the world — as two of [these] letters seem to agree that it does — then why is it not reasonable, and indeed moral, to try to limit one's use of that technology? Of course, I think that I am right to do this.

I would not think so, obviously, if I agreed with Nathaniel S. Borenstein that "'better' is in the mind of the beholder." But if he truly believes this, I do not see why he bothers with his personal computer's "up-to-the-minute reports on the workings of the EPA and the nuclear industry" or why he wishes to be warned about "urgent legislative issues." According to his system, the "better" in a bureaucratic, industrial, or legislative mind is as good as the "better" in his. His mind apparently is being subverted by an objective standard of some sort, and he had better look out.

Borenstein does not say what he does after his computer has drummed him awake. I assume from his letter that he must send donations to conservation organizations and letters to officials. Like James Rhoads, at any rate, he has a clear conscience. But this is what is wrong with the conservation movement. It has a clear conscience. The guilty are always other people, and the wrong is always somewhere else; that is why Borenstein finds his "electronic bulletin board" so handy. To the conservation movement, it is only production that causes environmental degradation; the consumption that supports the production is rarely acknowledged to be at fault. The ideal of the run-of-the-mill conservationist is to impose restraints upon production without limiting consumption or burdening the consciences of consumers.

But virtually all of our consumption now is extravagant, and virtually all of it consumes the world. It is not beside the point that most electrical power comes from strip-mined coal. The history of the exploitation of the Appalachian coal fields is long, and it is available to readers. I do not see how anyone can read it and plug in any appliance with a clear conscience. If Rhoads can do so, that does not mean that his conscience is clear; it means that his conscience is not working.

To the extent that we consume, in our present circumstances, we are guilty. To the extent that we guilty consumers are conservationists, we are absurd. But what can we do? Must we go on writing letters to politicians and donating to conservation organizations until the majority of our fellow citizens agree with us? Or can we do something directly to solve our share of the problem?

I am a conservationist. I believe wholeheartedly in putting pressure on the politicians and in maintaining the conservation organizations. But I wrote my little essay partly in distrust of centralization. I don't think that the government and the conservation organizations alone will ever make us a conserving society. Why do I need a centralized computer system to alert me to environmental crises? That I live every hour of every day in an environmental crisis I know from all my senses. Why then is not my first duty to reduce, so far as I can, my own consumption?

Finally, it seems to me that none of my correspondents recognizes the innovativeness of my essay. If the use of a computer is a new idea, then a newer idea is not to use one.

22

Computer Ethics

DEBORAH G. JOHNSON

The many roles that computers play in society raise a host of ethical and legal issues: privacy, cybercrime, ownership of intellectual property, liability for damages, accountability, and more. But to what extent are these issues unique to computers and to what extent are they simply new areas of application for well-established ethical and legal principles? Many of these issues have developed as computers and their uses have grown and permeated society. The advent of the Internet has intensified issues of computer ethics and created new and more complex ones. And, as computer technology continues to evolve, new and more difficult ethical issues are likely to arise. Deborah Johnson, one of the most respected voices in this area, probes the field of computer ethics in a systematic manner that provides an effective introduction and a set of guideposts to structure our thinking about its many dimensions.

Deborah Johnson is chair of the Department of Science, Technology, and Society and Anne Shirley Carter Olsson Professor of Applied Ethics in the School of Engineering and Applied Science at the University of Virginia. Johnson holds a Ph.D. in philosophy from the University of Kansas and has taught at Rensselaer Polytechnic Institute and Georgia Institute of Technology. She is the author or editor of several books, including Computer Ethics, *the third edition of which was published in 2001, and many articles. This essay appeared first as a chapter in* The Blackwell Guide to the Philosophy of Computing and Information *(2003), edited by Luciano Floridi.*

From *The Blackwell Guide to the Philosophy of Computing and Information*, ed. Luciano Floridi.

INTRODUCTION

From the moment of their invention, computers have generated complex social, ethical, and value concerns. These concerns have been expressed in a variety of ways, from the science fiction stories of Isaac Asimov (1970) to a dense three-volume treatise on social theory by Manuel Castells (1996, 1997, 1998), and with much in between. Generally, the literature describes the social consequences of computing, speculates on the meaning of computation and information technology in human history, and creatively predicts the future path of development of computer technology and social institutions around it. A small, though steadily increasing, number of philosophers has focused specifically on the *ethical issues*.

As computer technology evolves and gets deployed in new ways, certain issues persist — issues of privacy, property rights, accountability, and social values. At the same time, seemingly new and unique issues emerge. The ethical issues can be organized in at least three different ways: according to the type of technology; according to the sector in which the technology is used; and according to ethical concepts or themes. In this chapter I will take the third approach. However, before doing so it will be useful to briefly describe the other two approaches.

The first is to organize the ethical issues by type of technology and its use. When computers were first invented, they were understood to be essentially sophisticated calculating machines, but they seemed to have the capacity to do that which was thought to be uniquely human — to reason and exhibit a high degree of rationality; hence, there was concern that computers threatened ideas about what it means to be human. In the shadow of the Second World War, concerns quickly turned to the use of computers by governments to centralize and concentrate power. These concerns accompanied the expanding use of computers for record-keeping and the exponential growth in the scale of databases, allowing the creation, maintenance, and manipulation of huge quantities of personal information. This was followed by the inception of software control systems and video games, raising issues of accountability — liability and property rights. This evolution of computer technology can be followed through to more recent developments including the internet, simulation and imaging technologies, and virtual reality systems. Each one of these developments was accompanied by conceptual and moral uncertainty. What will this or that development mean for the lives and values of human beings? What will it do to the relationship between government and citizen? Between employer and employee? Between businesses and consumers?

A second enlightening approach is to organize the issues according to the sector in which they occur. Ethical issues arise in real-world contexts, and computer-ethical issues arise in the contexts in which computers are used. Each context or sector has distinctive issues, and if we ignore this context we can miss important aspects of computer-ethical issues. For example, in dealing with privacy protection in general, we might miss the special importance of privacy protection for *medical records* where confidentiality is so essential to the doctor–patient relationship. Similarly, one might not fully understand the appropriate role for computers in education were one not sensitive to distinctive goals of education.

Both of these approaches — examining issues by types and uses of particular technologies, and sector by sector — are important and illuminating; however, they take us too far afield of the philosophical issues. The third approach — the approach to be taken in this chapter — is to emphasize ethical concepts and themes that persist across types of technology and sectors. Here the issues are sorted by their philosophical and ethical content. In this chapter I divide the issues into two broad categories: (1) metatheoretical and methodological issues, and (2) traditional and emerging issues.

METATHEORETICAL AND METHODOLOGICAL ISSUES

Perhaps the deepest philosophical thinking on computer-ethical issues has been reflection on the field itself — its appropriate subject matter, its relationship to other fields, and its methodology. In a seminal piece entitled "What is Computer Ethics?" Moor (1985) recognized that when computers are first introduced into an environment, they make it possible for human beings (individuals and institutions) to do things they couldn't do before, and this creates *policy vacuums*. We do not have rules, policies, and conventions on how to behave with regard to the new possibilities. Should employers monitor employees to the extent possible with computer software? Should doctors perform surgery remotely? Should I make copies of proprietary software? Is there any harm in me taking on a pseudo-identity in an online chatroom? Should companies doing business online be allowed to sell the transaction-generated information they collect? These are examples of policy vacuums created by computer technology.

Moor's account of computer ethics has shaped the field of computer ethics with many computer ethicists understanding their task to be that of helping to fill policy vacuums. Indeed, one of the topics of interest in computer ethics is to understand this activity of filling policy vacuums. This will be addressed later on.

The Connection Between Technology and Ethics

While Moor's account of computer ethics remains influential, it leaves several questions unanswered. Hence, discussion and debate continue around the question of why there is or should be a field of computer ethics and what the focus of the field should be.

In one of the deeper analyses, Floridi (1999) argues for a metaphysical foundation for computer ethics. He provides an account of computer ethics in which information has status such that destroying information can itself be morally wrong. In my own work I have tried to establish the foundation of computer ethics in the nonobvious connection between technology and ethics (Johnson 2001). Why is technology of relevance to ethics? What difference can technology make to human action? To human affairs? To moral concepts or theories?

Two steps are involved in answering these questions. The first step involves fully recognizing something that Moor's account acknowledges, namely that technology often makes it possible for human beings to do what they could not do without it. Think of spaceships that take human beings to the moon; think of imaging technology that allows us to view internal organs; or think of computer viruses that wreak havoc on the internet.

Of course, it is not just that human beings can do what they couldn't do before. It is also that we can do the same sorts of things we did before, only in new ways. As a result of technology, we can travel, work, keep records, be entertained, communicate, and engage in warfare *in new ways*. When we engage in these activities using computer technology, our actions have different properties, properties that may change the character of the activity or action-type. Consider the act of writing with various technologies. When I write with paper and pencil, the pencil moves over paper; when I write using a typewriter, levers and gears move; when I write using a computer, electronic impulses change configurations in microchips. So, the physical events that take place when I write are very different when I use computer technology.

Using action theory, the change can be characterized as a change in the possible act tokens of an act type. An act type is a kind of action (e.g. reading a book, walking) and an act token is a particular instance of an act type. An act token is an instance of the act type performed by a particular person, at a particular time, and in a particular place. For example, "Jan is, at this moment, playing chess with Jim in Room 200 of Thornton Hall on the campus of University of Virginia" is an act token of the act type "playing chess." When technology is involved in the performance of an act type, a new set of act tokens may become possible. It is now possible, for example, to "play chess" while sitting in front of a computer and not involving another human being. Instead of manually moving three-dimensional pieces, one presses keys on a keyboard or clicks on a mouse. Thus, when human beings perform actions with computers, new sets of tokens (of act types) become possible. Most important, the new act tokens have properties that are distinct from other tokens of the same act type.

Computer technology instruments human action in ways that turn very simple movements into very powerful actions. Consider hardly-visible finger movements on a keyboard. When the keyboard is connected to a computer and the computer is connected to the internet, and when the simple finger movements create and launch a computer virus, those simple finger movements can wreak havoc in the lives of thousands (even millions) of people. The technology has instrumented an action not possible without it. To be sure, individuals could wreak havoc on the lives of others before computer technology, but not in this way and perhaps not quite so easily. Computer technology is not unique among technologies in this respect; other technologies have turned simple movements of the body into powerful actions, e.g. dynamite, automobiles.

Recognizing the intimate connection between technology and human action is important for stopping the deflection of human responsibility in technology-instrumented activities, especially when something goes wrong. Hence, the hacker cannot avoid responsibility for launching a virus on grounds that he simply moved his fingers while sitting in his home. Technology does nothing independent of human initiative; though, of course, sometimes human beings cannot foresee what it is they are doing with technology.

Thus, the first step in understanding the connection between computer technology and ethics is to acknowledge how intimate the connection between (computer) technology and human action can be. The second step is to connect human action to ethics. This step may seem too obvious to be worthy of mention since ethics is often understood to be exclusively the domain of human action. Even so, computer technology changes the domain of human action; hence, it is worth asking whether these changes have moral significance. Does the involvement of computer technology — in a human situation — have moral significance? Does the *instrumentation* of human action affect the character of ethical issues, the nature of ethical theory, or ethical decision-making?

The involvement of computer technology has moral significance for several reasons. As mentioned earlier, technology creates new possibilities for human action and this means that human beings face ethical questions they never faced before. Should we develop biological weapons and risk a biological war? Should I give my organs for transplantation? In the case of computer technology, is it wrong to monitor keystrokes of employees who are using computers? To place cookies on computers when the computers are used to visit a website? To combine separate pieces of personal data into a single comprehensive portfolio of a person?

When technology changes the properties of tokens of an act type, the moral character of the act type can change. In workplace monitoring, for example, while it is generally morally acceptable for employers to keep track of the work of employees, the creation of software that allows the employer to record and analyze every keystroke an employee makes raises the question in a new way. The rights of employers and employees have to be reconsidered in light of this new possibility. Or to use a different sort of example, when it comes to property rights in software, the notion of property and the stakes in owning and copying are significantly different when it comes to computer software because computer software has properties unlike that of anything else. Most notably, software can be replicated with no loss to the owner in terms of possession or usefulness (though, of course, there is a loss in the value of the software in the marketplace).

So, computers and ethics are connected insofar as computers make it possible for humans to do things they couldn't do before and to do things they could do before but in new ways. These changes often have moral significance.

APPLIED AND SYNTHETIC ETHICS

To say that computer technology creates new tokens of an act type may lead some to categorize computer ethics as a branch of applied or practical ethics. Once a computer ethical issue is understood to involve familiar act types, it might be

presumed, all that is necessary to resolve the issue is to use moral principles and theories that generally apply to the act type. For example, if the situation involves honesty in communicating information, simply follow the principle, "tell the truth," with all its special conditions and caveats. Or, if the situation involves producing some positive and negative effects, simply do the utilitarian calculation. This account of computer ethics is, however, as controversial as is the notion of "applied ethics" more generally.

For one thing, computer technology and the human situations arising around it are not always so easy to understand. As Moor has pointed out, often there are conceptual muddles (1985). What is software? What is a computer virus? How are we to conceptualize a search engine? A cookie? A virtual harm? In other words, computer ethicists do more than "apply" principles and theories; they do conceptual analysis. Moreover, the analysis of a computer-ethical issue often involves synthesis, synthesis that creates an understanding of both the technology and the ethical situation. A fascinating illustration of this is the case of a virtual rape (Dibbell 1993). Here a character in a multi-user virtual reality game rapes another character. Those participating in the game are outraged and consider the behavior of the real person controlling the virtual characters offensive and bad. The computer ethical issue involves figuring out what, if anything, wrong the real person controlling the virtual character has done. This involves understanding how the technology works, what the real person did, figuring out how to characterize the actions, and then recommending how the behavior should be viewed and responded to. Again, analysis of this kind involves more than simply "applying" principles and theories. It involves conceptual analysis and interpretation. Indeed, the synthetic analysis may have implications that reflect back on the meaning of, or our understanding of, familiar moral principles and theories.

To be sure, philosophical work in computer ethics often does involve drawing on and extending the work of well-known philosophers and making use of familiar moral concepts, principles, and theories. For example, computer ethical issues have frequently been framed in utilitarian, deontological, and social contract theory. Many scholars writing about the internet have drawn on the work of existentialist philosophers such as Søren Kierkegaard (Dreyfus 1999; Prosser & Ward 2000) and Gabriel Marcel (Anderson 2000). The work of Jürgen Habermas has been an important influence on scholars working on computer-mediated communication (Ess 1996). Recently van den Hoven (1999) has used Michael Walzer's "spheres of justice" to analyze the information society; Cohen (2000) and Introna (2001) have used Emmanuel Levinas to understand internet communication; Adams and Ofori-Amanfo (2000) have been connecting feminist ethics to computer ethics; and Grodzinsky (1999) has developed virtue theory to illuminate computer ethics.

Nevertheless, while computer ethicists often draw on, extend, and "apply" moral concepts and theories, computer ethics involves much more than this. Brey (2000) has recently argued for an approach that he labels "disclosive computer ethics." The applied ethics model, he notes, emphasizes controversial issues for which the ethical component is transparent. Brey argues that there are many

nontransparent issues, issues that are not so readily recognized. Analysis must be done to "disclose" and make visible the values at stake in the design and use of computer technology. A salient example here is work by Introna and Nissenbaum (2000) on search engines. They show how the design of search engines is laden with value choices. In order to address those value choices explicitly, the values embedded in search engine design must be uncovered and disclosed. This may sound simple but in fact uncovering the values embedded in technology involves understanding how the technology works and how it affects human behavior and human values.

Setting aside what is the best account of computer ethics, it should be clear that a major concern of the field is to understand its domain, its methodology, its reason for being, and its relationship to other areas of ethical inquiry. As computer technology evolves and gets deployed in new ways, more and more ethical issues are likely to arise.

TRADITIONAL AND EMERGING ISSUES

"Information society" is the term often used (especially by economists and sociologists) to characterize societies in which human activity and social institutions have been significantly transformed by computer and information technology. Using this term, computer ethics can be thought of as the field that examines ethical issues distinctive to "an information society." Here I will focus on a subset of these issues, those having to do with professional ethics, privacy, cyber crime, virtual reality, and general characteristics of the internet.

Ethics for Computer Professionals

In an information society, a large number of individuals are educated for and employed in jobs that involve development, maintenance, buying and selling, and use of computer and information technology. Indeed, an information society is dependent on such individuals — dependent on their special knowledge and expertise and on their fulfilling correlative social responsibilities. Expertise in computing can be deployed recklessly or cautiously, used for good or ill, and the organization of information technology experts into occupations/professions is an important social means of managing that expertise in ways that serve human well-being.

An important philosophical issue here has to do with understanding and justifying the social responsibilities of computer experts. Recognizing that justification of the social responsibilities of computer experts is connected to more general notions of duty and responsibility, computer ethicists have drawn on a variety of traditional philosophical concepts and theories, but especially social contract theory.

Notice that the connection between being a computer expert and having a duty to deploy that expertise for the good of humanity cannot be explained simply as a causal relationship. For one thing, one can ask "why?" Why does

the role of computer expert carry with it social responsibilities? For another, individuals acting in occupational roles are typically not acting simply as individual autonomous moral agents; they act as employees of companies or agencies, and may not be involved in the decisions that most critically determine project outcomes. Hence, there is a theoretical problem in explaining why and to what extent individuals acting in occupational roles are responsible for the effects of their work.

Social contract theory provides an account of the connection between occupational roles and social responsibilities. A social contract exists between members of an occupational group and the communities or societies of which they are a part. Society (states, provinces, communities) allows occupational groups to form professional organizations, to make use of educational institutions to train their members, to control admission, and so on, but all of this is granted in exchange for a commitment to organize and control the occupational group in ways that benefit society. In other words, a profession and its members acquire certain privileges in exchange for accepting certain social responsibilities.

The substantive content of those responsibilities has also been a topic of focus for computer ethicists. Computer professional groups have developed and promulgated codes of professional and ethical conduct that delineate in broad terms what is and is not required of computer experts. See, for example, the ACM [Association for Computing Machinery — the premier membership organization for computer professionals] Code of Ethics and Professional Conduct or the Code of Conduct of the British Computer Society. Since these codes are very general, there has been a good deal of discussion as to their appropriate role and function. Should they be considered comparable to law? Should there be enforcement mechanisms and sanctions for those who violate the code? Or should codes of conduct aim at inspiration? If so, then they should merely consist of a statement of ideals and need not be followed "to the letter" but only in spirit.

At least one computer ethicist has gone so far as to argue that the central task of the field of computer ethics is to work out issues of professional ethics for computer professionals. Gotterbarn (1995: 21) writes that the "only way to make sense of 'Computer Ethics' is to narrow its focus to those actions that are within the control of the individual *moral* computer professional."

While Gotterbarn's position is provocative, it is not at all clear that it is right. For one thing, many of the core issues in computer ethics are social value and policy issues, such as privacy and property rights. These are issues for all citizens, not just computer professionals. Moreover, many of the core issues faced by computer professionals are not unique to computing; they are similar to issues facing other occupational groups: What do we owe our clients? Our employers? When are we justified in blowing the whistle? How can we best protect the public from risk? Furthermore, since many computer professionals work in private industry, many of the issues they face are general issues of business ethics. They have to do with buying and selling, advertising, proprietary data, competitive practices, and so on. Thus, it would be a mistake to think that all of the ethical issues surrounding computer and information technology are simply ethical issues for computer professionals. Computer experts face many complex

and distinctive issues, but these are only a subset of the ethical issues surrounding computer and information technology.

Privacy

In an "information society" privacy is a major concern in that much (though by no means all) of the information gathered and processed is information about individuals. Computer technology makes possible a previously unimaginable magnitude of data collection, storage, retention, and exchange. Indeed, computer technology has made information collection a built-in feature of many activities, for example, using a credit card, making a phone call, browsing the web. Such information is often referred to as transaction-generated information or TGI.

Computer ethicists often draw on prior philosophical and legal analysis of privacy and focus on two fundamental questions: What is privacy? Why is it of value? These questions have been contentious and privacy often appears to be an elusive concept. Some argue that privacy can be reduced to other concepts such as property or liberty; some argue that privacy is something in its own right and that it is intrinsically valuable; yet others argue that while not intrinsically valuable, privacy is instrumental to other things that we value deeply — friendship, intimacy, and democracy.

Computer ethicists have taken up privacy issues in parallel with more popular public concerns about the social effects of so much personal information being gathered and exchanged. The fear is that an "information society" can easily become a "surveillance society." Here computer ethicists have drawn on the work of Bentham and Foucault suggesting that all the data being gathered about individuals may create a world in which we effectively live our daily lives in a panopticon (Reiman 1995). "Panopticon" is the shape of a structure that Jeremy Bentham designed for prisons. In a panopticon, prison cells are arranged in a circle with the inside wall of each cell made of glass so that a guard, sitting in a guard tower situated in the center of the circle, can see everything that happens in each and every cell. The effect is not two-way; that is, the prisoners cannot see the guard in the tower. In fact, a prison guard need not be in the guard tower for the panopticon to have its effect; it is enough that prisoners believe they are being watched. When individuals believe they are being watched, they adjust their behavior accordingly; they take into account how the watcher will perceive their behavior. This influences individual behavior and how individuals see themselves.

While computerized information-gathering does not physically create the structure of a panopticon, it does something similar insofar as it makes a good deal of individual behavior available for observation. Thus, data collection activities of an information society could have the panopticon effect. Individuals would know that most of what they do can be observed and this could influence how they behave. When human behavior is monitored, recorded, and tracked, individuals could become intent on conforming to norms for fear of negative consequences. If this were to happen to a significant extent, it might incapacitate individuals in acting freely and thinking critically — capacities necessary to realize democracy. In this respect, the privacy issues around computer technology go to the heart of freedom and democracy.

It might be argued that the panoptic effect will not occur in information societies because data collection is invisible so that individuals are unaware they are being watched. This is a possibility, but it is also possible that as individuals become more and more accustomed to information societies, they will become more aware of the extent to which they are being watched. They may come to see how information gathered in various places is put together and used to make decisions that affect their interactions with government agencies, credit bureaus, insurance companies, educational institutions, employers, etc.

Concerns about privacy have been taken up in the policy arena, with a variety of legislation controlling and limiting the collection and use of personal data. An important focus here has been comparative analyses of policies in different countries — for they vary a good deal. The American approach has been piecemeal, with separate legislation for different kinds of records (i.e., medical records, employment histories, credit records), whereas several European countries have comprehensive policies that specify what kind of information can be collected under what conditions in *all* domains. Currently the policy debates are pressured by the intensification of global business. Information-gathering organizations promise data subjects that they will only use information in certain ways; yet, in a global economy, data collected in one country — with a certain kind of data protection — can flow to another country where there is no or different protection. An information-gathering organization might promise to treat information in a certain way, and then send the information abroad where it is treated in a completely different way, thus breaking the promise made to the data subject. To assure that this does not happen, a good deal of attention is currently being focused on working out international arrangements and agreements for the flow of data across national boundaries.

Cybercrime and Abuse

While the threats to privacy described above arise from *uses* of computer and information technology, other threats arise from *abuses*. As individuals and companies do more and more electronically, their privacy and property rights become ever more important, and these rights are sometimes threatened by individuals who defy the law or test its limits. Such individuals may seek personal gain or may just enjoy the challenge of figuring out how to *crack* security mechanisms. They are often called *hackers* or *crackers*. The term *hacker* used to refer to individuals who simply loved the challenge of working on programs and figuring out how to do complex things with computers, but did not necessarily break the law. *Crackers* were those who broke the law. However, the terms are now used somewhat interchangeably to refer to those who engage in criminal activity.

The culture of hackers and crackers has been of interest not only because of the threat posed by their activities, but also because the culture of hackers and crackers represents an alternative vision of how computer technology might be developed and used, one that has intrigued philosophers. Hackers and crackers often defend their behavior by arguing for a much more open system of computing with a freer flow of information, creating an environment in which

individuals can readily share tools and ideas. In particular, the culture suggests that a policy of no ownership of software might lead to better computing. This issue goes to the heart of philosophical theories of property, raising traditional debates about the foundations of property, especially intellectual property.

Some draw on Locke's labor theory of property and argue that software developers have a natural right to control the use of their software. Others, such as me, argue that while there are good utilitarian reasons for granting ownership in software, natural rights arguments do not justify private ownership of software (Johnson 2001). There is nothing inherently unfair about living in a world in which one does not own and cannot control the use of software one has created.

Nevertheless, currently, in many industrialized countries there are laws against copying and distributing proprietary software, and computer ethicists have addressed issues around violations of these laws. Conceptually, some have wondered whether there is a difference between familiar crimes such as theft or harassment and parallel crimes done using computers. Is there any morally significant difference between stealing (copying and selling copies of) a software program and stealing a car? Is harassment via the internet morally any different than face-to-face harassment? The question arises because actions and interactions on the internet have some distinguishing features. On the internet, individuals can act under the shroud of a certain kind of anonymity. They can disguise themselves through the mediation of computers. This together with the reproducibility of information in computer systems makes for a distinctive environment for criminal behavior. One obvious difference in cybertheft is that the thief does not deprive the owner of the use of the property. The owner still has access to the software, though of course the market value of the software is diminished when there is rampant copying.

Computer ethicists have taken up the task of trying to understand and conceptualize cybercrimes as well as determining how to think about their severity and appropriate punishment. Criminal behavior is nothing new, but in an information society new types of crimes are made possible, and the actions necessary to catch criminals and prevent crimes are different.

Internet Issues

Arguably the internet is the most powerful technological development of the late twentieth century. The internet brings together many industries, but especially the computer, telecommunications, and media enterprises. It brings together and provides a forum for millions of individuals and businesses around the world. It is not surprising, then, that the internet is currently a major focus of attention for computer ethicists. The development of the internet has involved moving many basic social institutions from a paper and ink medium to the electronic medium. The question for ethicists is this: is there anything ethically distinctive about the internet? (A parallel question was asked in the last section with regard to cybercrime.)

The internet seems to have three features that make it unusual or special. First, it has an unusual scope in that it provides many-to-many communication on a global scale. Of course, television and radio as well as the telephone are

global in scale, but television and radio are one-to-many forms of communication, and the telephone, which is many-to-many, is expensive and more difficult to use. With the internet, individuals and companies can have much more frequent communication with one another, in real time, at relatively low cost, with ease and with visual as well as sound components. Second, the internet facilitates a certain kind of anonymity. One can communicate extensively with individuals across the globe (with ease and minimal cost), using pseudonyms or real identities, and yet one never has to encounter the others face-to-face. This type of anonymity affects the content and nature of the communication that takes place on the internet. The third special feature of the internet is its reproducibility. When put on the internet, text, software, music, and video can be duplicated *ad infinitum*. They can also be altered with ease. Moreover, the reproducibility of the medium means that all activity on the internet is recorded and can be traced.

These three features of the internet — global many-to-many scope, anonymity, and reproducibility — have enormous positive as well as negative potential. The global, many-to-many scope can bring people from around the globe closer together, relegating geographic distance to insignificance. This feature is especially freeing to those for whom travel is physically challenging or inordinately expensive. At the same time, these potential benefits come with drawbacks; one of the drawbacks is that this power also goes to those who would use it for heinous purposes. Individuals can — while sitting anywhere in the world, with very little effort — launch viruses and disrupt communication between others. They can misrepresent themselves and dupe others on a much larger scale than before the internet.

Similarly, anonymity has both benefits and dangers. The kind of anonymity available on the internet frees some individuals by removing barriers based on physical appearance. For example, in contexts in which race and gender may get in the way of fair treatment, the anonymity provided by the internet can eliminate bias; for example, in on-line education, race, gender, and physical appearance are removed as factors affecting student-to-student interactions as well as the teacher evaluations of students. Anonymity may also facilitate participation in beneficial activities such as discussions among rape victims or battered wives or ex-cons where individuals might be reluctant to participate unless they had anonymity.

Nevertheless, anonymity leads to serious problems of accountability and for the integrity of information. It is difficult to catch criminals who act under the shroud of anonymity. And anonymity contributes to the lack of integrity of electronic information. Perhaps the best illustration of this is information one acquires in chatrooms on the internet. It is difficult (though not impossible) to be certain of the identities of the persons with whom one is chatting. The same person may be contributing information under multiple identities; multiple individuals may be using the same identity; participants may have vested interests in the information being discussed (e.g., a participant may be an employee of the company/product being discussed). When one can't determine the real source of information or develop a history of experiences with a source, it is impossible to gauge the trustworthiness of the information.

Like global scope and anonymity, reproducibility also has benefits and dangers. Reproducibility facilitates access to information and communication; it allows words

and documents to be forwarded (and downloaded) to an almost infinite number of sites. It also helps in tracing cybercriminals. At the same time, however, reproducibility threatens privacy and property rights. It adds to the problems of accountability and integrity of information arising from anonymity. For example, when I am teaching a class, students can now send their assignments to me electronically. This saves time, is convenient, saves paper, etc. At the same time, however, the reproducibility of the medium raises questions about the integrity of the assignments. How can I be sure the student wrote the paper and didn't download it from the web?

When human activities move to the internet, features of these activities change and the changes may have ethical implications. The internet has led to a wide array of such changes. The task of computer ethics is to ferret out these changes and address the policy vacuums they create.

Virtual Reality

One of the most philosophically intriguing capacities of computer technology is "virtual reality systems." These are systems that graphically and aurally represent environments, environments into which individuals can project themselves and interact. Virtual environments can be designed to represent real-life situations and then used to train individuals for those environments, e.g., pilot training programs. They can also be designed to do just the opposite, that is, to create environments with features radically different from the real world, e.g., fantasy games. Ethicists have just begun to take up the issues posed by virtual reality and the issues are deep (Brey 1999). The meaning of actions in virtual reality is what is at stake as well as the moral accountability of individual behavior in virtual systems. When one acts in virtual systems one "does" something, though it is not the action represented. For example, killing a figure in a violent fantasy game is not the equivalent of killing a real person. Nevertheless, actions in virtual systems can have real-world consequences; for example, violence in a fantasy game may have an impact on the real player or, as another example, the pilot flying in the flight simulator may be judged unprepared for real flight. As human beings spend more and more time in virtual systems, ethicists will have to analyze what virtual actions mean and what, if any, accountability individuals bear for their virtual actions.

CONCLUSION

This chapter has covered only a selection of the topics addressed by philosophers working in the field of computer ethics. Since computers and information technology are likely to continue to evolve and become further integrated into the human and natural world, new ethical issues are likely to arise. On the other hand, as we become more and more accustomed to acting with and through computer technology, the difference between "ethics" and "computer ethics" may well disappear.

REFERENCES

Adams, A. and Ofori-Amanfo, J. 2000. "Does gender matter in computer ethics?" *Ethics and Information Technology* 2(1): 37–47.

Anderson, T. C. 2000. "The body and communities in cyberspace: a Marcellian analysis." *Ethics and Information Technology* 2(3): 153–8.

Asimov, I. 1970. *I, Robot.* Greenwich, CT: Fawcett Publications.

Brey, P. 1999. "The ethics of representation and action in virtual reality." *Ethics and Information Technology* 1(1): 5–14.

Brey, P. 2000. "Disclosive computer ethics." *Computers & Society*, Dec.: 10–16.

Castells, M. 1996. *The Rise of the Network Society.* Malden, MA: Blackwell Publishers.

——— 1997. *The Power of Identity.* Malden, MA: Blackwell Publishers.

——— 1998. *The End of Millennium.* Malden, MA: Blackwell Publishers.

Cohen, R. A. 2000. "Ethics and cybernetics: Levinasian reflections." *Ethics and Information Technology* 2(1): 27–35.

Dibbell, J. 1993. "A rape in cyberspace: how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society." *The Village Voice*, Dec. 23: 36–42.

Dreyfus, H. L. 1999. "Anonymity versus commitment: the dangers of education on the internet." *Ethics and Information Technology* 1(1): 15–21.

Ess, C., ed. 1996. *Philosophical Perspectives on Computer-Mediated Communication.* Albany: State University of New York Press.

Floridi, L. 1999. "Information ethics: on the philosophical foundation of computer ethics." *Ethics and Information Technology* 1(1): 37–56.

Gotterbarn, D. 1995. "Computer ethics: responsibility regained." In D. G. Johnson and H. Nissenbaum, eds., *Computers, Ethics and Social Values.* Englewood Cliffs, NJ: Prentice Hall, pp. 18–24.

Grodzinsky, F. S. 1999. "The practitioner from within: revisiting the virtues." *Computers & Society* 29(1): 9–15.

Introna, L. D. 2001. "Proximity and simulacra: ethics in an electronically mediated world." *Philosophy in the Contemporary World* (forthcoming).

——— and Nissenbaum, H. 2000. "Shaping the web: why the politics of search engines matters." *The Information Society* 16(3): 169–85.

Johnson, D. G. 2001. *Computer Ethics*, 3rd ed. Upper Saddle River, NJ: Prentice Hall.

Moor, J. 1985. "What is computer ethics?" *Metaphilosophy* 16(4): 266–75.

Prosser, B. T. and Ward, A. 2000. "Kierkegaard and the internet: existential reflections on education and community." *Ethics and Information Technology* 2(3): 167–80.

Reiman, J. H. 1995. "Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future." *Computer and High Technology Law Journal* 11: 27–44.

van den Hoven, J. 1999. "Privacy and the varieties of informational wrongdoing." *Australian Journal of Professional and Applied Ethics* 1(1): 30–43.

23

The Internet Under Siege

LAWRENCE LESSIG

In the early and mid-1990s, when the Internet was just beginning to grow into the vast network it is today, it was a huge laboratory for experimentation with new technologies and new ideas. Its capabilities, Lawrence Lessig writes, engendered "an explosion of creativity." But that era has passed as quickly as it arose. Today, says Lessig, "Under the guise of protecting private property, a series of new laws and regulations are dismantling the very architecture that made the Internet a framework for global innovation." The owners of old media (for example, the firms that control the production and distribution of popular music) are reining in the potential of the Internet to make fundamental changes in the way media are distributed (e.g., through Napster and other online music trading technologies). Worst of all, Lessig believes, the U.S. Congress and governments throughout the industrialized world are collaborating in the actions of these reactionary forces through such regulations and laws as the Digital Millennium Copyright Act, which bans technologies intended to circumvent copyright protections.

Lawrence Lessig is one of the most articulate and thoughtful spokesmen for openness in information and telecommunications technology. He is professor of law and John A. Wilson Distinguished Faculty Scholar at Stanford University and the founding director of Stanford's Center for Internet and Society. Lessig is a prolific writer and a much sought after speaker and has been a participant in many court proceedings and congressional hearings relating to such topics as The U.S. v. Microsoft, *The Computer Decency Act, and Napster. He is author of* Code: Version 2.0 *(2007),* Free Culture *(2004), and* The Future of Ideas: The Fate of the Commons in the Connected World *(2001).*

From *Foreign Policy*, Issue #127, Nov.–Dec. 2001. Reprinted by permission of International Creative Management, Inc.