

Importance of Computer Ethics and Morality in Society

Ruobing Wang^{1*}

¹ *Engineering and Computer Science, Syracuse University, Syracuse, NY, the U.S., 13244*

**Corresponding author's e-mail: rwang79@syr.edu*

ABSTRACT

Computer ethics emerged in the 1980s as a field that deals with the ethical analysis of privacy and security issues in technology. The field is responsible for analyzing the moral duties of computer users and professionals and ethical issues in public policy. The digital advances in this essay are considered to cause related ethical problems both in workplaces and daily routine at the same time, e.g., cyber frauds, data abuse, and so forth. With these issues as the background, by using a literature review and case study, this essay takes the connection between cybercrime and ethical issues as the subject, discussing the risky consequences of lack of computer ethics and the positive impact of computer ethics, with its feasibility and necessity. Firstly, some citations from previous scholars interested in related subjects are applied in this essay, with the purpose of collecting a range of negative circumstances and data from official institutions, attached with ethic problems and computer usage. Then, this research mainly focuses on recently increasing cyber-crimes and privacy breach cases, through the provision and in-depth analysis of data over the years, to explore the causes of the current situation. Finally, it develops a series of effective recommendations in order to cope with the increased cases reported by cybercrime victims in this essay, based on the outcomes analyzed from previous data and cases. This paper finds the universality of computer technology brings ethical problems. Many data leakage and information abuse will contribute to a very serious negative impact on both individuals and society. However, once people have computer ethics and morality, it will be a very effective way in helping current problems.

Keywords: *computer ethics, computer morality*

1. INTRODUCTION

Ethics deals with the analysis of human attributes, social structures, and policies. Ethics helps us distinguish good from bad, and right from wrong. There are two common theoretical approaches that ethicists try to depict our moral intuitions about what is right and wrong. These are deontology and consequentialism (Gotterbarn, 2020).[2] Deontology approaches summarize that the moral duties of an individual are independent of any good or bad outcome that may arise. Consequentialism explains that human actions are wrong to the point that they have bad outcomes. Although there are ethical principles that usually inform legislation, it is recognized in ethics that legislation cannot work in place of morality. As a result, corporations and individuals are obliged to not only consider the legality but also the morality of their deeds. There are many questions regarding ethical issues which require ethical analysis. In ethical analysis, the moral

dilemmas present in the ethical issues are clarified and a proposition of solutions is made.

Today, computer ethics has evolved dramatically. Through this evolution, it has created problems as well as the importance in most activities within a society. Natalia et. al (2018) [9], explain that through computer advancements and constantly changing nature, the area of computer technology is one that is tough to assign a specific set of moral codes. Moreover, computing creates a variety of ethical problems (Natalia, et. al) [9]. This paper discusses both the importance and consequences of lack of computer ethics. Some of the consequences discussed include increased cyber-crimes such as money practices, telemarketing funds Computer privacy, and the arrival of artificial and system experts are discussed. The significance of computer ethics that are discussed includes societal well-being, honesty and trustworthiness, safeguard of data, privacy respect, creation of job opportunities.

2. CONSEQUENCES OF LACK OF COMPUTER ETHICS

The need for computer ethics is a result of the adverse effects brought by computers in society. This is because although society has benefited from the use of computers, there have been some adverse issues accompanied by their use. There are issues such as computer crime has proved to be expensive as companies lose a lot of money annually. A lot of money has been devoted to curbing these issues for instance, repairing damages caused by hackers and those who create viruses. The costs are also attributed to the unreliable hardware and software, abandoned

systems and also lawsuits resulting from privacy invasions and mix-ups of databases.

2.1 Increased cyber crimes

According to recent studies [5][6], companies are facing problems as a result of the growing number of computer crimes attributed to technological advancements. Examples of these malpractices are ATM frauds, money exchange and mobile frauds, and telemarketing frauds. Here are some related tables and diagrams illustrating the number of cyber-crimes, losses reported and related complaints that occurred in the U.S.A.

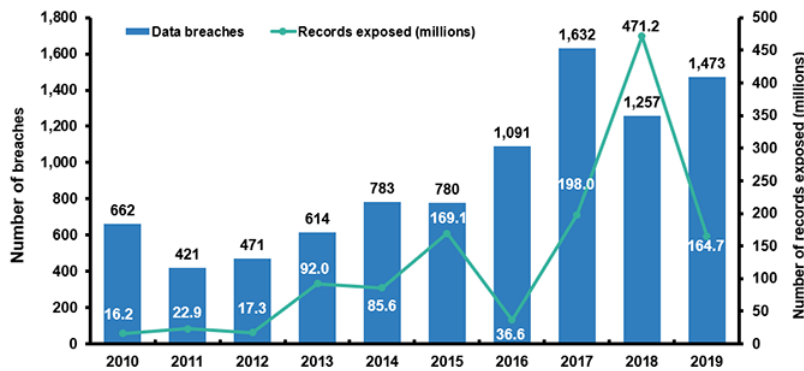


Figure 1. Number of Data Breaches and Records Exposed, 2010-2019

(Source: Identity Theft Resource Center, 2019 End of Year Data Breach Report)

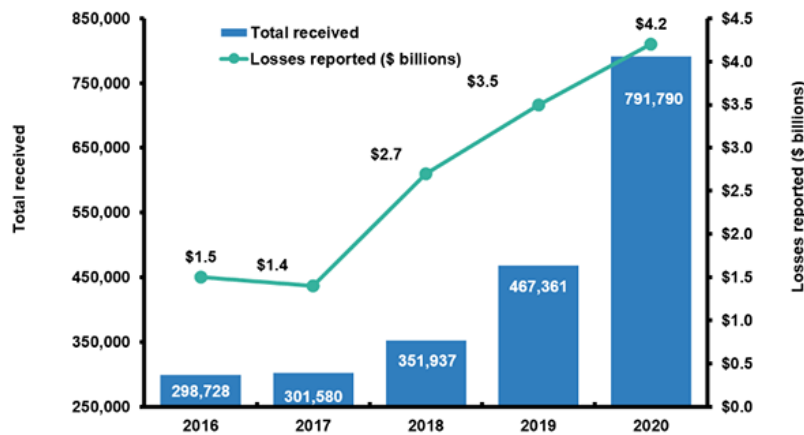


Figure 2. Cybercrime Complaints and losses reported, 2016-2020

(Source: Internet Crime Complaint Center)

In modern society, computer unreliability is becoming a major issue; United States estimates that as much as \$4 billion a year is attributed to computer crashes or downtime. Human lives have also been endangered as a result of computer unreliability when software with bugs is used to control aircraft, railroad signals, and even systems for dispatching ambulances.

The unreliability results from the computer complexity hence the need to be thoroughly tested before use. Computer systems can be unmanageable because of their massive complexity and can consequentially result in high-cost overruns. Therefore, computer professionals are exploring different ways to upscale the quality of software, but the progress is moving slowly.

2.2 Computer Privacy

Computer privacy is another issue that is becoming intractable in the current society where computer systems are used to store, process, manipulate, and transmit a lot of information regarding individuals and organizations. Issues related to database management such as mistaken identities, mix-ups and manipulated, data usually occur because we put too much trust in information that is stored electronically (Weiss, 1987) [13]. There have been cases of interference of personal information such as driver's licenses and credit card which have resulted in miseries. Data stored by national security agencies such as the FBI, the United Kingdom's Police Commission (PNC) and other agencies has led to concerns regarding the quality and volume of the information that they possess. There have been controversies over such practices by the agencies such as monitoring of email, database marketing, and even calling number identification on mobile phones. This has pushed governments around the world into tightening and strictly adhering to privacy laws

2.3 Arrival of artificial intelligence and expert systems

Technology advancements have led to the arrival of artificial intelligence (AI) and expert systems which have resulted in ethical, technical, and legal issues. These problems have derailed advancements towards the holy grail of AI as many people are still skeptical about it. There have been questions on whether computers can be ever trusted to make judgments involving legal, political, and administrative matters (Barnard, De Ridder, Pretorius, & Cohen, 2003) [1]. For instance, there is still uncertainty whether computers can be trusted to run aircraft control systems or even nuclear power stations without human backup given that we are aware of the bugs that are present in software. The use of expert systems and AI in day-to-day activities has been deterred by legal laws that discourage people from using them. There are critics who are still questioning if AI is really a proper goal for humans and if there is a need to replace human labor in carrying out tasks when unemployment is still a problem.

A number of ethical issues have been raised despite the fact the option to commit or not commit malpractice should not bring any amoral dilemma for the general population. Some people have gone to the extent of making a distinction between crimes against individuals and victimless crimes against institutions such as banks and companies. However, it is hard to categorize a company as a lesser victim compared to an individual especially when it involves wealth deprivation. Today it is not uncommon to find some people copying computer software while justifying that many people do it or

because some well-known software is very expensive. This is despite the fact that they are aware that doing so is a blatant infringement of the owner's rights and is therefore against the law. Therefore, there is a need to protect the rights of the respective companies to ensure the computer industry keeps moving.

2.4 Workplace computerization

Computer ethics involves the protection of individuals from online predation by disallowing the use of proprietary software without permission, privacy breaching, work interference, among many other occurrences. Over the past years, computing field has never had time or organizational ability to formulate a set of moral rules to govern the industry. However, with the current advancements in technology there has been need to lay down a set of rules to govern the computing field and the computer professionals. For instance, today a programmer is required to have a certificate of competency before being granted permission to work on major projects especially those involving systems that support life. This will ensure that computer professionals are certified, which will help reduce bugs present in software, limit malfunction risks, and even reduce incidences involving project runaways.

Although advancements in technology have improved our lives, they have consequentially led to ethical dilemmas which have threatened professions. There have been several malpractices that have been encountered in the past years which include; privacy invasion, phishing, pornography, computer viruses, and thefts (Barnard, De Ridder, Pretorius, & Cohen, 2003). As a result, it has become essential to understand the importance of computer ethics in order to create a sound environment for computer operations. These ethics cover the following fields of computer usage all over the world; financial, social, and legal fields. Computers can be manipulated to undertake many functions that can be applied in diverse places in society as a result of the new computing technology (Williams 1997). The importance of computer ethics is paramount because.

3. POSITIVE IMPACTS OF COMPUTER ETHICS

3.1 Individuals and further developments

3.1.1 Fosters computer knowledge and understanding

It helps us understand the good and bad outcomes when using the computer online. For instance, hacking can be either good or bad. Hacking is bad when the aim is to steal security log-ins and steal data from a company or an institution. This typically is a bad act that should not be attempted at all costs. On the other

side, there hacking can help government agencies such as the FBI to acquire crucial and fundamental information when locating criminals and terrorists. Therefore, computer ethics helps us clearly comprehend the good and bad outcomes of using computers and as a result aid us in operating computers properly without breaking the code of conduct (Mohsin, 2020) [7].

3.1.2 Enhances safety of data

Safety of data. Apart from communication, computers are used to store various types of data. Therefore, it is up to you to decide what you get involved in accessing or downloading online. This is because coming in contact with malicious sites and platforms invites different types of viruses that can obviously get into your computer and cause it to crash. However, if you use your computer as it is supposed to be used, you are creating a safe haven for your work and personal information (Nissenbaum, 2017) [10]. Computer ethics aim to ensure that you are using your computer as per the stipulated guidelines to ensure that you data and information is safe from malicious activities.

3.1.3 Promotes honesty and trustworthiness

It promotes honesty and trustworthiness among the computing professionals. This will derail them from making deliberate deceptive advances but will on the contrary reveal or disclose their intentions and also disclose certain limitations pertaining to a system or system design. (Schinzinger & Martin, 2017) [11]. Confidentiality to the stakeholders should be respected unless stated otherwise by the law requirements.

3.2 Social advance and legal enhancement

3.2.1 Increases societal well-being

It contributes to the well-being of the society. Fundamental human rights are protected and the culture diversity is respected. This is because computing essentials aim at minimizing negative impacts that result from the computing systems which include safety and health threats.

3.2.2 Creates job opportunities

It promotes jobs of computer professionals who develop software. Software developers are professionals who develop various computer software and programs in technical companies. Software piracy can cost these professionals a fortune when people access the software without paying for them. Most people will think that accessing the software illegally would not affect the respective companies because of the ideology that they are rich or even if it does affect them, nobody cares. This continued mindset where people prefer piracy to

buy software can negatively impact the software companies as there are thousands of people involved in unethical purchases and distributions. Therefore, there is a need for cushioning by a set of rules and guidelines that form computer ethics which ensure that the software developers are not affected by the already stated malpractices.

3.2.3 Property rights are followed

Property rights are honored. It is against the law to bridge terms of agreement, copyrights, and trade secrets. Proper authorization is mandatory when making copies of software whereas it is illegal to make unauthorized duplication of software and other files. This enables computer and software users to be ethical and responsible as it is against the law to transact businesses dealing with pirated copies of software.

It ensures proper credit is given for intellectual property. It is the work of computing professionals to take care of all intellectual property and it is illegal for one to take credit for other people's work and ideas even in cases where there is no copyrights protection.

3.3 Public information security

3.3.1 Avoids misuse of personal information

It prevents deliberate misuse of personal information. When we read the terms and conditions outlined by the computing professionals, we are confident that our credentials will not be used for any bad intentions. This is because, most of the time we are obliged to disclose our personal information when accessing systems which can be very risky.

3.3.2 Privacy is respected

It ensures that the privacy of others is respected. Computer professionals are obliged to maintain integrity of personal data due to increased possible violations of privacy of personal information brought by the current computing technology. It is the duty of the professionals to make sure that the data or the information transmitted is accurate while protecting any access or disclosure that is unauthorized. In addition to that, there is need of laying down procedures to enable corrections and reviews of errors by the individuals (Moor, 2017) [8].

3.3.3 Reduces spread of false information

It plays a fundamental role in reducing the spread of false information. Social media usage triggered an explosion in the spread of information today. This also implies that false and unverified information or news can spread fast through emails and networking sites. It is, however, against code of conduct to circulate inaccurate information. There have been many incidences where pop-ups and mails are used to circulate

false information or give alerts which are not true with the intent of marketing and selling certain products. Therefore, computer ethics ensures that there is no direct or indirect involvement in spreading information that is inaccurate or unverified as the information can hurt or harm other individuals or organizations.

3.4 Timely and effective supervision

3.4.1 Controls the use of artificial intelligence

It will help govern the use of artificial intelligence. Artificial intelligence has raised a lot of questions which are of vital importance and should be studied as it has opened up a wide range of applications. Some are scared about the use of robots in our daily lives and how they will interact with humans (Lunker, 2008). These concerns should be looked into by computer professionals and this can only be done when there are sets of rules which can govern their operations and the field at large.

3.4.2 Computer and internet advancement

The rapid development in Internet and computer technology leads to the growth of Internet crime, which can affect any region or country in the world. Awareness raising and legislation are therefore needed to prevent crimes related to computers and the Internet. There need to be laws to stipulate a set of rules that would ensure that there is efficient and reliable communication and transmission of information (Khan et al., 2020)[4]. The rules should also discipline individuals and organizations who take part in malpractices and take necessary actions to prevent occurrences that may cause harm to others.

4. CONCLUSION

Computer ethics is something that we should abide by out of our own free will and desire rather than being forced on us. Without effective supervision and comprehensive legislation, ethics and morality problems may occur frequently when using computers. Since there lack of compulsive and comprehensive laws towards cyberspace, it can be more difficult for everyone to abide by moral requirements. As we mentioned before, an increasing number of cases reporting cyber-crimes may cause a huge loss of social value and property damage to the public. Hence, if we attach enough significance to cope with issues, people can use their computers in a more secure environment. With the rising improvements in technology, the ethical application is crucial in developing and implementing strategies. Apart from improving peoples' security, it would be a remarkable advance both on legislation and technology. The authorities need to implement strict rules and regulations to ensure all computer users are responsible and answerable to their actions. This essay

analyzes the causes of cybercrime and identifies the need and urgency of applying computer ethics and morality. Meanwhile, it also reminds readers of the diverse cybercrime forms and the magnitude of the danger it poses, which must be brought to the attention of the public and the government.

AUTHORS' CONTRIBUTIONS

This paper is independently accomplished by the author.

ACKNOWLEDGMENTS

Firstly, I would like to thank my mentor, Min Han, who supports me and provides me numerous considerate suggestions all the time. Without her help, I would not be able to complete this essay honestly. Then, I am grateful to these scholars and researchers who make efforts to study these programs. Absorbing so much inspiration from their works and literature, I could determine the structure and content of my essay. Finally, I want to say thanks to my friends and classmates, for their endless supports and encouragement during my writing.

REFERENCES

- [1] Barnard, A., De Ridder, C., Pretorius, L., & Cohen, E. (2003). Integrating computer ethics into the computing curriculum: A framework for implementation. Proceedings of the 2003 InSITE Conference. doi:10.28945/2619
- [2] Gotterbarn, D. (2020). The use and abuse of computer ethics. *The Ethics of Information Technologies*, 335-340. doi:10.4324/9781003075011-24
- [3] Introduction to information technology and intellectual property law. (2019). *Information Technology and Intellectual Property Law*. doi:10.5040/9781526506870.ch-001
- [4] Khan, M. U., Sajid, Z., Sohail, M., Aziz, S., Ibraheem, S., & Naavi, S. Z. (2020). Electrohysteroqram based term and preterm delivery classification system. 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH). doi:10.1109/smart-tech49988.2020.00033
- [5] Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, 45(3), 58-74.
- [6] Lallie, H. S., Shepherd, L. A., Nurse, J., Erola, A., & Bellekens, X. . (2020). Cyber security in the age

of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic.

- [7] Mohsin, K. (2020). Global perspective of cybercrimes and related laws. SSRN Electronic Journal. doi:10.2139/ssrn.3673938
- [8] Moor, J. H. (2017). What is computer ethics? *. *Computer Ethics*, 31-40. doi:10.4324/9781315259697-7
- [9] Natalia, P., Paschkevich, V., Haftor, D. (2018). Ethical Reflections on Consequences of Technological Displacement. *Reason, Faith and Practice in Our Common Home*, 186.
- [10] Nissenbaum, H. (2017). Protecting privacy in an Information Age: The problem of privacy in public. *Computer Ethics*, 331-368. doi:10.4324/9781315259697-35
- [11] Schinzinger, R., & Martin, M. W. (2017). Commentary: Informed consent in engineering and medicine. *Engineering Ethics*, 253-263. doi:10.4324/9781315256474-22
- [12] Selwyn, N. (2018). Telling tales on technology: The ethical dilemmas of critically researching educational computing. *Ethical Dilemmas in Qualitative Research*, 42-56. doi:10.4324/9781315186894-5
- [13] Weiss, E. A. (1987). Self-assessment procedure XVII. *Communications of the ACM*, 30(10), 886-890. doi:10.1145/30408.30421