This is a preprint version of the following article:
Brey, P. (2007). 'Computer Ethics in (Higher) Education,' in Ed. G. Dodig-Crnkovic and S. Stuart, Eds., *Computation, Information, Cognition: The Nexus and the Liminal*. Cambridge Scholars Press.

Computer Ethics in (Higher) Education

1. Introduction

Computer ethics is a major new field of study that addresses ethical issues in the use, development and management of information technology, as well as in the formulation of general societal policies regarding the regulation of information technology in society (Johnson, 2000; Tavani, 2003; Spinello, 2000; Baird et al., 2000; Forester and Morrison, 1994; Baase, 1997). Increasingly, computer ethics is a subject that is taught in universities, high schools, and other educational settings. This paper addresses the role of computer ethics in the education system, focusing specifically on university education and university policy. It will also, more briefly, address its role in high school education and high school policies. As my main thesis, I will be arguing that universities have a vital role in generating awareness of ethical issues in the use, development and management of information technology. As I will be arguing, universities should be addressing these ethical issues in two ways:

1) in *computer ethics policies*: given the importance of information technology in the practices of today's universities, and given the possibilities of unethical use of this technology by students and staff, universities should ensure that they have policies regarding the use and management of information technology by students and staff.

2) in *computer ethics education*: given the importance of information technology in virtually every contemporary profession, universities should ensure that their curricula pay attention to ethical issues in the use, management or development of information technology. Such education should be part of more general education on the societal aspects of information technology.

Sections 2 and 3 cover the first of these two points: computer ethics policies in the university. In section 2, I will discuss a variety of ethical issues regarding the use and management of information technology by students and staff. In section 3, I will focus on one specific issue: academic freedom and free speech, and the importance of good policies on this issue in the use and management of information technology on campus.[1]

[1] These two sections are based on a study that discusses ethical aspects of the use and management of information technology in higher education, called *Ethical Issues for the Virtual University* (Brey, 2003). The report was written for the cEVU project coordinated by EuroPACE and supported by the European Committee, for a publication for the European Committee. An online version is due to appear on http://www.cevu.org.

Sections 4 through 7 consider the second point, that of computer ethics education, which will be related to the broader issue of education on societal aspects of information technology. In section 4, I will outline a field of study which I call social and humanistic studies of computing (SHC) and contrast this with applied studies of societal aspects of computing (ASC). In section 5, I will argue for the importance of both SHC and ASC in university curricula and relate their roles to academic and professional functions of university education. In section 6, I will describe how courses in SHC and ASC may be taught in practice, illustrating this with a description of the minor ICT and Society which I have helped to develop at my university, and with a description of a course in Computers and Society. In section 7, I will assess the relation of computer ethics to SHC and ASC, and its role in the university curriculum. I will outline educational goals for computer ethics education and provide a brief description of a course in computer ethics that meets these goals.[2]

In the concluding section 8, finally, I will briefly summarize my points and consider how my analysis of computer ethics in university education and policy would translate to a different area: that of secondary or high school education.

2. Information technology and ethical student and staff behavior

In this section, I will address the question of how the use of computers in education changes the settings in which moral values function, for students and staff members. My focus will be on the new moral challenges and new possibilities for immoral behavior for students and staff that may arise with the use of information technology in higher education. These moral challenges arise in part because electronic environments afford new types of actions that may require new moral codes, such as copying software and hacking. Yet, they also arise in part because certain types of immoral actions, such as plagiarism and invasions of privacy, are easier to perform in electronic settings, as well as harder to detect or control. What follows are six types of morally questionable behavior that depend on the use of computers and computer networks in (higher) education.

- *Digital plagiarism*
  Plagiarism has always existed in education, including higher education, where it is one of the major forms of academic dishonesty. Assignments handed in by students may turn out to be copied from fellow students or to be taken over, in part or in whole, from existing published works. In a way, computers and the Internet only add to the means that students have at their disposal to commit plagiarism. However, they make it much easier to do and much harder to detect. As Austin and Brown have argued, plagiarism has become easier for students in two ways: "word processing programs allow students to easily "cut and paste" information from the Internet or other electronic media to develop a paper that appears to be original work" and "students' use of Internet information that may be unavailable in traditional sources makes documenting academic dishonesty more difficult to faculty." (1999, p. 21; see

[2] These four sections, and the corresponding part in the conclusion, are based on the paper "The role of social and ethical studies of IT in the university curriculum" presented at *FINE* (Foundations of Information Ethics), Hiroshima, Japan, February 27-28, 2001.

also Hinman, 2002). Particularly worrisome, as they point out, is the existence of "term paper mills," which offer pre-written term papers to students on a range of topics, and many of which also offer to write papers specifically for students for a fee.

- *Breaking copyright and software theft*
  It is well known that the illegal copying of copyrighted media (texts, music works, movies and software programs) is widespread throughout society. Moreover, many people who engage in such activity do not consider themselves to be doing something that is patently immoral. This is certainly true for college students. Cohen and Cornwell (1989) and Glass and Wood (1996), for example, found that a large majority of college students do not perceive the illegal copying of software as unethical.

  This attitude of college students seems to match developments in the current information age, in which the Internet increasingly functions as the most important information medium that people use. Hinman (2002) has argued that the very structure of the Internet undermines the notion of private intellectual property on the web: "The inner dynamic of the Web moves us increasingly toward a much more communal notion of property". As he explains, the Web stimulates copying because the very nature of browser technology necessitates making copies, because perfect copies can be made at virtually no cost, and because making digital copies does not involve physical theft from the person who owns the original (34). It may be added to this that many information sources on the Web are not obviously copyrighted, and many even lack an identifiable author (Kolko, 2002). Lipinski and Britz (1999) argue, moreover, that digital copying can often be morally, if not legally, defended because of the fact that access to information is a critical need in an age of information that may in some cases override proprietary rights.

  Hence, the traditional legal paradigm of intellectual property is increasingly challenged by a new paradigm that emphasizes unrestrained access to, and use of, information. It is difficult to find an adequate moral compass to navigate the new landscape, not only for students, but for staff as well. Moral and legal confusion may moreover also result from the vagueness of "fair use" provisions in copyright law, that do not clearly state when copying for personal use or display in classroom settings is permitted, and from the existence of corporate licenses at universities, or departments therein, that may permit students to freely use or copy media that they do not own themselves.

- *Hacking*
  Hacking is breaking into computer systems for unauthorized purposes, which may be either malicious or nonmalicious. Hacking may involve, for example, snooping around on someone's personal computer through remote access, intentionally modifying or destroying files to which one has not been granted access, releasing computer viruses, stealing passwords or files, exposing personal information, and stealing electronic money (see Forester and Morrison, 1994, ch. 5 and Baase, 1997, ch. 7). Students and staff members at both virtual and conventional universities may engage in hacking for a variety of reasons. They may simply be unaware that they are breaking into a computer system, they may just be curious, they may be out to

harm someone, they may want to benefit themselves, or they may have entirely different reasons. Malicious hacking is clearly morally problematic, but nonmalicious hacking has been defended by hackers as morally acceptable and socially harmless or even beneficial (cf. Baase, p. 242). Clearly, universities need clear policies and guidelines on hacking (including policies that define what kinds of computer systems access are unauthorized for whom) and probably need to distinguish malicious from nonmalicious hacking.

- *Improper use of computer resources*
  Hacking is the use of computer resources to which one is not supposed to have access. However, students and staff may also have authorized access to computer resources, but then go on to use these resources improperly. They may have a university Internet account, or they may use a computer system or computer network or computer software that is owned by the university, or they may use computerized services offered by the university, and do so in a way that does not meet the university's standards for proper use of that particular resource. For example, students may use their student account to run their own Internet business, contrary to the university's policies. Or students may open up a popular website or service that generates loads of traffic that incapacitates the university's server, e.g., peer to peer downloads of MP3 files. Or staff members may use the university's server or computer systems to download or view or store content that is either illegal or against the university's policies (e.g., racist or fascist materials or pornography). Or members of the academic community may spread computer viruses or worms. Clearly, universities need policies regarding the proper use of computer resources in an academic context by students and staff.

- *(Anonymous) harassment and hate speech*
  In universities, there may be various electronic means of communicating messages to other members of the academic community, as well as to persons outside the university: e-mail, electronic bulletin boards, IRC (the exchange of short one-on-one messages without a significant time lag), collaborative virtual environments and web pages constitute some of the most important ones. As in face-to-face communication, these computer-mediated forms of communication can be used to send threatening, obscene, inflammatory or harassing messages. These may include discriminatory messages, used to disparage individuals or groups based on gender, race, sexual orientation, religion, age, or disability. Such messages are generally not considered to be acceptable in an academic setting, as educators strive to ensure that the classroom, if not the campus at large, functions as a safe, nonthreatening environment for students as well as for staff. In this, the same principles apply for virtual classrooms and campuses as for their physical counterparts (cf. Ferganchick-Neufang, 1998).

  Moreover, in curbing harassing and obscene messages, educators will simultaneously have to make sure that they are not unduly limiting free speech (see also the section 3). As Baase has pointed out (p. 212), speech on computer systems is often treated differently from other forms of speech, and there is a tendency for less tolerance for offensive talk that takes place online. If this is true, then extra care must be taken to ensure that student discussion in the virtual classroom can take place as

freely as student discussion in the physical classroom. It would be a loss if students would be more hesitant to voice their opinions because they are using an electronic medium.

A feature of computer-mediated communication that deserves special mention is the ease by which anonymous or pseudonymous messages can be sent, for example through anonymous remailer services. Baase (1997, 214-5) points out that anonymous messages posted over the Internet can have good and bad uses. She claims that anonymity provides protection for victims of violence and abuse and users of illegal drugs who seek counseling and advice and for whistleblowers who wish to report on unethical or illegal activity in their organization without fear of retribution. However, anonymity can also be used for criminal and antisocial purposes: to perpetuate fraud, to harass people, to threaten or libel people with impunity, and ruin their reputation by spreading rumors (Baase, p. 214-5; see also Kling et al., 2000). Universities may hence want to consider having policies for anonymous electronic communication.

- *Breaches of informational privacy and confidentiality*

Privacy is generally considered to be an individual right in Western countries, and many nations have privacy laws (or data protection laws, as they are sometimes called in Europe). It is nowadays generally recognized that new technologies, and particularly information and communication technologies, raise new privacy issues, for example concerning electronic databases and online privacy (e.g., Cate, 1997; Agre and Rotenberg, 1998). Many of these new privacy issues can be expected to apply to the use of universities that make a lot of use of online instruction and communication. In such universities, many important activities of members of the university can in principle be monitored or recorded electronically. This includes not only student administration but also classroom discussion, student-to-student and student-to-faculty e-mail contact, and the online behavior of students in general. The walls of classrooms and offices at such a university are much more permeable than those of classical universities, making eavesdropping much easier, and it happens much more frequently that the things that are said and done in them are recorded so as to be available for later scrutiny, or can be copied for distribution.

At many (conventional) universities, privacy policies remain limited to student privacy policies that protect student records from being accessed by third parties without authorization. Since many student records are nowadays stored in electronic format, these policies must be supplemented with good system security. Electronic records should be adequately protected so as to avoid unauthorized access to them. Many universities nowadays also have policies that address the electronic posting of grades, which are considered to be privacy-sensitive.

Many more privacy issues can be raised at a university that has much of its communication and instruction online, however. Consider, first, the confidentiality of classroom or group discussion or one-to-one and one-to-many. Can students be sure that these discussions are not logged or monitored by administrators, that they are not made accessible on public networks, and that access to them cannot be easily hacked? In a study of privacy in online learning environments, Tu (2002) argues that class discussions over a connection that is not secure may either inhibit discussion or force

students to take risks in disclosing more personal information. He argues in favor of more private interaction environments, which he claims to be "key to increasing interactivity" (315). As he claims: "A sound learning environment will allow learners to adjust to the ideal levels of privacy and give students more secure and more comfortable environments to increase their social presence to enhance social interaction" (315).

Other relevant online privacy issues that may occur include:[3]

1. *Personal information on public computers*. When students or staff use publicly accessible computers, they may unknowingly leave personal information behind, such as cached web pages (accessed web pages that are left in temporary storage on the disk drive and may remain there even after a browser is closed) and cookies (small files that are put on a hard disk by a web site to identify users and their preferences), that are then available for inspection by others.
2. *File sharing*. Student or faculty computers may contain software that makes files on them accessible to other users on the campus network and outside without knowledge of the owner, or may allow files to be stored on a central server that are then accessible to others without their permission. This could allow strangers to read these files that may contain personal information.
3. *Publicly accessible databases*. Many universities have databases that have public access, for example databases that contain directories for students and staff. These databases may contain privacy-sensitive information for which students and staff have given no permission.
4. *University web pages and bulletin boards*. Web pages maintained by the university, by faculty or by students may contain personal information that invades the privacy of others. Likewise, postings and repostings (forwarded messages) on bulletin boards or in other electronic forums may contain personal information of third parties for which no authorization has been given.
5. *Search engines*. Search engines can be used to collect personal information about students or staff. Specifically, a university's own search engine may be used to collect personal information that is found on the university's intranet or campus network. If such a search engine has access to many sites, it may give a detailed profile of people. It may tell about a student, for example, what courses (s)he is enrolled in, what student groups (s)he is a member of, and what campus events (s)he has participated in.
6. *Third party market research*. Students constitute an interesting population for some marketers and market researchers, and they may try to enlist educators to help them acquire information on students, or solicit directly to students. The data collected by these parties is likely to be privacy-sensitive.

[3] See, amongst others, the Stanford Privacy Project at http://www.stanford.edu/group/privacyproject/ and Spinello, 2000, ch. 5.

> Clearly, then, universities will need privacy policies to protect the privacy rights of students and staff and to create secure learning environments in which members of the community interact with each other on a basis of trust.

Based on the previous discussion, I suggest that universities should consider developing policies regarding the use of information technology that include some or all of the following:

- Policies concerning digital plagiarism and academic dishonesty in online assessment.[4]
- Policies concerning copyright and software theft.[5]
- Policies concerning hacking. These should be supplemented by clear access guidelines to different systems and should probably distinguish malicious from nonmalicious hacking.
- Policies concerning the proper use of computer resources of the university.
- Policies concerning online anonymity and pseudo anonymity, online harassment and hate speech, which should at the same time, not impose unacceptable limits on free speech.
- Privacy policies for personal information stored in databases and for online privacy.

3. Academic freedom and information technology

Intellectual freedom is the freedom to use one's intellect in a way of one's own choosing, and to both hold, receive and disseminate ideas without restraint. The American Library Association defines it as "the right of every individual to both seek and receive information from all points of view without restriction" and holds that intellectual freedom "provides for free access to all expressions of ideas through which any and all sides of a question, cause or movement may be explored."[6] Intellectual freedom has often been defended as a core Western value, as a necessary prerequisite for democracy and cultural progress (cf. Morse, 2001).

Academic freedom is intellectual freedom as it exists within the academy: it is the free pursuit of knowledge by scholars and students. Clark, in an important study of the higher education system, claims that academic freedom involves freedom of research, freedom of teaching, and freedom of learning (1983, p. 248). As he points out, the liberties of academic freedom are sought at various levels: students seek freedom to learn what they want, scholars seek freedoms in teaching and research within their department, departmental groups seek self-determination within the university, and the university

---

[4] See Olt (2002) for a discussion of strategies for minimizing academic dishonesty in online assessment.

[5] See, e.g., the 1999 statement on copyright of the American Association of University Professors at http://www.aaup.org/statements/Redbook/Spccopyr.htm

[6] Intellectual Freedom and Censorship Q and A of the American Library Association at http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/Intellectual_Freedom3/Basics/Intellectual_Freedom_and_Censorship_QandA.htm

seeks autonomy from the state and from outside groups (p. 248). Basic to this push for liberties is, according to Clark, "the desire for individual self-expression". Teachers want to teach to be able to say what they please without restraint or fear of retribution. Those who learn want to learn in a way that helps realize their life plan: they want be able to choose what they learn, how they learn it, and at what pace they learn it.

In discussing academic freedom and information technology, some authors have argued that information technology enhances academic freedom for students by offering them more choice, for instance by making a university education available through e-learning for students (e.g. employed persons or disabled persons) who are unable to physically attend classes. More generally, also, authors have been emphasizing the greater informational freedom that results from the Internet as an education medium, as it enhances opportunities for academic communication, information retrieval and teaching.

However, many authors also identify challenges to academic freedom that may arise from the use of computers and the Internet in education. A major challenge that has been discussed is the challenge of content selection with resulting limitations on free speech. Academic freedom means, amongst others, free access to information and freedom of speech for both students and faculty. When speech or information is carried by a digital medium, however, limitations may be imposed quite easily: an administrator, system operator or list moderator may block certain types of messages, delete certain web pages or block certain e-mail addresses in a matter of seconds. Thus, both students and faculty are in a dependent position concerning their ability to acquire information and voice opinions via computer networks.

Regarding free access to information, universities sometimes place filters on their Internet traffic that effectively block access to certain web sites or to bulletin boards or messages that contain certain types of content (Rosenberg, 2001). Filtering or blocking may be done for efficiency reasons, for instance because it is found that certain sites, such as adult sites, generate a large amount of web traffic that causes net congestion. However, it may also be done as a form of censorship, to prevent users from having access to certain types of information that are considered immoral or illegal or otherwise undesirable. For instance, access may be blocked to sites with adult content, with racist or fascist content, or with illegal software available for download. Though such efforts are understandable, it may be questioned if such content control can be reconciled with the demands of academic freedom. Moreover, the use of filtering software has a reported disadvantage, which is that it invariably filters too much. Filters usually block access to messages based on the occurrence in them of certain key words. This ignores context, however, and so often leads to 'suitable' content being blocked. For instance, sites or messages may be blocked that study pornography rather than containing it, or challenge racism instead of promoting it.

Regarding free speech, universities may try to exercise control over the types of speech that are exercised by students and staff over the university network. They may, for example, have policies against certain types of speech that are considered undesirable, may remove or block messages that do not adhere to such policies. For example, the University of California, San Diego imposed a speech code in 1995 that stated: "The use of University resources such as electronic mail to disparage individuals or groups on the basis of gender, race, sex, sexual orientation, age, disability, or religion, is strictly prohibited and violates University policy." (quoted in Baase, 1997, p. 212). Universities

may also monitor speech by eavesdropping on on-line communications and accessing student and faculty files on university servers.

While many forms of content control at universities probably result from efforts to protect individuals and groups from harassment and libel and foster a secure academic environment, there is nevertheless a serious risk that academic freedom and free speech are limited in the process. The ability to voice unpleasant and dissenting opinions has always been central to academic freedom and to freedom of speech, and a necessary prerequisite for social and intellectual criticism. When student and faculty fear that their electronically communicated views and opinions may be reprimanded or blocked, or worry that their communication may be (anonymously) monitored by parties who are in a position of power relative to them, free speech may be stifled and academic freedom may be hurt as a result. A serious and continuous effort is needed, therefore, to balance any the need to protect individuals and groups from harassment against the need to promote free speech and academic freedom.

In conclusion, the following policy recommendations may be made to universities regarding the use of information technology in a way that respects academic freedom and free speech:

- Universities, whether conventional or electronic/virtual, should be committed to protecting academic freedom, which includes freedom of research, freedom of learning and freedom of teaching, as well as overall freedom of speech. Their policies and procedures should reflect this commitment.

- Universities should be very cautious about filtering, blocking or removing electronic information or messages, monitoring computer systems and electronic communications of students and staff, and proposing speech codes for electronic communications. If any such actions are to be taken at all, they should respect as well as possible academic and intellectual freedom as well as personal privacy.

4. Computer ethics and social and humanistic studies of computing

I will now turn to the issue of computer ethics education in the university. Computer ethics as a field of study is (arguably) part of a wider field of study which may be called *social and humanistic studies of computing* (SHC). SHC are studies by scholars in the humanities and social sciences of computers and their roles in society. I define SHC as theoretical or nonapplied studies of the way in which various forms of information technology shape, and are themselves shaped by, aspects of their *social context*. By the social context of computer systems, I mean any aspect of individuals, collectives or social systems that constitutes part of the environment within which one or more computer systems are used. Hence, a study of the psychological effects of regular Internet use is a study in SHC. So is a study of the influence of computer networks on the structure of large organizations, a study of cultural practices of users of mobile computing devices, a study of cultural images of computers throughout history, of or a study of the role of information technology in globalization. Studies in SHC hence consider any sort of way in which information and communication technologies (ICTs) relate to their larger

context of use. Studies in SHC are *theoretical*, as opposed to *applied*. Their primary aim is not to change practices or develop policies. It is only to understand.

Over the past twenty or so years, the amount of research within the scope of SHC, as defined here, has increased dramatically. Still, SHC is not often seen as a coherent field of study. There has been some effort by social scientists, however, to turn *social* studies of computing into a field, for example by the late Rob Kling, former editor of the journal *The Information Society*, who has been promoting the label '*social informatics*' to designate social studies of computing. But on most counts, the coherence within the field of SHC is limited. Nevertheless, there are nowadays specialized journals that help give it coherence, such as *The Information Society*, *Computers and Society, New Media and Society, Information Technology & People* and *Information, Communication and Society,* as well as specialized societies and conference series.

Next to the emergence of SHC, there has been an emergence of various kinds of *applied* research on societal aspects of computing. Here, there is even less coherence between the various approaches that exist. Therefore, when I speak of *applied studies of societal aspects of computing* (ASC), I do not refer to a field but just an existing set of studies and approaches that are often unrelated to each other. Research in ASC has in common that it is not primarily concerned with a theoretical understanding of the social context of computer systems, although such theoretical knowledge usually plays a useful role in applied research. Instead, research in ASC is concerned with developing effective tools for professionals in various fields for coping with various societal aspects of computer systems. Such studies include applied studies on computer law, computer-assisted education, management and computing, and e-commerce, amongst others. SHC and ASC are hence complementary in the way they approach societal or nontechnical aspects of ICTs: the first is concerned with gaining at theoretical understanding, the second with developing practical know-how.

5. SHC and ASC in the university curriculum

Let me now turn to the question of the role that both SHC and ASC should have in the university curriculum. I take university education to have both an *academic* and a *professional* function. In some study programs, the academic function is emphasized. These are programs that lead to an academic degree. They are aimed at equipping students with theoretical knowledge within a field and with research skills for developing more theoretical knowledge in that field. Other university study programs lead to a professional degree. In such programs, the educational emphasis is on professional knowledge and skills, and the research skills that are taught relate to research aimed at developing *applied* forms of knowledge, or on *applying* knowledge in specific contexts.

Now, it is certainly not the case that the academic and professional functions of university education are mutually exclusive. Academic study programs always also have a professional role, in that they train students to become members of a certain profession. This is the profession of an academic scientist, equipped with research skills for furthering a specialized field. Conversely, professional degree programs at the university level tend to have an academic component, in that they emphasize academic, theoretical knowledge and skills. Theoretical knowledge acquired in a professional university

program is considered important as a theoretical background for more applied tasks. For instance, a mechanical engineer should have a basic training in Newtonian mechanics because this theoretical knowledge is relevant to the applied knowledge and skills that are the primary focus of a mechanical engineering program.

Theoretical knowledge is not just important as a preliminary to mastering applied knowledge and skills, however. It is frequently also considered important for the more general academic outlook that is the landmark of university education. This general academic outlook is realized through courses in *general education*, some of which emphasize *cultural literacy and societal knowledge*, others of which emphasize *general cognitive and professional skills*. Someone with a university degree, whether academic or professional, is not just expected to excel in his or her field, but also to adhere to certain minimum standards of cultural literacy, and to have good general cognitive skills. That is, he or she is supposed to have an *above average understanding of society, culture and history*, and to have *above average cognitive skills in analysis and synthesis*.

To summarize, some university programs focus on academic education, emphasizing theoretical knowledge and research skills, whereas others emphasize nonacademic professional knowledge and skills. Yet, every university program promotes a general academic outlook by offering courses in general education that are outside one's specialty. Given this characterization of university education, there are at least two reasons why is advisable to make education in SHC and ASC a *required* part of today's university curriculum.

First of all, there are good reasons to suppose that the general education component in a university program should pay attention to issues in SHC. This is because, I claim, such a program would give a shallow and outdated picture of society if it left out an analysis of the great changes that information technology is effecting in virtually every sector of society. The economy, government, education, health care, religion, scientific research, the media, entertainment, the arts, organizations, the workplace, interpersonal relations, and many other core institutions of society are being transformed through information and communication technologies. If one were living at the time that the industrial revolution would take place, one would not want a general education program to focus on preindustrial society. Instead, one would want it to pay attention to industrialization processes and the changes these are affecting. Likewise, one would expect a contemporary general education program to pay attention to the current information revolution, including the roles and effects of information technologies.

Education in SHC may not just be desirable within an education program because it is an important part of a general education component. It may also provide part of the background or context within which a good professional is able to situate his or her work. This role of SHC education can perhaps be illustrated best by looking at computer science curricula. Computer science curricula focus on knowledge and skills by which computer professional may design, operate or manage certain types of technologically complex systems. Much of the knowledge this requires is technological: it pertains to the rules according which these systems operate. However, computer systems also have to make a good fit with their social context. Users have to be able to use them well, organizations have to benefit from them, and sometimes society as a whole is supposed to benefit as well. A good fit between a computer system and its social context is not the mere result of it executing certain input-output functions without error. The technology

also has to work in harmony with its social context. Therefore, a broader understanding of how computer systems impact and fit in with various aspects of their social context is, if not necessary, then at least highly advisable if one is to be a good computer scientist. And this means that education in SHC is defensible as a required component in computer science curricula.

Second, within the professional component of a university program, there is a clear need for specialized courses dealing with the role of information technology within someone's specific profession. That is, there is a special need for courses in ASC. Nowadays, there are few professions left in which information technology does not play an important role. Obviously, nearly every professional will be using information technologies as an *end-user*. But this not the role of information technology in their profession I am referring to. It is not clear that special courses in ASC are required to be a better end-user of information technology. Instead, what are required are just courses that teach one how to use the technology, and these are not courses in ASC because they do not normally focus on contextual aspects of information technology.

However, next to end-users, many professionals are also *decision-makers* regarding information technology. That is, in the course of their professional duties, they may be deciding that certain computer systems will be used, purchased or implemented, they may be deciding by whom they will be used and what they will be used for, and they may shape or influence various policies regarding the development, acquisition and use of information technologies. Because, increasingly, professionals have to make such *IT-related choices*, and because of the great impact such choices may have because of the revolutionary transformative power of information technology, it is increasingly important to include relevant education components on ASC in professional curricula. For example, in a policy program, it would nowadays be advisable to have a course on policy and information technology, because of the likelihood that professionals in this field will be making policy choices in which information technologies play key roles. Likewise, in an education studies program, it would be advisable to have education on computers in education, because of the profound impact that computers are having on education.

I conclude that because of the general education requirement in university curricula, and in some cases also because of the professional function of curricula (as in the case of computer science), education in SHC is highly advisable. Specifically, it would in my opinion be advisable to have a required course on "*Computers and Society*" across the university curriculum. Moreover, an equally good case can be made that professional programs should contain at least one relevant course in ASC. This course should focus on the role of information technology within that specific professional field and should convey professional knowledge and skills that enable intelligent professional choices regarding the role of information technology within that field.

For some programs, one course in SHC and one course in ASC may not be enough. It certainly would not be enough for programs that train one to be a computer professional. Specifically, I would propose that a computer science program would devote at least 10% of its professional component on SHC and ASC. This means that not more than 90% of the professional component should be devoted to the technical aspects of computer systems, and at least 10% should consider the fit between computer systems and their social context.

6. Teaching SHC and ASC

In this section, I will take SHC teaching at my own university, The University of Twente in the Netherlands, as an example. The University of Twente, grants academic degrees in engineering and applied social science. There are bachelor and master programs in various engineering fields, such as electrical engineering, computer science, and design engineering, and bachelor and master programs in various applied social science fields, such as education, policy and business administration. Students follow a three-year bachelor program which includes a half-year minor program in a field different from their area of specialization, after which they follow a one-year or two-year master program. Students are free to choose a minor program to their liking and they also have some amount of choice regarding the master programs they may follow immediately after completing a specific bachelor program.

At my university, I have taken the initiative to start a new interdisciplinary *minor program* called *ICT and Society*. This minor is the equivalent of half-a-year of university education, or 820 study hours, and is stretched over the course of an entire academic year. In the academic year in which they take the minor, students hence have 50% time to work on the minor and 50% time to take courses in their own field. The minor ICT and Society is not currently a required minor for any degree program at my university, but it is a recommended minor for several programs.

The aim of the minor ICT and Society is twofold. The primary aim is to acquaint students with basic issues in SHC. A secondary aim is to teach general professional skills for decision-making in relation to computer systems. This is a general ASC component of the major. Students have a degree of freedom to tailor the ASC component to their own professional area. In this way, the minor ICT and Society equips students with the basic understanding and skills to provide them with general education in this vital area and to deal with the social context of computing in their prospective careers.

To further these two aims, the ICT and Society minor is set up to have the following structure. In the first trimester of the academic year, students take three introductory courses. The first is a basic course on the technical aspects of computer systems. This course aims to familiarize students with basic properties of computer systems and the ways they are used in society. Computer science students participating in the minor do not have to take this course, and have the option of taking another course relevant to their professional interests, such as a course in computer law (which is not a required course in their own professional curriculum). The second course, taught by me, is a basic course on computers and society. It treats social aspects of computing as one would expect in a course dealing with basic SHC issues. The third course is a course on the role of computer systems in organizations (both governmental and commercial). This topic was considered by us to be an important SHC topic for the students at our university, because most will be assuming important roles in commercial or governmental organizations. This is why we decided to devote a special course to it.

In the second trimester, students take applied courses that can be characterized as courses in ASC. One course provides students with tools to do technology assessment of information technologies. This course aims to enable students to do general assessments

of the societal or organizational impacts of new computer systems. A second course focuses on two specific topics: e-commerce and e-government. It studies models and theories within these two areas and teaches about applications and application methodologies in both areas. A third course focuses on virtual communities, and looks at methods for investigating such communities, as well as at assessing the conditions under which such communities function well. In the third trimester, finally, students take up a small research project within one or more of the aforementioned areas. They may do so individually or (preferably) in small groups in which people from different disciplines work together.

For many students, however, a half-year program on ICT and Society may be too much of a good thing. I would not advise it to become a required minor for any program, with a possible exception of the computer science curriculum. In the previous section, though, I argued for a *required* course *Computers and Society* across the university curriculum. I will now consider what such a course may look like. The aim of a course in computers and society would be to acquaint students with basic issues in SHC, that is, it would teach about the role of information technology in various sectors of society and regarding various aspects their social context. A course on Computers and Society would leave students with a basic understanding of how ICT is transforming social institutions and practices. I now present a possible list of topics for a course in Computers and Society. Most courses would make a selection from this list:

1. *ICT in contemporary society*. A qualitative and quantitative assessment of the role of ICT in current society. A quick survey of the role of ICT and in various sectors of society (e.g., regarding work, the business world, medicine, education, government, the media, and everyday life), and related issues and problems. Key statistics on the users and uses of ICT.
2. *The Information Revolution and the Information Society*. A broad macro-perspective on the way in which ICT has changed the economy and social institutions in recent history. With a brief introduction to some theoretical perspectives, e.g., Beniger's theory of the Control Revolution (Beniger, 1986) or Castells' trilogy on the information age (e.g., Castells, 2000).
3. *Social history of ICT and its role in society*. A historical survey of the birth and spread of the digital computer, and social and cultural changes resulting from it. Attention is paid to changing functions of the computer in the workplace, in the economy, and in organizations, to past social struggle, and to images of and discourses on ICT.
4. *ICT and the economy*. An assessment of the role of ICT in the economy and of the difference between Fordist and postfordist economies. A consideration of the role of producers and consumers in this process.
5. *ICT and politics*. An assessment of the way in which ICT is transforming politics, both regarding the relation of citizens to the state, the relation of corporations to the state and its citizens, and the hierarchical structure of organizations. A treatment of specific political issues like privacy, freedom, democracy, and social justice.
6. *ICT and law*. An assessment of the way in which ICT is transforming law. Problems and issues like informational freedom, privacy, and intellectual property.

7. *ICT and social structure*. An assessment of the way in which social structures, roles, relationships and behaviors are changing because of ICT. Topics may include the 'digital divide' between 'information-haves and have-nots,' changing roles of various social groups (e.g., women, the elderly), the changing structure of social relationships, and changes in communication.
8. *ICT and culture*. An assessment of the way in which cultural beliefs, practices and experiences are changing because of ICT. This may include an assessment of the changing role of media, of the changing role of communication and information, changes in lifestyles, and the emergence of new cultural forms.
9. *ICT and human psychology*. An assessment of psychological changes correlated with the use of ICT. Mental processing of information with new media; changes in personality and social psychology; changes in conceptions of reality, time and space.
10. *ICT and the future*. Current expectations and scenarios for future technologies and trends in the information society.

There are nowadays various good textbooks that could be used in such a course. A very good textbook is Richard S. Rosenberg, *The Social Impact of Computers*. Also excellent is *The Network Society*, written by my University of Twente colleague Jan van Dijk. Other books are the reader *Computers in Society* edite by Kathryn Schellenberg, Rob Kling's *Computerization and Controversy: Value Conflicts and Social Choices*, and Paul Winter's *Computers and Society*.

I currently teach two rather broad courses on computers and society. The course that I offer in the context of the minor ICT and Society is called *Humans and Information Technology*. It is not currently a required course for any degree program. The other course is called *The Information Society* and it is a required course for first-year computer science students. In both these courses I teach many of the topics that can be found in he above list. In this way, I hope to acquaint students with what I see as the main topics in Social and Humanistic studies of Computing.

7. Teaching Computer ethics

For computer science students, or for other students specializing to become a computer professional of some sort (e.g., students specializing in library science or computer-assisted education) it would be highly advisable to have, in addition to a required Computers and Society course, a required course in *computer ethics*. Computers and Society courses for non-IT professionals should preferably include an ethics component, which considers ethical aspects of the use of information technology, and ethical aspects of social and policy choices that are made in society regarding information technology. To understand the role of computer ethics in the university curriculum, an understanding is needed of the kind of knowledge and skills that are the hallmark of it. I will try to arrive at such an understanding by analyzing the goals of computer ethics education and its relation to the goals of education in SHC and ASC.

To start with the second issue, is computer ethics a form of social and humanistic studies of computing, aimed at a *theoretical* understanding of ethical aspects of computing, or is it rather a form of *applied* research on societal aspects of computing,

aimed at developing practical professional tools? If one would take as one's point of departure Jim Moor's influential conception of computer ethics, one would have to conclude it is both. Moor claims: "On my view, computer ethics is the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology." (1985, p. 266). Quite clearly, the analysis Moor refers to in the first part of his statement is a central concern of SHC, whereas the formulation and justification of policies referred to in the second part clearly belongs to ASC. Thus we have more fundamental studies in computer ethics that belong to SHC and that are aimed at an understanding of ethical issues relating to computers and their uses, and we have more applied studies in computer ethics, that belong to ASC and that are aimed at arriving at specific policies.

In teaching a course in computer ethics, one may of course emphasize either the more fundamental or the more applied dimension of computer ethics. In a professional program for computer science students, one may want to opt for a course in computer ethics that is mostly applied, and that focuses on professional roles of computer scientists. In program in policy studies, or in law, or in science, technology and society, one would likely emphasize more fundamental issues in computer ethics. Normally, however, a course in computer ethics would integrate both dimensions. Regarding privacy, for example, it would both teach general moral theory on privacy, specific moral analyses of informational privacy, the various ways in which privacy considerations come up in contemporary computer systems and their uses, existing privacy law and policies, and professional responsibilities for protecting privacy.

An ideal course in computer ethics, then, should have both the goal of promoting an understanding of major ethical issues in computing, as well as of providing aspiring professionals with tools for giving content to their own professional responsibility in dealing with computer systems. In constructing such a course, one should begin with a selection of moral issues regarding computers that can be considered to be the most pressing in contemporary society. The will include many of well-known issues in the computer ethics literature. My own selection would certainly include issues of privacy, autonomy, justice (with special emphasis tot the problem of the so-called 'digital divide'), democracy, (informational) freedom and quality of life. Second, one should opt for a 'rich' presentation of these issues, in which one treats both (i) their moral worth and significance; (ii) the way they come up in current computing controversies (include here a consideration of one or more exemplary cases); (iii) past policies and laws that have been devised to deal with them; (iv) professional responsibilities regarding the issue and ways in which professionals may deal with them.

The way in which the professional component of a computer ethics course is set up will depend strongly on the nature of the professional program within which the course is situated. Obviously, in a law program, a course in computer ethics would focus on ethical issues in computer law, and how to deal with them professionally. In a program in education studies, a course in computer ethics would focus on ethical issues in designing education programs involving computers and in using computers in the classroom. In a program in computer science, there should be special emphasis on ethical issues in the design of computer systems and software (cf. Friedman and Nissenbaum, 1997; Brey, 1998, 2000), as well as in their maintenance and their operation. In all cases, the emphasis should not just be on the ethical issues that come up in these professions,

but also on the professional responsibility to deal with them, and the practical procedures one may follow in dealing with them.

8. Conclusion and implications for high school education

In this essay, I have argued for the importance of computer ethics policies and computer ethics education in higher education. I have argued that universities should have policies that address the ethical use and management of information technology on campus by students and staff. Relevant ethical issues include digital plagiarism and academic dishonesty in online assessment, copyright and software theft, the proper use of university computer resources, hacking, informational and online privacy, online anonymity and pseudonymity, online harassment and hate speech, and academic freedom and free speech online.

I have also argued for the importance of computer ethics education in higher education, which I have situated as part of a broader effort to help students understand societal aspects of information technology. I have argued in favor of a required course in university curricula on Computers and Society, that acquaints students with basic issues regarding the role of ICT in contemporary society, and a required course in ASC in professional programs, that focuses on the role of information technology within the relevant professional field and that conveys professional knowledge and skills that enable intelligent choices regarding the role of information technology within that field. I have also argued for computer ethics as a required course in professional programs that prepare students to become computer professionals. These courses should both acquaint students with major ethical issues in computing, and provide them with practical tools for giving content to their own professional responsibility in relation to computer systems.

Let me close by focusing on computer ethics policies and education on social and ethical aspects of IT in education *prior* to university, specifically in *secondary or high school education*. Regarding computer ethics policies, it will be clear that most of the policy issues for the use and management of information technology that apply to higher education also apply to secondary education: hacking, informational privacy, digital plagiarism and so forth are issues that may play in high school just as much as they may play at universities. One major difference may be the issue of academic freedom and freedom of speech. Because high school students have not yet reached adulthood, high schools arguably have an obligation to protect students from certain online content or ideas, unlike universities. Also they may arguably go futher than universities in limiting free speech in order to protect students from harassment and to provide a safe learning environment. Opinions on how far high schools may go on these points are bound to differ, however.

Let me turn, finally, education on social and ethical aspects of IT in secondary education. A difference between higher and secondary education is that in secondary education, there is less of an expectation that students will have a serious decision-making responsibility regarding information technology in their future profession. Hence, education in and SHC and ASC at the secondary school level may not be justified by reference to the future profession of secondary education students. The previously presented argument for attention to SHC in general education, however, certainly applies

to secondary education as well. Therefore, acquainting students with the role of ICT in society should be considered a legitimate and important topic in secondary education.

Next to this, I think there are also good reasons why an attention to ethical issues regarding ICT has a place in secondary education. Secondary education is the learning phase at which ethics can first be taught. Moral issues like abortion, the death penalty, and genetic engineering are great issues to explore in secondary school, not through an emphasis on moral theory, but though an emphasis on cases, and moral learning through a joint discussion of such cases. Their own morality in their everyday life should certainly also be a topic. In relation to this, it would be very useful to discuss with students the ethical issues that come up for *users* of information technology, for example in using the Internet, and to discuss also their own moral stance on these issues, as (potential) users of the technology.

Such a discussion is particularly important because information technology is not yet a technology that has reached "closure" (Pinch & Bijker, 1987). That is, the interpretations, rules, policies and patterns of behavior surrounding information technology are not yet as fixed as they are around many other technologies. The world of cyberspace is not yet an orderly society. It is still a bit the Wild West, and as this vast new space is being colonized, and made into an orderly society, everyone should be asking the question of what kind of society we want it to be. We as adults should not just ask this question to ourselves and to each other, but also to the new generation that will inhabit it.

References

Agre, P. & Rotenberg, M. (1998). *Technology and Privacy: The New Landscape*. Cambridge and London: MIT Press.

Austin, M.J. & Brown, L.D. (1999). 'Internet plagiarism: Developing strategies to curb student academic dishonesty,' *The Internet and higher education* 2:21-33.

Baase, S. (1997). *A gift of fire: Social, Legal and ethical issues in computing*. Upper Sadle River: Prentice Hall.

Baird, R. M. & Ramsower, R. & Rosenbaum, S.E. (eds.) (2000). *Cyberethics*. New York: Prometheus Books.

Beniger, J. (1986). *The Control Revolution: Technological and Economic Origins of the Information Sociey*. Cambridge, MA: Harvard University Press.

Brey, P. (1998) The Politics of Computer Systems and the Ethics of Design, in *Computer Ethics: Philosophical Enquiry* (ed. J. van den Hoven), Rotterdam University Press, Rotterdam.

Brey, P. (2000). Disclosive Computer Ethics. Computers and Society 30: 4, 10-16.

Brey, P. (2003). *Ethical Issues for the Virtual University*. Report for the cEVU Project (EuroPACE/European Commission). To appear online on www.cevu.org.

Castells, M. (2000). *The Rise of The Network Society*, 2nd ed. Blackwell.

Cate, F. (1997). *Privacy in the Information Age*. Washington, D.C.: Brookings Institutions Press.

Chester, A. & Gwynne, G. (1998). 'Online Teaching: Encouraging Collaboration through Anonymity,' *Journal of Computer Mediated Communication* 4 (2).

Clark, B.R. (1983). *The higher education system: Academic organization in cross-national perspective*. Berkeley: University of California press.

Cohen, E. & Cornwell, L. (1989). 'A question of ethics: developing information system ethics,' *Journal of Business Ethics* 8: 431-437.

Dijk, J. van (1999). *The Network Society*. Sage.

Forester, T. & Morrison, P. (1994). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in computing*, 2nd ed. Cambridge and London: MIT Press.

Friedman, B. and Nissenbaum, H. (1997) Bias in Computer Systems, in *Human Values and the Design of Computer Technology* (ed. B. Friedman), Cambridge University Press, Cambridge.

Glass, R. & Wood., W. (1996). 'Situational Determinants of Software Piracy: An Equity Theory Perspective,' *Journal of Business Ethics* 15: 1189-1198.

Hinman, L.M. (2002). 'The impact of the internet on our moral lives in academia,' *Ethics and information technology* 4: 31-35.

Johnson, D. (2000). *Computer Ethics*, 3rd ed. Upper Sadle River: Prentice Hall.

Kling, R. & Lee, Y. & Teich, A. & Frankel, M.S. (2000). '*Anonymous communication policies for the internet: Results and recommendations of the AAAS conference and assessing anonymous communication on the internet: Policy deliberations,'* In: Baird, R. M. & Ramsower, R. & Rosenbaum, S.E. (eds.) *Cyberethics*. New York: Prometheus Books.

Kling, R. (ed.), *Computerization and Controversy: Value Conflicts and Social Choices*. 2nd ed. Academic Press.

Kolko, B. (2000). '*Intellectual property in synchronous and collaborative virtual space,'* In: In: Baird, R., Ramsower, R. & Rosenbaum, S. (eds.) *Cyberethics*. New York: Prometheus Books.

Lipinski, T.A. & Britz, J.J. (1999). 'Deconstructing (the concept of) Intellectual Property: Designing and Incorporating Alternative Models of Property Ownership in the New Millennium and the Protection of Indigenous Knowledge,' *Proceedings of Ethicomp 99*. Luiss University, Rome, 5-8 October 1999. CD-ROM (1-13).

Moor, J. (1985) What is Computer Ethics? *Metaphilosophy*, **16**, 266-275.

Morse, J.F. (2001). 'Intellectual freedom and economic sufficiency as educational entitlements,' *Studies in philosophy and education* 20:201-211.

Olt, M.R. (2002). 'Ethics and distance education: strategies for minimizing academic dishonesty in online assessment.' *Online journal of distance learning administration*, vol. 5 (3). Unpaginated. http://www.westga.edu/~distance/ojdla/fall53/olt53.html.

Pinch, T., and Bijker, W. (1987). 'The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other,' in Bijker, W., Pinch, T., and Hughes, T., eds., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1987.

Rosenberg, R. (1997). *The Social Impact of Computers*. 2nd ed. Academic Press.

Rosenberg, R.S. (2001). 'Controlling access to the internet: the role of filtering.' *Ethics and Information Technology* 3:35-54.

Schellenberg, K. (ed.) (1999). *Computers in Society*. 8th ed. McGraw-Hill Higher Education.

Spinello, R. (2000). *Cyberethics. Morality and Law in Cyberspace*. Sudbury, MA: Jones and Bartlett Publishers.

Tavani, H. (2003). *Ethics and Technology: Ethical Issues in an Age of information and Communication Technology*. Wiley.

Tu, Chih-Hsiung (2002). 'The relationship between social presence and online privacy,' *The internet and higher education* 5:293-318.

Winters, P. (1997). *Computers and Society*. Greenhaven Press.