This is a file in the archives of the Stanford Encyclopedia of Philosophy.

version history	**Stanford Encyclopedia of Philosophy**	last substantive content change

HOW TO CITE THIS ENTRY

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

AUG 14 2001

This document uses XHTML/Unicode to format the display. If you think special symbols are not displaying correctly, see our guide Displaying Special Characters.

Computer Ethics: Basic Concepts and Historical Overview

Computer ethics is a new branch of ethics that is growing and changing rapidly as computer technology also grows and develops. The term "computer ethics" is open to interpretations both broad and narrow. On the one hand, for example, computer ethics might be understood very narrowly as the efforts of professional philosophers to apply traditional ethical theories like utilitarianism, Kantianism, or virtue ethics to issues regarding the use of computer technology. On the other hand, it is possible to construe computer ethics in a very broad way to include, as well, standards of professional practice, codes of conduct, aspects of computer law, public policy, corporate ethics--even certain topics in the sociology and psychology of computing.

In the industrialized nations of the world, the "information revolution" already has significantly altered many aspects of life -- in banking and commerce, work and employment, medical care, national defense, transportation and entertainment. Consequently, information technology has begun to affect (in both good and bad ways) community life, family life, human relationships, education, freedom, democracy, and so on (to name a few examples). Computer ethics in the broadest sense can be understood as that branch of applied ethics which studies and analyzes such social and ethical impacts of information technology.

In recent years, this robust new field has led to new university courses, conferences, workshops, professional organizations, curriculum materials, books, articles, journals, and research centers. And in the age of the world-wide-web, computer ethics is quickly being transformed into "global information ethics".

1. Some Historical Milestones

1940s and 1950s

Computer ethics as a field of study has its roots in the work of MIT professor Norbert Wiener during World War II (early 1940s), in which he helped to develop an antiaircraft cannon capable of shooting down fast warplanes. The engineering challenge of this project caused Wiener and some colleagues to create a new field of research that Wiener called "cybernetics" -- the science of information feedback systems. The concepts of cybernetics, when combined with digital computers under development at that time, led Wiener to draw some remarkably insightful ethical conclusions about the technology that we now call ICT (information and communication technology). He perceptively foresaw revolutionary social and ethical consequences. In 1948, for example, in his book *Cybernetics: or control and communication in the animal and the machine*, he said the following:

> It has long been clear to me that the modern ultra-rapid computing machine was in principle an ideal central nervous system to an apparatus for automatic control; and that its input and output need not be in the form of numbers or diagrams. It might very well be, respectively, the readings of artificial sense organs, such as photoelectric cells or thermometers, and the performance of motors or solenoids ... . we are already in a position to construct artificial machines of almost any degree of elaborateness of performance. Long before Nagasaki and the public awareness of the atomic bomb, it had occurred to me that we were here in the presence of another social potentiality of unheard-of importance for good and for evil. (pp. 27-28)

In 1950 Wiener published his monumental book, *The Human Use of Human Beings*. Although Wiener did not use the term "computer ethics" (which came into common use more than two decades later), he laid down a comprehensive foundation which remains today a powerful basis for computer ethics research and analysis.

Wiener's book included (1) an account of the purpose of a human life, (2) four principles of justice, (3) a powerful method for doing applied ethics, (4) discussions of the fundamental questions of computer ethics, and (5) examples of key computer ethics topics. [Wiener 1950/1954, see also Bynum 1999]

Wiener's foundation of computer ethics was far ahead of its time, and it was virtually ignored for decades. On his view, the integration of computer technology into society will eventually constitute the remaking of society -- the "second industrial revolution". It will require a multi-faceted process taking decades of effort, and it will radically change everything. A project so vast will necessarily include a wide diversity of tasks and challenges. Workers must adjust to radical changes in the work place; governments must establish new laws and regulations; industry and businesses must create new policies and practices; professional organizations must develop new codes of conduct for their members; sociologists and psychologists must study and understand new social and psychological phenomena; and philosophers must rethink and redefine old social and ethical concepts.

1960s

In the mid 1960s, Donn Parker of SRI International in Menlo Park, California began to examine unethical and illegal uses of computers by computer professionals. "It seemed," Parker said, "that when people entered the computer center they left their ethics at the door." [See Fodor and Bynum, 1992] He collected examples of computer crime and other unethical computerized activities. He published "Rules of Ethics in Information Processing" in *Communications of the ACM* in 1968, and headed the development of the first Code of Professional Conduct for the Association for Computing Machinery (eventually adopted by the ACM in 1973). Over the next two decades, Parker went on to produce books, articles, speeches and workshops that re-launched the field of computer ethics, giving it momentum and importance that continue to grow today. Although Parker's work was not informed by a general theoretical framework, it is the next important milestone in the history of computer ethics after Wiener. [See Parker, 1968; Parker, 1979; and Parker et al., 1990.]

1970s

During the late 1960s, Joseph Weizenbaum, a computer scientist at MIT in Boston, created a computer program that he called ELIZA. In his first experiment with ELIZA, he scripted it to provide a crude imitation of "a Rogerian psychotherapist engaged in an initial interview with a patient". Weizenbaum was shocked at the reactions people had to his simple computer program: some practicing psychiatrists saw it as evidence that computers would soon be performing automated psychotherapy. Even computer scholars at MIT became emotionally involved with the computer, sharing their intimate thoughts with it. Weizenbaum was extremely concerned that an "information processing model" of human beings was reinforcing an already growing tendency among scientists, and even the general public, to see humans as mere machines. Weizenbaum's book, *Computer Power and Human Reason* [Weizenbaum, 1976], forcefully expresses many of these ideas. Weizenbaum's book, plus the courses he offered at MIT and the many speeches he gave around the country in the 1970s, inspired many thinkers and projects in computer ethics.

In the mid 1970s, Walter Maner (then of Old Dominion University in Virginia; now at Bowling Green State University in Ohio) began to use the term "computer ethics" to refer to that field of inquiry dealing with ethical problems aggravated, transformed or created by computer technology. Maner offered an experimental course on the subject at Old Dominion University. During the late 1970s (and indeed into the mid 1980s), Maner generated much interest in university-level computer ethics courses. He offered a variety of workshops and lectures at computer science conferences and philosophy conferences across America. In 1978 he also self-published and disseminated his *Starter Kit in Computer Ethics*, which contained curriculum materials and pedagogical advice for university teachers to develop computer ethics courses. The *Starter Kit* included suggested course descriptions for university catalogs, a rationale for offering such a course in the university curriculum, a list of course objectives, some teaching tips and discussions of topics like privacy and confidentiality, computer crime, computer decisions, technological dependence and professional codes of ethics. Maner's trailblazing course, plus his *Starter Kit* and the many conference workshops he conducted, had a significant impact upon the teaching of computer ethics across America. Many university courses were put in place because of him, and several important scholars were attracted into the field.

1980s

By the 1980s, a number of social and ethical consequences of information technology were becoming public issues in America and Europe: issues like computer-enabled crime, disasters caused by computer failures, invasions of privacy via computer databases, and major law suits regarding software ownership. Because of the work of Parker, Weizenbaum, Maner and others, the foundation had been laid for computer ethics as an academic discipline. (Unhappily, Wiener's ground-breaking achievements were essentially ignored.) The time was right, therefore, for an explosion of activities in computer ethics.

In the mid-80s, James Moor of Dartmouth College published his influential article "What Is Computer Ethics?" (see discussion below) in *Computers and Ethics*, a special issue of the journal *Metaphilosophy* [Moor, 1985]. In addition, Deborah Johnson of Rensselaer Polytechnic Institute published *Computer Ethics* [Johnson, 1985], the first textbook -- and for more than a decade, the defining textbook -- in the field. There were also relevant books published in psychology and sociology: for example, Sherry Turkle of MIT wrote *The Second Self* [Turkle, 1984], a book on the impact of computing on the human psyche; and Judith Perrolle produced *Computers and Social Change: Information, Property and Power* [Perrolle, 1987], a sociological approach to computing and human values.

In the early 80s, the present author (Terrell Ward Bynum) assisted Maner in publishing his *Starter Kit in Computer Ethics* [Maner, 1980] at a time when most philosophers and computer scientists considered the field to be unimportant [See Maner, 1996]. Bynum furthered Maner's mission of developing courses and organizing workshops, and in 1985, edited a special issue of *Metaphilosophy* devoted to computer ethics [Bynum, 1985]. In 1991 Bynum and Maner convened the first international multidisciplinary conference on computer ethics, which was seen by many as a major milestone of the field. It brought together, for the first time, philosophers, computer professionals, sociologists, psychologists, lawyers, business leaders, news reporters and government officials. It generated a set of monographs, video programs and curriculum materials [see van Speybroeck, July 1994].

1990s

During the 1990s, new university courses, research centers, conferences, journals, articles and textbooks appeared, and a wide diversity of additional scholars and topics became involved. For example, thinkers like Donald Gotterbarn, Keith Miller, Simon Rogerson, and Dianne Martin -- as well as organizations like Computer Professionals for Social Responsibility, the Electronic Frontier Foundation, ACM-SIGCAS -- spearheaded projects relevant to computing and professional responsibility. Developments in Europe and Australia were especially noteworthy, including new research centers in England, Poland, Holland, and Italy; the ETHICOMP series of conferences led by Simon Rogerson and the present author; the CEPE conferences founded by Jeroen van den Hoven; and the Australian Institute of Computer Ethics headed by Chris Simpson and John Weckert.

These important developments were significantly aided by the pioneering work of Simon Rogerson of De Montfort University (UK), who established the Centre for Computing and Social Responsibility there. In Rogerson's view, there was need in the mid-1990s for a "second generation" of computer ethics developments:

> The mid-1990s has heralded the beginning of a second generation of Computer Ethics. The time has come to build upon and elaborate the conceptual foundation whilst, in parallel, developing the frameworks within which practical action can occur, thus reducing the probability of unforeseen effects of information technology application [Rogerson, Spring 1996, 2; Rogerson and Bynum, 1997].

2. Defining the Field of Computer Ethics

From the 1940s through the 1960s, therefore, there was no discipline known as "computer ethics" (notwithstanding the work of Wiener and Parker). However, beginning with Walter Maner in the 1970s, active thinkers in computer ethics began trying to delineate and define computer ethics as a field of study. Let us briefly consider five such attempts:

When he decided to use the term "computer ethics" in the mid-70s, Walter Maner defined the field as one which examines "ethical problems aggravated, transformed or created by computer technology". Some old ethical problems, he said, are made worse by computers, while others are wholly new because of information technology. By analogy with the more developed field of medical ethics, Maner focused attention upon applications of traditional ethical theories used by philosophers doing "applied ethics" -- especially analyses using the utilitarian ethics of the English philosophers Jeremy Bentham and John Stuart Mill, or the rationalist ethics of the German philosopher Immanual Kant.

In her book, *Computer Ethics*, Deborah Johnson [1985] defined the field as one which studies the way in which computers "pose new versions of standard moral problems and moral dilemmas, exacerbating the old problems, and forcing us to apply ordinary moral norms in uncharted realms," [Johnson, page 1]. Like Maner before her, Johnson recommended the "applied ethics" approach of using procedures and concepts from utilitarianism and Kantianism. But, unlike Maner, she did not believe that computers create wholly new moral problems. Rather, she thought that computers gave a "new twist" to old ethical issues which were already well known.

James Moor's definition of computer ethics in his article "What Is Computer Ethics?" [Moor, 1985] was much broader and more wide-ranging than that of Maner or Johnson. It is independent of any specific philosopher's theory; and it is compatible with a wide variety of methodological approaches to ethical problem-solving. Over the past decade, Moor's definition has been the most influential one. He defined computer ethics as a field concerned with "policy vacuums" and "conceptual muddles" regarding the social and ethical use of information technology:

> A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with new capabilities and these in turn give us new choices for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of computer ethics is to determine what we should do in

such cases, that is, formulate policies to guide our actions.... One difficulty is that along with a policy vacuum there is often a conceptual vacuum. Although a problem in computer ethics may seem clear initially, a little reflection reveals a conceptual muddle. What is needed in such cases is an analysis that provides a coherent conceptual framework within which to formulate a policy for action [Moor, 1985, 266].

Moor said that computer technology is genuinely revolutionary because it is "logically malleable":

Computers are logically malleable in that they can be shaped and molded to do any activity that can be characterized in terms of inputs, outputs and connecting logical operations....Because logic applies everywhere, the potential applications of computer technology appear limitless. The computer is the nearest thing we have to a universal tool. Indeed, the limits of computers are largely the limits of our own creativity [Moor, 1985, 269]

According to Moor, the computer revolution is occurring in two stages. The first stage was that of "technological introduction" in which computer technology was developed and refined. This already occurred in America during the first forty years after the Second World War. The second stage -- one that the industrialized world has only recently entered -- is that of "technological permeation" in which technology gets integrated into everyday human activities and into social institutions, changing the very meaning of fundamental concepts, such as "money", "education", "work", and "fair elections".

Moor's way of defining the field of computer ethics is very powerful and suggestive. It is broad enough to be compatible with a wide range of philosophical theories and methodologies, and it is rooted in a perceptive understanding of how technological revolutions proceed. Currently it is the best available definition of the field.

Nevertheless, there is yet another way of understanding computer ethics that is also very helpful--and compatible with a wide variety of theories and approaches. This "other way" was the approach taken by Wiener in 1950 in his book *The Human Use of Human Beings*, and Moor also discussed it briefly in "What Is Computer Ethics?" [1985]. According to this alternative account, computer ethics identifies and analyzes the impacts of information technology upon human values like health, wealth, opportunity, freedom, democracy, knowledge, privacy, security, self-fulfillment, and so on. This very broad view of computer ethics embraces applied ethics, sociology of computing, technology assessment, computer law, and related fields; and it employs concepts, theories and methodologies from these and other relevant disciplines [Bynum, 1993]. The fruitfulness of this way of understanding computer ethics is reflected in the fact that it has served as the organizing theme of major conferences like the National Conference on Computing and Values (1991), and it is the basis of recent developments such as Brey's "disclosive computer ethics" methodology [Brey 2000] and the emerging research field of "value-sensitive computer design". (See, for example, [Friedman, 1997], [Friedman and Nissenbaum, 1996], [Introna and Nissenbaum, 2000].)

In the 1990s, Donald Gotterbarn became a strong advocate for a different approach to defining the field of computer ethics. In Gotterbarn's view, computer ethics should be viewed as a branch of professional ethics, which is concerned primarily with standards of practice and codes of conduct of computing professionals:

There is little attention paid to the domain of professional ethics -- the values that guide the day-to-day activities of computing professionals in their role as professionals. By computing professional I mean anyone involved in the design and development of computer artifacts... The ethical decisions made during the development of these artifacts have a direct relationship to many of the issues discussed under the broader concept of computer ethics [Gotterbarn, 1991].

With this professional-ethics definition of computer ethics in mind, Gotterbarn has been involved in a number of related activities, such as co-authoring the third version of the ACM Code of Ethics and Professional Conduct and working to establish licensing standards for software engineers [Gotterbarn, 1992; Anderson, et al., 1993; Gotterbarn, et al., 1997].

3. Example Topics in Computer Ethics

No matter which re-definition of computer ethics one chooses, the best way to understand the nature of the field is through some representative examples of the issues and problems that have attracted research and scholarship. Consider, for example, the following topics:

- 3.1 Computers in the Workplace
- 3.2 Computer Crime
- 3.3 Privacy and Anonymity
- 3.4 Intellectual Property
- 3.5 Professional Responsibility
- 3.6 Globalization
- 3.7 The Metaethics of Computer Ethics

(See also the wide range of topics included in the recent anthology [Spinello and Tavani, 2001].)

3.1 Computers in the Workplace

As a "universal tool" that can, in principle, perform almost any task, computers obviously pose a threat to jobs. Although they occasionally need repair, computers don't require sleep, they don't get tired, they don't go home ill or take time off for rest and relaxation. At the same time, computers are often far more efficient than humans in performing many tasks. Therefore, economic incentives to replace humans with computerized devices are very high. Indeed, in the industrialized world many workers already have been replaced by computerized devices -- bank tellers, auto workers, telephone operators, typists, graphic artists, security guards, assembly-line workers, and on and on. In addition, even professionals like medical doctors, lawyers, teachers, accountants and psychologists are finding that computers can perform many of their traditional professional duties quite effectively.

The employment outlook, however, is not all bad. Consider, for example, the fact that the computer industry already has generated a wide variety of new jobs: hardware engineers, software engineers, systems analysts, webmasters, information technology teachers, computer sales clerks, and so on. Thus it appears that, in the short run, computer-generated unemployment will be an important social problem; but in the long run, information technology will create many more jobs than it eliminates.

Even when a job is not eliminated by computers, it can be radically altered. For example, airline pilots still sit at the controls of commercial airplanes; but during much of a flight the pilot simply watches as a computer flies the plane. Similarly, those who prepare food in restaurants or make products in factories may still have jobs; but often they simply push buttons and watch as computerized devices actually perform the needed tasks. In this way, it is possible for computers to cause "de-skilling" of workers, turning them into passive observers and button pushers. Again, however, the picture is not all bad because computers also have generated new jobs which require new sophisticated skills to perform -- for example, "computer assisted drafting" and "keyhole" surgery.

Another workplace issue concerns health and safety. As Forester and Morrison point out [Forester and Morrison, 140-72, Chapter 8], when information technology is introduced into a workplace, it is important to consider likely impacts upon health and job satisfaction of workers who will use it. It is possible, for example, that such workers will feel stressed trying to keep up with high-speed computerized devices -- or they may be injured by repeating the same physical movement over and over -- or their health may be threatened by radiation emanating from computer monitors. These are just a few of the social and ethical issues that arise when information technology is introduced into the workplace.

3.2 Computer Crime

In this era of computer "viruses" and international spying by "hackers" who are thousands of miles away, it is clear that computer security is a topic of concern in the field of Computer Ethics. The problem is not so much the physical security of the hardware (protecting it from theft, fire, flood, etc.), but rather "logical security", which Spafford, Heaphy and Ferbrache [Spafford, et al, 1989] divide into five aspects:

1. Privacy and confidentiality
2. Integrity -- assuring that data and programs are not modified without proper authority
3. Unimpaired service
4. Consistency -- ensuring that the data and behavior we see today will be the same tomorrow
5. Controlling access to resources

Malicious kinds of software, or "programmed threats", provide a significant challenge to computer security. These include "viruses", which cannot run on their own, but rather are inserted into other computer programs; "worms" which can move from machine to machine across networks, and may have parts of themselves running on different machines; "Trojan horses" which appear to be one sort of program, but actually are doing damage behind the scenes; "logic bombs" which check for particular conditions and then execute when those conditions arise; and "bacteria" or "rabbits" which multiply rapidly and fill up the computer's memory.

Computer crimes, such as embezzlement or planting of logic bombs, are normally committed by trusted personnel who have permission to use the computer system. Computer security, therefore, must also be concerned with the actions of trusted computer users.

Another major risk to computer security is the so-called "hacker" who breaks into someone's computer system without permission. Some hackers intentionally steal data or commit vandalism, while others merely "explore" the system to see how it works and what files it contains. These "explorers" often claim to be benevolent defenders of freedom and fighters against rip-offs by major corporations or spying by government agents. These self-appointed vigilantes of cyberspace say they do no harm, and claim to be helpful to society by exposing security risks. However every act of hacking is harmful, because any known successful penetration of a computer system requires the owner to thoroughly check for damaged or lost data and programs. Even if the hacker did indeed make no changes, the computer's owner must run through a costly and time-consuming investigation of the compromised system [Spafford, 1992].

3.3 Privacy and Anonymity

One of the earliest computer ethics topics to arouse public interest was privacy. For example, in the mid-1960s the American government already had created large databases of information about private citizens (census data, tax records, military service records, welfare records, and so on). In the US Congress, bills were introduced to assign a personal identification number to every citizen and then gather all the government's data about each citizen under the corresponding ID number. A public outcry about "big-brother government" caused Congress to scrap this plan and led the US President to appoint committees to recommend privacy legislation. In the early 1970s, major computer privacy laws were passed in the USA. Ever since then, computer-threatened privacy has remained as a topic of public concern. The ease and efficiency with which computers and computer networks can be used to gather, store, search, compare, retrieve and share personal information make computer technology especially threatening to anyone who wishes to keep various kinds of "sensitive" information (e.g., medical records) out of the public domain or out of the hands of those who are perceived as potential threats. During the past decade, commercialization and rapid growth of the internet; the rise of the world-wide-web; increasing "user-friendliness" and processing power of computers; and decreasing costs of computer technology have led to new privacy issues, such as data-mining, data matching, recording of "click trails" on the web, and so on [see Tavani, 1999].

The variety of privacy-related issues generated by computer technology has led philosophers and other thinkers to re-examine the concept of privacy itself. Since the mid-1960s, for example, a number of scholars have elaborated a theory of privacy defined as "control over personal information" (see, for example, [Westin, 1967], [Miller, 1971], [Fried, 1984] and [Elgesem, 1996]). On the other hand, philosophers Moor and Tavani have

argued that control of personal information is insufficient to establish or protect privacy, and "the concept of privacy itself is best defined in terms of restricted access, not control" [Tavani and Moor, 2001] (see also [Moor, 1997]). In addition, Nissenbaum has argued that there is even a sense of privacy in public spaces, or circumstances "other than the intimate." An adequate definition of privacy, therefore, must take account of "privacy in public" [Nissenbaum, 1998]. As computer technology rapidly advances -- creating ever new possibilities for compiling, storing, accessing and analyzing information -- philosophical debates about the meaning of "privacy" will likely continue (see also [Introna, 1997]).

Questions of anonymity on the internet are sometimes discussed in the same context with questions of privacy and the internet, because anonymity can provide many of the same benefits as privacy. For example, if someone is using the internet to obtain medical or psychological counseling, or to discuss sensitive topics (for example, AIDS, abortion, gay rights, venereal disease, political dissent), anonymity can afford protection similar to that of privacy. Similarly, both anonymity and privacy on the internet can be helpful in preserving human values such as security, mental health, self-fulfillment and peace of mind. Unfortunately, privacy and anonymity also can be exploited to facilitate unwanted and undesirable computer-aided activities in cyberspace, such as money laundering, drug trading, terrorism, or preying upon the vulnerable (see [Marx, 2001] and [Nissenbaum, 1999]).

3.4 Intellectual Property

One of the more controversial areas of computer ethics concerns the intellectual property rights connected with software ownership. Some people, like Richard Stallman who started the Free Software Foundation, believe that software ownership should not be allowed at all. He claims that all information should be free, and all programs should be available for copying, studying and modifying by anyone who wishes to do so [Stallman, 1993]. Others argue that software companies or programmers would not invest weeks and months of work and significant funds in the development of software if they could not get the investment back in the form of license fees or sales [Johnson, 1992]. Today's software industry is a multibillion dollar part of the economy; and software companies claim to lose billions of dollars per year through illegal copying ("software piracy"). Many people think that software should be ownable, but "casual copying" of personally owned programs for one's friends should also be permitted (see [Nissenbaum, 1995]). The software industry claims that millions of dollars in sales are lost because of such copying. Ownership is a complex matter, since there are several different aspects of software that can be owned and three different types of ownership: copyrights, trade secrets, and patents. One can own the following aspects of a program:

1. The "source code" which is written by the programmer(s) in a high-level computer language like Java or C++.
2. The "object code", which is a machine-language translation of the source code.
3. The "algorithm", which is the sequence of machine commands that the source code and object code represent.
4. The "look and feel" of a program, which is the way the program appears on the screen and interfaces with users.

A very controversial issue today is owning a patent on a computer algorithm. A patent provides an exclusive monopoly on the use of the patented item, so the owner of an algorithm can deny others use of the mathematical formulas that are part of the algorithm. Mathematicians and scientists are outraged, claiming that algorithm patents effectively remove parts of mathematics from the public domain, and thereby threaten to cripple science. In addition, running a preliminary "patent search" to make sure that your "new" program does not violate anyone's software patent is a costly and time-consuming process. As a result, only very large companies with big budgets can afford to run such a search. This effectively eliminates many small software companies, stifling competition and decreasing the variety of programs available to the society [The League for Programming Freedom, 1992].

3.5 Professional Responsibility

Computer professionals have specialized knowledge and often have positions with authority and respect in the community. For this reason, they are able to have a significant impact upon the world, including many of the things that people value. Along with such power to change the world comes the duty to exercise that power responsibly [Gotterbarn, 2001]. Computer professionals find themselves in a variety of professional relationships with other people [Johnson, 1994], including:

employer　　-- employee

client　　　-- professional

professional -- professional

society　　　-- professional

These relationships involve a diversity of interests, and sometimes these interests can come into conflict with each other. Responsible computer professionals, therefore, will be aware of possible conflicts of interest and try to avoid them.

Professional organizations in the USA, like the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronic Engineers (IEEE), have established codes of ethics, curriculum guidelines and accreditation requirements to help computer professionals understand and manage ethical responsibilities. For example, in 1991 a Joint Curriculum Task Force of the ACM and IEEE adopted a set of guidelines ("Curriculum 1991") for college programs in computer science. The guidelines say that a significant component of computer ethics (in the broad sense) should be included in undergraduate education in computer science [Turner, 1991].

In addition, both the ACM and IEEE have adopted Codes of Ethics for their members. The most recent ACM Code (1992), for example, includes "general moral imperatives", such as "avoid harm to others" and "be honest and trustworthy". And also included are "more specific professional responsibilities" like "acquire and maintain professional competence" and "know and respect existing laws pertaining to professional work." The IEEE Code of Ethics (1990) includes such principles as "avoid real or perceived conflicts of interest whenever possible" and "be honest and realistic in stating claims or estimates based on available data."

The Accreditation Board for Engineering Technologies (ABET) has long required an ethics component in the computer engineering curriculum. And in 1991, the Computer Sciences Accreditation Commission/Computer Sciences Accreditation Board (CSAC/CSAB) also adopted the requirement that a significant component of computer ethics be included in any computer sciences degree granting program that is nationally accredited [Conry, 1992].

It is clear that professional organizations in computer science recognize and insist upon standards of professional responsibility for their members.

3.6 Globalization

Computer ethics today is rapidly evolving into a broader and even more important field, which might reasonably be called "global information ethics". Global networks like the Internet and especially the world-wide-web are connecting people all over the earth. As Krystyna Gorniak-Kocikowska perceptively notes in her paper, "The Computer Revolution and the Problem of Global Ethics" [Gorniak-Kocikowska, 1996], for the first time in history, efforts to develop mutually agreed standards of conduct, and efforts to advance and defend human values, are being made in a truly global context. So, for the first time in the history of the earth, ethics and values will be debated and transformed in a context that is not limited to a particular geographic region, or constrained by a specific religion or culture. This may very well be one of the most important social developments in history. Consider just a few of the global issues:

Global Laws

If computer users in the United States, for example, wish to protect their freedom of speech on the internet, whose laws apply? Nearly two hundred countries are already interconnected by the internet, so the United States Constitution (with its First Amendment protection for freedom of speech) is just a "local law" on the internet -- it does not apply to the rest of the world. How can issues like freedom of speech, control of "pornography", protection of intellectual property, invasions of privacy, and many others to be governed by law when so many countries are involved? If a citizen in a European country, for example, has internet dealings with someone in a far-away land, and the government of that land considers those dealings to be illegal, can the European be tried by the courts in the far-away country?

Global Cyberbusiness

The world is very close to having technology that can provide electronic privacy and security on the internet sufficient to safely conduct international business transactions. Once this technology is in place, there will be a rapid expansion of global "cyberbusiness". Nations with a technological infrastructure already in place will enjoy rapid economic growth, while the rest of the world lags behind. What will be the political and economic fallout from rapid growth of global cyberbusiness? Will accepted business practices in one part of the world be perceived as "cheating" or "fraud" in other parts of the world? Will a few wealthy nations widen the already big gap between rich and poor? Will political and even military confrontations emerge?

Global Education

If inexpensive access to the global information net is provided to rich and poor alike -- to poverty-stricken people in ghettos, to poor nations in the "third world", etc.-- for the first time in history, nearly everyone on earth will have access to daily news from a free press; to texts, documents and art works from great libraries and museums of the world; to political, religious and social practices of peoples everywhere. What will be the impact of this sudden and profound "global education" upon political dictatorships, isolated communities, coherent cultures, religious practices, etc.? As great universities of the world begin to offer degrees and knowledge modules via the internet, will "lesser" universities be damaged or even forced out of business?

Information Rich and Information Poor

The gap between rich and poor nations, and even between rich and poor citizens in industrialized countries, is already disturbingly wide. As educational opportunities, business and employment opportunities, medical services and many other necessities of life move more and more into cyberspace, will gaps between the rich and the poor become even worse?

3.7 The Metaethics of Computer Ethics

Given the explosive growth of Computer ethics during the past two decades, the field appears to have a very robust and significant future. Two important thinkers, however, Krystyna Gorniak-Kocikowska and Deborah Johnson, have recently argued that computer ethics will disappear as a separate branch of ethics. In 1996 Gorniak-Kocikowska predicted that computer ethics, which is currently considered a branch of applied ethics, will eventually evolve into something much more.[1] According to her hypothesis, "local" ethical theories like Europe's Benthamite and Kantian systems and the ethical systems of other cultures in Asia, Africa, the Pacific Islands, etc., will eventually be superceded by a global ethics evolving from today's computer ethics. "Computer" ethics, then, will become the "ordinary" ethics of the information age.

In her 1999 ETHICOMP paper [Johnson, 1999], Johnson expressed a view which, upon first sight, may seem to be the same as Gorniak's.[2] A closer look at the Johnson hypothesis reveals that it is a different kind of claim than Gorniak's, though not inconsistent with it. Johnson's hypothesis addresses the question of whether or not the name "computer ethics" (or perhaps "information ethics") will continue to be used by ethicists and others to refer to ethical questions and problems generated by information technology. On Johnson's view, as information

technology becomes very commonplace -- as it gets integrated and absorbed into our everyday surroundings and is perceived simply as an aspect of ordinary life -- we may no longer notice its presence. At that point, we would no longer need a term like "computer ethics" to single out a subset of ethical issues arising from the use of information technology. Computer technology would be absorbed into the fabric of life, and computer ethics would thus be effectively absorbed into ordinary ethics.

Taken together, the Gorniak and Johnson hypotheses look to a future in which what we call "computer ethics" today is globally important and a vital aspect of everyday life, but the name "computer ethics" may no longer be used.

Bibliography

- Anderson, Ronald, Deborah Johnson, Donald Gotterbarn and Judith Perrolle (February 1993) "Using the New ACM Code of Ethics in Decision Making," Communications of the ACM, Vol. 36, 98-107.
- Brey, Philip (2001) "Disclosive Computer Ethics." In R. A. Spinello and H. T. Tavani, eds., Readings in CyberEthics, Jones and Bartlett.
- Bynum, Terrell Ward (1993) "Computer Ethics in the Computer Science Curriculum." In Bynum, Terrell Ward, Walter Maner and John L. Fodor, eds. (1993) Teaching Computer Ethics, Research Center on Computing & Society.
- Bynum, Terrell Ward (1999), "The Foundation of Computer Ethics", a keynote address at the AICEC99 Conference, Melbourne, Australia, July 1999. Published in the June 2000 issue of Computers and Society.
- Conry, Susan (1992) "Interview on Computer Science Accreditation." In Bynum, Terrell Ward and John L. Fodor, creators, Computer Ethics in the Computer Science Curriculum (a video program), Educational Media Resources.
- Elgesem, Dag (1996) "Privacy, Respect for Persons, and Risk." In Ess, Charles, ed., Philosophical Perspectives on Computer-Mediated Communication, State University of New York Press.
- Fodor, John L. and Terrell Ward Bynum, creators. (1992) What Is Computer Ethics? [a video program], Educational Media Resources.
- Forester, Tom and Perry Morrison (1990) Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing, MIT Press.
- Fried, Charles (1984) "Privacy." In Schoeman, F. D., ed., Philosophical Dimensions of Privacy, Cambridge University Press.
- Friedman, Batya, ed. (1997) Human Values and the Design of Computer Technology, Cambridge University Press.
- Friedman, Batya and Helen Nissenbaum (1996) "Bias in Computer Systems", ACM Transactions on Information Systems, Vol. 14, No. 3, 330-347.
- Gorniak-Kocikowska, Krystyna (1996) "The Computer Revolution and the Problem of Global Ethics." In Bynum and Rogerson (1996) Global Information Ethics, Opragen Publications, 177-90.
- Gotterbarn, Donald (1991) "Computer Ethics: Responsibility Regained," National Forum: The Phi Beta Kappa Journal, Vol. 71, 26-31.
- Gotterbarn, Donald (2001) "Informatics and Professional Responsibility", Science and Engineering Ethics, Vol. 7, No. 2.
- Gotterbarn, Donald, Keith Miller, and Simon Rogerson (1997) "Software Engineering Code of Ethics," Information Society, Vol. 40, No. 11, 110-118.
- Introna, Lucas D. (1997) "Privacy and the Computer: Why We Need Privacy in the Information Society," Metaphilosophy, Vol. 28, No. 3, 259-275.
- Introna, Lucas D. and Helen Nissenbaum (2000) "Shaping the Web: Why the Politics of Search Engines Matters", The Information Society, Vol. 16, No.3, 1-17.
- Johnson, Deborah G. (1985) Computer Ethics, Prentice-Hall, 2nd Edition, 1994.
- Johnson, Deborah G. (1992) "Proprietary Rights in Computer Software: Individual and Policy Issues." In Bynum, Terrell Ward, Walter Maner and John L. Fodor, eds. (1992) Software Ownership and Intellectual Property Rights, Research Center on Computing & Society.

- Johnson, Deborah G. (1999) "Computer Ethics in the 21st Century", a keynote address at the ETHICOMP99 Conference, Rome, Italy, October 1999. Published in Spinello, Richard A. and Herman T. Tavani, eds. (2001) Readings in CyberEthics, Jones and Bartlett.
- Kocikowski, Andrzej (1996) "Geography and Computer Ethics: An Eastern European Perspective." In Bynum, Terrell Ward and Simon Rogerson, eds. (1996) Global Information Ethics, Opragen Publications, 201-10. (The April 1996 issue of Science and Engineering Ethics)
- The League for Programming Freedom (1992) "Against Software Patents." In Bynum, Terrell Ward, Walter Maner and John L. Fodor, eds. (1992) Software Ownership and Intellectual Property Rights, Research Center on Computing & Society.
- Maner, Walter (1980) Starter Kit in Computer Ethics, Helvetia Press (published in cooperation with the National Information and Resource Center for Teaching Philosophy). [Originally self-published by Maner in 1978.]
- Maner, Walter (1996) "Unique Ethical Problems in Information Technology," In Bynum and Rogerson. (1996) 137-52.
- Marx, Gary T. (2001) "Identity and Anonymity: Some Conceptual Distinctions and Issues for Research". In J. Caplan and J. Torpey, Documenting Individual Identity. Princeton University Press.
- Miller, A. R. (1971) The Assault on Privacy: Computers, Data Banks, and Dossiers, University of Michigan Press.
- Moor, James H. (1985) "What Is Computer Ethics?" In Bynum, Terrell Ward, ed. (1985) Computers and Ethics, Blackwell, 266-75. [Published as the October 1985 issue of Metaphilosophy.]
- Moor, James H. (1997) "Towards a Theory of Privacy in the Information Age," Computers and Society, Vol. 27, No. 3, 27-32.
- Nissenbaum, Helen (1995) "Should I Copy My Neighbor's Software?" In D. Johnson and H. Nissenbaum, eds., Computers, Ethics, and Social Responsibility, Prentice Hall.
- Nissenbaum, Helen (1998) "Protecting Privacy in an Information Age: The Problem of Privacy in Public," Law and Philosophy, Vol. 17, 559-596.
- Nissenbaum, Helen (1999) "The Meaning of Anonymity in an Information Age," The Information Society, Vol. 15, 141-144.
- Parker, Donn (1968) "Rules of Ethics in Information Processing," Communications of the ACM, Vol. 11., 198-201.
- Parker, Donn (1979) Ethical Conflicts in Computer Science and Technology. AFIPS Press.
- Parker, Donn, S. Swope and B.N. Baker (1990) Ethical Conflicts in Information & Computer Science, Technology & Business, QED Information Sciences.
- Perrolle, Judith A. (1987) Computers and Social Change: Information, Property, and Power. Wadsworth.
- Rogerson, Simon (Spring 1996) "The Ethics of Computing: The First and Second Generations," The UK Business Ethics Network News.
- Rogerson, Simon and Terrell Ward Bynum (June 9, 1995) "Cyberspace: The Ethical Frontier," Times Higher Education Supplement, The London Times.
- Sojka, Jacek (1996) "Business Ethics and Computer Ethics: The View from Poland." In Bynum and Rogerson. (1996) Global Information Ethics, Opragen Publications, 191-200.
- Spafford, Eugene, et al. (1989) Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats, ADAPSO.
- Spafford, Eugene (1992) "Are Computer Hacker Break-Ins Ethical?" Journal of Systems and Software, January 1992, Vol. 17, 41-47.
- Spinello, Richard A. and Herman T. Tavani, eds. (2001) Readings in CyberEthics, Jones and Bartlett.
- Stallman, Richard (1992) "Why Software Should Be Free." In Bynum, Terrell Ward, Walter Maner and John L. Fodor, eds. (1992) Software Ownership and Intellectual Property Rights, Research Center on Computing & Society, 35-52.
- Tavani, Herman T. (1999) "Privacy On-Line," Computers and Society, Vol. 29, No. 4, 11-19.
- Tavani, Herman T. and James H. Moor (2001) "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies", Computers and Society, Vol. 31, No. 1, 6-11.
- Turkle, Sherry (1984) The Second Self: Computers and the Human Spirit, Simon & Schuster.
- Turner, A. Joseph (1991) "Summary of the ACM/IEEE-CS Joint Curriculum Task force Report: Computing Curricula, 1991," Communications of the ACM, Vol. 34, No. 6., 69-84.

- van Speybroeck, James (July 1994) "Review of Starter Kit on Teaching Computer Ethics" (Terrell Ward Bynum, Walter Maner and John L. Fodor, eds.) Computing Reviews, 357-8.
- Weizenbaum, Joseph (1976) Computer Power and Human Reason: From Judgment to Calculation, Freeman.
- Westin, Alan R.(1967) Privacy and Freedom, Atheneum.
- Wiener, Norbert (1948) Cybernetics: or Control and Communication in the Animal and the Machine, Technology Press.
- Wiener, Norbert (1950/1954) The Human Use of Human Beings: Cybernetics and Society, Houghton Mifflin, 1950. (Second Edition Revised, Doubleday Anchor, 1954.)

Other Internet Resources

- ACM SIGCAS, Special Interest Group on Computers and Society, Association for Computing Machinery
- Australian Institute of Computer Ethics
- Centre for Computing and Social Responsibility, (De Montfort University, UK)
- Computer Ethics Bibliography, by Herman Tavani (Rivier College)
- Electronic Frontier Foundation
- Electronic Privacy Information Center
- Research Center on Computing & Society, (Southern Connecticut State University)

Related Entries

privacy | property

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Stanford Encyclopedia of Philosophy