



(/home)

[BLOG \(/BLOG\)](#)[HELP \(/HELP\)](#)[CONTACT \(/CONTACT-US\)](#)[LOGIN \(/MEMBERS\)](#)[ABOUT \(/ABOUT\)](#)[CHAPTERS \(/CHAPTERS\)](#)[PROGRAMS \(/PROGRAMS\)](#)[EVENTS \(/TECHNOLOGY-EVENTS\)](#)[BENEFITS \(/BENEFITS\)](#)[JOIN NOW \(/JOIN-NOW\)](#)[Home \(/\) / Blog](#)

BLOG

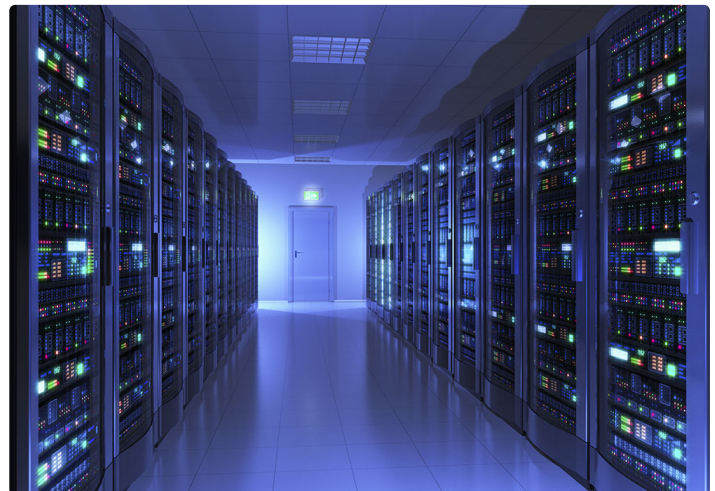
ETHICAL PROBLEMS IN COMPUTING

 Jul 4, 2017, 15:46 PM /  Lou Berzai

Editor's Note: This is the third of a series of articles on Ethics from 1991 AITP President and faculty member of the University of Notre Dame, Lou Berzai, CSP, CCP. This article was a paper from some theories discussion in Lou's ethics classes.

The first two articles are:

- *How Ethical Theories Apply to IT Professionals*
(<http://192.168.0.142/blog/aitp-blog/2017/06/27/how-ethical-theories-apply-to-it->



professionals)

- *Ethical Decision Making and the IT Professional*

(<https://www.aitp.org/blog/aitp-blog/2017/06/29/ethical-decision-making-and-the-it-professional/>)

Because of its constantly changing nature, the area of computer technology is one that is difficult to assign a specific set of moral codes, although it is necessary that ethics be considered when making decisions in this area. Computing creates a whole new set of ethical problems, unique unto itself.



(https://www.aitp.org/join-now/?utm_source=aitp-blog&utm_medium=ad&utm_campaign=student-membership&utm_content=ethical-problems-in-computing)

Such problems include:

"...the unauthorized use of hardware, the theft of software, disputed rights to products, the use of computers to commit fraud, the phenomenon of hacking and data theft, sabotage in the form of viruses, responsibility for the reliability of output, making false claims for computers, and the degradation of work." (Forester 4)

These problems engender a whole new set of ethical questions, including:

- "is copying software really a form of stealing"
- "are so-called 'victimless' crimes... more acceptable than crimes with human victims"
- "does information on individuals stored in a computer constitute an intolerable invasion of privacy?" (Forester 4 – 5)

These questions demand that ethical principles be applied to their resolution because without the consideration of ethics, these gray areas can easily become completely black.

To begin with, it seems that there are four big areas of computer ethics. They are "(1) computer crime; (2) responsibility for computer failure; (3) protection of computer property, records, and software; and (4) privacy of the company, workers, and customers". (De George 338) This part of our discussion will focus primarily on computer crime and privacy.

Computer Crime

Computer Crime is intellectual, white-collar crime. Those that commit such crimes must be intelligent enough to manipulate a computer system and in such a position to access it in the first place. One example of computer crime is stealing funds via computer. Often the worst that can happen to such a thief is that he/she is merely required to return the stolen money. Many times that person will be fired, assuming he/she is an employee, but may be quickly hired by a competitor because of his/her skill. This creates practically no deterrent to committing computer theft because legal action is not often taken against the perpetrator.

Another example is unauthorized computer entry. In entering a computer unauthorized, the perpetrator can steal a company's trade secrets and data. Such a crime could be committed by an employee aiming to sell such secrets to a competitor or by an outside source wanting to steal such secrets to promote his/her own well-being. This crime involves both an invasion of property and privacy and also compromises the computer system itself.

This crime goes along with the idea of hacking. Hacking is defined as "any computer-related activity which is not sanctioned or approved of by an employer or owner of a system or network" (Forester 44). Such an activity deals with the ethical dilemma of who actually owns information and who should have access to that information. At many universities, Computer Science professors have their students hack into the university's system to prove their skill and knowledge of computer systems.

This poses a serious ethical dilemma. Since the students are not causing any harm to the system, is such an action morally reprehensible or acceptable? Many computer professionals feel that this act is not ethically sanctioned and the Computer Science professors must address the issue of computer ethics more fervently in their classes.

Privacy

Another area of computer ethics regards privacy. The privacy issue focuses on the computer's most basic functions, "its capacity to store, organized, and exchange records". (Johnson 58) A great deal of the concern has to do with the amount of information gathering that is made possible by computers. This puts people's personal information in a vulnerable position. If someone hacks into a computer system, all this information is at his/her disposal. In this way, such crimes as identity theft can occur.

Furthermore, when stored information can be easily exchanged, the effect of a small error can be magnified. Such errors can stay in the system indefinitely. Computers "create the possibility that incidents in one's life or errors in one's records will follow one through life, profoundly affecting how one is perceived and treated". (Johnson 60) It is because of this effect that people lose control over their lives and the information about them.

Thus it seems that there are both good and bad consequences of computerized records. A good consequence is that an organization's need for information suggests "access to relevant information might improve decision making and, therefore, make organizations more efficient". (Johnson 63) This in turn provides a positive result for the individual because it could mean better services or savings.

However, bad consequences still exist. These are related to the fact that "information is used to make decisions about individuals and such decisions may be based on irrelevant and inaccurate information." (Johnson 63) There is no way to insure that the power exercised by organizations because of this access to information is used fairly. Thus it seems that there should be a balance between the need for information on the part of an organization and the interests of the individual.

Ethical responsibility of IT pros

Another area of concern in conjunction with all of this has to do with the power computer professionals wield because of their knowledge of computer systems. Computer professionals can act in one of two ways: "(1) When it is unclear, assume information is in the public realm until there is some evidence that it is not; or (2) When it is unclear, assume information is private unless or until there is evidence that it is not". (Johnson 70)

It is desirable that a professional adopt the second rule because it allows the professional to protect him or herself from ethical indiscretions, while the first allow for a greater chance of ethical breach.

There are two main reasons for concern regarding this allocation of power to computer professionals. "First, increasing power in the hands of some often leads to exploitation of others, and this is an ethical matter. Second, certain kinds of power are necessary for a decent life, a moral life, and so this also may be an ethical matter". (Johnson 73)

Computer professionals should have an obligation to use the information they have access to in a proper manner, but some chose to use this information immorally to the detriment of others.

The power of the computer professional also poses a threat because it is entirely centralized. As noted previously, computers allow for large amounts of information to be stored in one small space. Concern about this centralization arose because "people reasoned that in a democratic society there is a struggle between the government and the citizenry such that as government agencies become more and more powerful, citizen control and citizen input may become less and less effective". (Johnson74) Some people fear that if the government has too much control over information, their privacy will be compromised. Those who do not want to see computers in the hands of the government but rather in the hands of individuals, oppose the centralization of power.

This idea of the centralization of power coincides with the concept that technology contributes to feeling of alienation. Alienation has to do with loss of control in the world in which one lives. This is visible in the fact that because of increased technology

advancements, computers have taken over jobs that once belonged to people.

An example of this is the concept of artificial intelligence (AI). This is an attempt by computer experts to simulate the components of human intelligence through machines. This engenders many ethical dilemmas, however, because it forces one to ask "not just whether AI itself is a possible goal, but whether AI is a proper goal of human endeavor". (Forester 129) It degrades the human condition to replace humans with intelligent machines, so is this really necessary? This ties in with the original dilemma about the power manifested in technology. It is of key importance that those who hold such power do not abuse it.

Computer technology brings about a whole new field of ethical dilemmas. From computer crime to privacy to the power of computer professionals, this technology has shifted the way the business world must think about ethical decisions. Yet this is difficult because there is no overarching positive ethical force in the American business community. Combined with the fact that technology changes so rapidly, it is hard to establish firm moral codes of conduct regarding computers and follow them strictly.

There are many gray areas for which to account. Many times people chose to blame the computers when they run into trouble. In reality, however, it is the people that make the mistakes because they are the ones that created the technology. People merely use computers as scapegoats to avoid responsibility. This is why it is of utmost significance to educate people about the power, and potential abuses, of computer technology. It is only in doing so that society will acquire a firm grasp of computer ethics and handle moral dilemmas regarding computing in an ethical and proper manner.

Ethical Problems in Computing Bibliography

Business Ethics – De George, Richard T. .Englewood cliffs, NJ: Prentice Hall, 1995

Ethics and the Management of Computer Technology – E. W. Michael Hoffman, Jennifer Mills Moore Cambridge, MA: Oelgeschlager, Gunn & Hain, Publishers, Inc., 1982

Computer Ethics – Forester, Tom and Perry Morrison Cambridge, MA: the MIT Press, 1990

Ethical Decision Making in Everyday Work Situations – Guy, Mary: New York: Wuorum books, 1990

Computer Ethics – Johnson, Deborah G. Englewood cliffs, NJ: Prentice-Hall, Inc., 1985



CompTIA

[About Us \(/about\)](#)

[Contact Us \(/contact-us\)](#)

 (<https://www.youtube.com/comptia>)

 (<https://www.facebook.com/comptiaaitp>)

 (<https://twitter.com/CompTIAAITP>)

 (<https://www.linkedin.com/groups/109439>)

CERTIFICATION

CompTIA IT Certifications (<https://certification.comptia.org/>)

Store (<https://www.comptiastore.com/>)

Blog ([/blog](#))

Account Login (<https://www.certmetrics.com/comptia/login.aspx>)

ASSOCIATION

CompTIA - The IT Industry Association (<https://www.comptia.org>)

CompTIA AITP – The IT Professional Association (/)

PARTNERS

CompTIA Authorized Partner Program (<https://partners.comptia.org/>)

GOVERNMENT RELATIONS

CompTIA Advocacy (<https://www.comptia.org/advocacy>)

PHILANTHROPY

Creating IT Futures Foundation (<https://www.creatingitfutures.org/>)

Copyright © CompTIA, Inc. All Rights Reserved

Terms of use (<https://www.comptia.org/terms-conditions>)

Privacy Statement (<https://www.comptia.org/privacy-statement>)

Trademarks (<https://www.comptia.org/trademarks>)