables executives to evolve the strategy targeting to achieve highly sustainable market share. In the electronic landscape of digital avenues and crossroads, the value of IT versus society has been portrayed from different ankles and aspects, because the more the power of technology increases, the more negative social costs IT creates. Thus, in spite of its advantages, IT is capable of potentially ruining cultural and societal values. [6, p. 168] Nonetheless, the relationship between Information Technology and society supports the fact that *IT is the available means for society to function*. [8]

OPPORTUNITIES, CHALLENGES AND SOLUTIONS

Opportunities

Top managers have the opportunity to cultivate a robust business environment that is lawful, impervious to breaches, and designed to thwart unethical conduct across the enterprise. The importance of a unified cultural plan with integrated policies and standards that define goals and objectives is invaluable. [6, p.

173], [6, p. 162] Ethics and morals should take precedence at the top of hiring checklists with the intent to raise awareness of the consequences yielded by employee unethical behavior, since many IT executives have expressed concerns about technical workers engaging into circumventing security systems. [3]

Challenges

Since IT precipitates changes that must be linked and aligned with the rest of the organizational IT infrastructure in the pursuit of targeted goals, rapid changes impact prevailing procedures thus heightening moral risks that innovators need to conceptualize and prevent. Thus, establishing ethical policies that espouse relevant IT issues is considered mandatorily indispensable, along with an appropriately administered training program that provides insight into the consistency between organizational conduct and organizational culture. [9, chap. III]

Solutions

Large corporations have long developed corporate information systems Code of Ethics to guard against employee unethical conduct. On this ground, top executives are absolutely responsible for the development of those Information Systems Codes of Ethics that espouse ethical concerns stemming from the five ethical aspects of information systems as outlined, and moreover inexhaustibly rekindle and enforce their applicability across the corporate landscape. [6, p. 174]

METHODOLOGY

The literature includes information extracted from regular and electronic textbooks, regular and computer magazine articles, journals, and university websites. The type of sampling was based on novice and advanced computer users. Research activity was enticing, yet, with limitations, such as the fruitless attempt to extract statistical information for an imagery illustration of the scope and severity of ethically indecorous behavior.

FUTURE DIRECTIONS

The continuing transformation of IT into a commodity entails the adoption of advanced measures for the protection of assets. Issues that can be further investigated, are: **Question 1:** *Does Information Technology promote better working conditions for users?* **Hypothesis 1:** *When top managers invest on the intelligent application of Information Technology, users will enjoy working toward fulfillment of the organizational mission.* **Question 2:** *What are the measures that organizations need to take to secure themselves?* **Hypothesis 2:** *When organizations employ stringent risk management controls, they secure themselves to prevent illegitimate interaction.*

CONCLUSION

Information Technology was born of strategic motivation to bring an entirely different set of dynamics in the administration of different economic goals. As needs evolve incrementally, employees and managers are expected to coordinate their efforts and activities aiming to achieve a common purpose and create shared value. However, in the realization of business objectives, the risks that IT creates become more important than the advantages it provides. Therefore, taking sufficient care to deter unethical entanglements should be the fundamental driver in the individual, organizational, social, and

political environments. In essence, the technological regime should be structured to function reliably, consistently, and efficiently, bridging ethics over the delivery of flawless execution, as a necessary precondition to the development of trust that subsequently engenders loyalty in the aggregate welfare.

REFERENCES

[1] Agresti, William W. (July 2004), *CE2IT: Continuous Ethics Enhancement for IT Professionals*, IT Professional Magazine, 6(4), 64, 61-63. Retrieved April 16, 2009, from the ABI/INFORM Global database. http://www2.computer.org/cms/Computer.org/dl/mags/it/2004/04/figures/f40641.gif

[2] Epstein, Dan. (2008), *Agency Outsourcing is All About Productivity, Not Just Downsizing*. National Underwriter / Property & Casualty Risk & Benefits Management, Dec. 15, 2008, Vol. 112, Issue 47, p-17-18, 2p. Retrieved May 3, 2009 from the Business Source Premier database.

[3] Hoffman Thomas. (2008), *IT Execs Put Ethics, Morals At Top of Hiring Checklists,* Computerworld, Nov. 17, 2008, Vol. 42, Issue 46, p 8-8, 1/3p; (AN 35451456). Retrieved April 24, 2009 from the Business Source Premier database.

[4] Johnson, Deborah, Nissenbaum, Helen, Mulligan Deirdre, & De George, Richard. (2006, 2007). *Privacy in Public: Ethics, Privacy and the Technology of Public Surveillance*. Retrieved April 16, 2009 from Indiana University Bloomington, Poynter Center http://poynter.indiana.edu/privacy.shtml

[5] Johnston, Allen C., & Hale, Ron. (2009), *Improved Security through Information Security Governance,* Communications of the ACM, Jan. 2009, Vol. 52, Issue 1, p 126-129, 4p, 3 charts. Retrieved March 10, 2009 from the Business Source Premier database.

[6] Laudon, Kenneth C., & Laudon, Jane P. (2006), *Management Information Systems, Managing the Digital Firm*, Upper Saddle River, New Jersey, Pearson Education, Inc.

[7] Panko, Raymond R. (2004), *Corporate Computer and Network Security*, Upper Saddle River, New Jersey, Pearson Education, Inc.

[8] *Phenomenological Approaches to Ethics and Information Technology* (2005) Retrieved April 16, 2009 from the Stanford Encyclopedia of Philosophy http://plato.stanford.edu/entries/ethics-it-phenomenology/

[9] Schultz, Robert A. (2006), *Contemporary Issues in Ethics and Information Technology*, Hershey, PA: IRM Press. Retrieved on March 12, 2009 from: http://library.books24x7.com/book/id_12289/viewer.asp?booid=12289&chunkid=0674066103

[10] Whitman, Michael E., & Mattord, Herbert J. (2004). *Management of Information Security*, Boston, Massachusetts: Thomson Learning, Inc., Course Technology