

The overall strategy of utilitarianism is to try to bring about the greatest benefit and least harm for the greatest number of people. It is important to note that risks and probabilities count also, because increased risk of harm is bad and increased probability of benefit is good.

You can make use of these ideas in your case analysis by examining for each person (regardless of his or her station in life) the likely benefits and harms for that person. The best course of action would be the one that is likely to bring about, for the greatest number of people, the most benefit and the least harm.

- 2 **Aristotelian ideas** Key ideas in the ethical theories of Aristotle and his followers are virtues and vices. The virtues include positive character traits such as *courage, integrity, honesty, fidelity, reliability, generosity, responsibility, self-discipline, temperance, modesty, and persistence* (to name several examples). According to Aristotle, people who are appropriately raised by their families and their communities will usually develop patterns of behavior consistent with the virtues. And given appropriate experiences, they will come to recognize examples of virtue and vice.

Aristotle described the ethical virtues as rational character traits that occupy an appropriate middle ground between unreasonable extremes. *Courage*, for example, is a positive trait associated with rational control of fear. It lies between the excess of *cowardice*, associated with fear-driven behavior, and the deficiency of *foolhardiness*, associated with a lack of appropriate fear. *Good temper* is a virtue associated with rational control of anger; while the vice of *irascibility* is unreasonable proneness to anger, and the vice of *apathy to wrong doing* is unreasonable lack of anger about injustice.

To perform an Aristotelian analysis of a case, you should systematically identify the virtuous behavior of participants, as well as any examples of surrender to the vices.

- 3 **Kantian ideas** Philosopher Immanuel Kant made respect for persons the central concept in his ethical theory. Because human beings are rational beings, said Kant, they have worth in themselves and do not need anything outside of themselves to give them worth. For this reason, the fundamental principle of Kant's ethics, which he called *the categorical imperative*, can be stated this way:

THE CATEGORICAL IMPERATIVE Always treat every person, including yourself, as a being that has worth in itself, never merely as a being to be used to advance someone else's goals.

According to Kant, therefore, one must always respect the worth and dignity of a person, and never merely use him or her. Lying and cheating, for example, would be unethical because they involve merely using other people to achieve your own goals. Failure to uphold the rights of

someone would be unethical because it would not show proper respect for the that person, and it would not allow the person to be a responsible agent taking responsibility for his or her own life.

In your case analysis, you can take advantage of Kant's ethical insight by asking whether each participant in the situation has been treated in a manner consistent with the categorical imperative.

7. Draw relevant ethical conclusions about the case

By engaging in all or most of the above-described "steps" of analysis, you are likely to have gained an impressive set of insights into the ethical issues and alternatives, putting you in a good position to draw relevant conclusions. What are the key ethical issues? Did anyone do anything unethical? Why do you think so? If the case involves possible future actions, what should those actions be, and what are the relevant ethical considerations that would justify them? If there are competing values or considerations, how would you rank them and why?

8. Draw relevant lessons about the future

If some of the participants in the case acted unethically, how can similar actions be prevented or decreased in the future? If you have identified any "policy vacuums" that need to be filled, what new policies would you recommend, and what are the ethical considerations that would justify them? It is worth noting that any new policies that you recommend will have the best chance of being adopted by the relevant community if they are similar in significant ways to already existing policies. A policy that "sticks out like a sore thumb" and seems to fly in the face of common standards of good practice would need a very persuasive ethical justification to be accepted.

A Sample Case to Analyze: The Extortionist Softbot

Given the above-presented "heuristic method of case analysis", we are now in position to consider a sample case (fictional, but realistic) and to develop an example case analysis. Our imagined case is this:

The case of the extortionist softbot

The term "softbot" is short for "software robot." A softbot resides within a computer or a network of computers and performs various "actions" there.

A "planner-based" softbot is a kind of "intelligent agent" that is assigned goals by a user and then employs artificial intelligence to create and carry out a plan to fulfill the user's goals. Planner-based softbots can travel through computer networks, such as the Internet, gathering information and using that information to perform various software-driven tasks.

CharityBot.com is a software company that creates planner-based softbots to help charitable organizations raise money. One of their most successful products is a "softbot template" called EMAILFUNDER, which can be used by charitable organizations to create their own customized softbots for soliciting donations over the Internet. EMAILFUNDER combines several software "agents" that perform various tasks:

E_RESEARCHER This *research agent* crawls through the Internet gathering various kinds of information about individuals – information from web pages, databases, news services, credit agencies, chat rooms, and so on.

E_PROFILER Using information from E_RESEARCHER, this *personal profile agent* creates profiles of individual people – their email addresses, employment records, economic status, credit ratings, leisure-time activities, social activities, friends and associates, and many other kinds of information.

E_MAEI_WRITER The user provides a sample email message to this *email writing agent*, which then uses information from E_PROFILER to generate emailed solicitations asking people to donate money. E_MAEI_WRITER is artificially intelligent and is able to generate minor variations of the sample email message by using information from personal profiles and substituting relevant words. CharityBot.com considers this to be a major selling point of EMAILFUNDER because customized emails can play upon the interests of recipients, making them more likely to donate money to the charity.

MESSAGE_TESTR This *statistical testing agent* keeps statistics about the success rate of each variation of the sample email message. After E_MAEI_WRITER has created a new version of the sample message and has emailed it to a thousand recipients, MESSAGE_TESTR determines the percentage of successful solicitations. If a particular message proves to be especially effective as a fundraiser, E_MAEI_WRITER is instructed to send out many thousands of copies. E_MAEI_WRITER and MESSAGE_TESTR, working together, can create and test dozens of message variations per week.

E_BANKR This *electronic banking agent* receives credit-card based donations and deposits them electronically into the charity's bank account. It also automatically updates the charity's financial records to take account of the new funds.

Within weeks of hitting the market, EMAILFUNDER created a number of customized softbots that proved to be reasonably successful fundraisers for a number of charities. When Joe Biggheart, the chief fundraiser for a child cancer charity, learned about this, he decided to try EMAILFUNDER for a major fundraising project.

Joe leased a copy of EMAILFUNDER from CharityBot.com and attended a workshop to learn how to use it. During the workshop, Joe expressed some worries about the quality and appropriateness of email messages written by E_MAEI_WRITER. He also expressed some concern about possible privacy violations associated with personal profiles. The workshop leaders seemed annoyed by Joe's questions, and they quickly assured him that his worries were unfounded. Joe was surprised that they were annoyed, and he quickly changed the subject.

After the workshop, Joe dismissed his worries and initiated his fundraising project by providing a sample email message to his softbot and placing the softbot onto the Internet. Joe's sample message began as follows:

Dear {recipient},

We recently learned of your interest in children and health, and so we are writing to ask you to consider making a donation to the Children's Anti-Cancer Fund. We hope that you will be able to make a generous gift; and if you find it possible to give \$1,000 or more, we will list your name on our "Web Site of Excellence" to honor you for your commitment to children and health.

After three days, Joe checked the electronic bank account of the Children's Anti-Cancer Fund and was pleased to find that nearly \$1,000 had already been donated.

Because of a family crisis, Joe had to be away from the office for nearly a week. When he returned to the office, he was surprised to see how much money had been donated while he was away, and he anxiously read the computer-generated variation of his fund-raising letter to see why it had been so successful. Here is what he read:

Dear {recipient},

We recently learned of your interest in children and lust, and so we are writing to ask you to consider making a donation to the Children's Anti-Cancer Fund. We hope that you will be able to make a generous gift; and if you find it impossible to give \$1,000 or more, we will list your name on our "Web Site of Excellence" to honor you for your commitment to children and lust.

Joe Biggheart was horrified to learn that his softbot, which was created by using EMAILFUNDER, had sent this computer-generated "extortion letter" to thousands of wealthy men who were regular visitors of pornographic web sites. As a result, several of those men donated large sums of money to the

Children's Anti-Cancer Fund. In addition, Joe discovered that his email box was filled with angry messages.

Joe immediately contacted CharityBot.com and told them about the disastrous email. A quick internal investigation revealed that the word "lust" had mistakenly been left off of the "words to avoid" list used by E_MAEI_WRITER. In addition, a preliminary investigation by one of CharityBot.com's software engineers revealed the strong possibility that a "bug" in the E_MAEI_WRITER software caused the word "impossible" to be substituted for "possible."

During the next few days, Joe and the Children's Anti-Cancer Fund were named in a dozen lawsuits, and three foreign countries sought to extradite Joe and others in order to try them for extortion and violations of privacy laws. A week later, the Children's Anti-Cancer Fund went out of business.

An Example Case Analysis

1. Take the ethical point of view

To begin an ethical analysis of this imagined case, we should start by "taking the ethical point of view," trying to avoid any bias or prejudice in our judgments and to view all those involved in a fair and even-handed way.

2. Develop a detailed case description

Our case description should "stick to the facts" that are actually mentioned or strongly implied; and we should avoid inserting additional "facts" that could significantly alter ethical judgments. Our description should identify the important participants and their roles in the case. The following description seems appropriate:

Participants and their roles

1 Humans

Joe Biggheart Joe leased EMAILFUNDER from CharityBot.com, created a softbot using EMAILFUNDER, provided a sample email message to the softbot, and placed the softbot onto the Internet. Although he had some concerns about "the quality and appropriateness of email messages written by E_MAEI_WRITER" and about "possible privacy violations associated with personal profiles," he dismissed these worries when the CharityBot.com workshop leaders became annoyed and assured him that his worries were misplaced.

Recipients of the email message A few sent large donations to the Children's Anti-Cancer Fund after receiving the "extortion" message; many recipients sent outraged email to Joe Biggheart; and a few brought a suit against Joe and his charity organization.

Software engineers from CharityBot.com They originally created and tested EMAILFUNDER before it was marketed. Later they discovered that "lust" had mistakenly been left off of the "avoid these words" list used by E_MAEI_WRITER. One software engineer also determined that E_MAEI_WRITER probably had a program "bug" that caused the word "impossible" to be substituted for "possible".

Workshop leaders for CharityBot.com They taught the workshop on using EMAILFUNDER, became annoyed with Joe's worries, and dismissed them as unfounded.

Prosecutors in some foreign countries They attempted to extradite Joe Biggheart and other officers of his charity in order to try them for extortion and privacy violations.

2 Non-Human Agents

E_RESEARCHER This software agent gathered information on the Internet about people who frequently visited pornography web sites.

E_PROFILER This software agent created personal profiles of individuals from data provided by E_RESEARCHER.

E_MAEI_WRITER This software agent created the "extortion" message by substituting the word "lust" for "health," as well as substituting "impossible" for "possible;" then it sent the resulting message to thousands of wealthy men who had frequented pornographic web sites.

3. Try to "see" the ethical issues

Now that we have a case description with which to work, we can use our "ethical eye" to try to spot problems and possible issues. What ethical questions instantly come to mind? What aspects of this case make you feel "uneasy" and or concerned, even if you cannot yet say why?

Ethical Questions

- 1 Joe's softbot created an email message that resulted in serious harm to lots of people. Who is responsible for this situation? Did anyone intentionally cause harm, or was it unintended?

- 2 If the harm was unintended, can anyone be blamed for being negligent or irresponsible? Or was this simply an unfortunate accident that could not have been foreseen or prevented?

Worries

- 1 Joe used a product created by CharityBot.com, and now he faces very serious problems. He was only trying to do good. It doesn't seem fair that Joe should bear all the blame by himself.
- 2 E_RESEARCHER and E_PROFILER, working together, can gather and list all sorts of information about people and their personal lives. This doesn't seem right.
- 3 It doesn't seem right that Joe should have to worry about laws in other countries besides his own.

4. Use your ethical reasoning skills

This is the "step" in which you try to think of precedents and similar situations; try to imagine who might be offended and why; and try to put yourself "in the other person's shoes."

Precedents and similarities At first glance, this looks like a case of extortion and blackmail, because a message was sent that seemed to threaten the recipient if money is not paid. However, there is a very important difference, because we have no reason to believe that E_MAL_WRIER knew what it was writing or was even capable of having intentions at all. And, given the fact that Joe Biggheart was "horrified" by the letter, we have good reason to believe that he did not intend to threaten anyone.

Objectors All those people who were harmed are likely to raise objections, including people who received the "extortionist" email, all those who worked for the Children's Anti-Cancer Fund, children with cancer who were expecting help from the fund, Joe Biggheart, and many family members and friends of all these other objectors. Staff members and owners of CharityBot.com also might face damages. The objectors are likely to express their objections to law enforcement officials, officers of the Children's Anti-Cancer Fund, and managers and owners of CharityBot.com.

Key issues are likely to be (i) whether anyone intentionally caused harm, (ii) whether any laws were broken, (iii) whether anyone was culpably negligent, (iv) whether anyone should be punished and how, and (v) how people can be fairly compensated for their losses.

Standing "in the other person's shoes" Recipients of the softbot's email who never were involved in child pornography or pedophilia, are bound to be furious,

anxious to protect their reputations, and likely to want some compensation for their suffering. Recipients who were involved in child pornography or pedophilia are likely to feel relieved that the email was a mistake and hopeful that they will not be found out because of it. Joe Biggheart is likely to feel betrayed by CharityBot.com, whom he trusted to provide a reliable and safe software product. He may seek to blame everything on CharityBot.com and avoid any blame himself. Supporters of the Children's Anti-Cancer Fund, plus children with cancer and their families are likely to want the good work of the Fund to somehow be continued; and they are likely to ask the government to find a way to prevent such problems in the future.

5. Discuss the case with others

Other people may see the world from a different perspective, and they have had experiences that are different from yours. It is a good idea, therefore, to seek discussions with others about the case. For example, a lawyer or law student might see some legal issues that you overlooked, a computer security expert may offer some helpful suggestions about the risks of using softbots, and a friend who has been involved in a negligence lawsuit might have some helpful insights.

Interim Conclusions

Depending upon needs and circumstances, many case analyses can be concluded at this point by drawing relevant conclusions. For example, we can already draw the following inferences:

Joe Biggheart was trying to do good for children who have cancer, and he did not intend to harm anyone; but Joe had some worries about risks and privacy that he dismissed too easily. He should have followed up on these.

People at CharityBot.com did not take the risks of using softbots seriously enough. The software engineers may not have been concerned enough about such risks, the workshop leaders seem to have dismissed the risks too easily, and the company apparently did not inform its clients about the risks of using their products or similar ones from other companies. These problems may result in lawsuits against CharityBot.com filed by people who were harmed.

Of course, there is much more that could be said, and there are more ideas that can be developed from further analysis.

In addition to making these preliminary ethical judgments, we have hit upon some important *unresolved* computer ethics issues that society will have to face in the future. For example,

Softbots are not ethically aware of what they do, yet they are given the capacity to perform all kinds of "actions". Society needs to figure out how to make softbots behave as if they were ethical agents, even though they aren't. Could there be "ethical rules" for softbots? (See Eichmann 1994) We apparently have identified some important "policy vacuums" here.

When people (and softbots) from one country engage in actions on the Internet, they might be violating laws and rules in many other countries. Since no one can know all the laws and rules of all the countries of the world, how can anyone know whether he or she (or his or her softbot) is acting ethically on the Internet? A large set of "policy vacuums" seems to be lurking here.

For those who wish to pursue the implications of this case further, there are many additional analysis techniques available, and some of these are illustrated below. (Because of space limitations, only a few illustrations are given here. A more complete set of examples can be found on the web sites associated with this textbook (see the Preface above). The most definitive account of case analysis techniques that I know about is Maner's excellent article and associated web site "Heuristic Methods for Computer Ethics" (2002).)

6a. Perform a "professional standards analysis"

It is clear from our interim conclusions that several key ethical questions concern actions of ICT professionals working for CharityBot.com. Because of this, it will be helpful to select a relevant code of ethics and apply appropriate principles to the case. Let us use the Software Engineering Code of Ethics and Professional Practice (see Appendix A1 in Part III below) to analyze the actions of the software engineers who created EMAILFUNDER:

According to principle 1.03 of the Software Engineering Code of Ethics and Professional Practice, software engineers should "approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy, or harm the environment. The ultimate effect of the work should be to the public good." It seems clear from our analysis above that the CharityBot.com software engineers violated this principle by failing to pay sufficient attention to, or ignoring, quality concerns and privacy risks.

According to principle 1.04 of that same code of ethics, software engineers should "disclose to appropriate persons or authorities any actual or potential danger

to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents." If the CharityBot.com software engineers did not know about the risks of using their products, they were negligent; and if they *did* know, they violated this principle by failing to notify their supervisors and clients.

6b. Perform a "roles and responsibilities analysis"

In addition to the software engineers who created EMAILFUNDER, several other people played important roles in this case. These include, for example, chief fundraiser Joe Biggheart and the workshop leaders from CharityBot.com. Let us consider their respective roles and responsibilities:

Joe Biggheart's roles and responsibilities As chief fundraiser for the Children's Anti-Cancer Fund, Joe was responsible for selecting and carrying out fundraising projects that were legal and safe. Given his worries about the appropriateness of software-written email messages, and also about possible privacy violations, he should have been more persistent and investigated these concerns more fully. He dismissed these worries rather too quickly when the workshop leaders became annoyed with him.

Workshop leaders' roles and responsibilities The CharityBot.com workshop leaders were responsible, not only for instruction of clients in the use of company products, they also should have taken more seriously the reliability and privacy questions that Joe raised in the workshop.

An important fact about this case is that *non-human agents* (e.g., E_MAIL_WRITER) were significant "actors" in this situation. They had roles and "responsibilities," but they were not ethical agents who could be held accountable in the usual sense of this term. As indicated above, this raises a number of questions about the "ethics" of software agents.

6c. Perform a "stakeholder analysis"

No one significantly benefited in this case, but a number of people were seriously harmed. These include Joe Biggheart, recipients of the emailed message, children with cancer and their families, staff members and stockholders of CharityBot.com, and staff members of the Children's Anti-Cancer Fund. Let us consider two of these stakeholders here. (A *complete* stakeholder analysis is normally recommended for an in-depth understanding of a case, but space limitations make that impossible here. See the web sites associated with this textbook for a more complete stakeholder analysis.)

Recipients of the message Clearly, recipients of the "extortion" message suffered harm from it. Their privacy was invaded, most were shocked or at least annoyed, and surely some were embarrassed to have their interest in pornography revealed. A few of the recipients felt threatened enough to send large sums of money to the charity, and a number of the recipients were angry enough to initiate lawsuits.

Children with cancer The children who were being helped, or would have been helped, by the Children's Anti-Cancer Fund were among the most seriously harmed. Some will likely find assistance elsewhere, but others may not; and some of the children might actually die from lack of proper medical care.

6d. Perform a "systematic policy analysis"

The above discussion has already identified a variety of "policies to guide one's conduct" which are relevant to this case. These include, for example, international extradition treaties, laws regarding extortion and negligence, and ethical principles included in professional codes of ethics. Let us consider two other types of policies.

International agreements In addition to the extradition treaties mentioned above, there are other relevant international "policies." For example, international privacy agreements, such as the "Safe Harbors Agreement" between the United States and European countries, could help to resolve privacy violation questions about personal profiles created by E_RESEARCHER and E_PROFILER.

Corporate policies Both CharityBot.com and the Children's Anti-Cancer Fund should have had policies in place to deal with privacy and security issues regarding the use of software. Both organizations would have benefited if such issues had been seriously addressed before the disastrous email was sent, and much harm could have been avoided.

6e. Perform an "ethical theory analysis"

Traditional ethical theories of the "great philosophers" can be seen as efforts to understand and systematize many important aspects of ethical practice. (This is similar to the role of "great scientific theories", which attempt to understand and systematize scientific practice.) For this reason, traditional

ethical theories can often shed useful light upon a case that is being analyzed. Consider the following utilitarian, Aristotelian and Kantian points about the present case:

Utilitarian points To behave in an ethical manner, according to the utilitarians, staff members of CharityBot.com, as well as those in the Children's Anti-Cancer Fund (especially Joe Biggheart) should have seriously considered the risks, as well as the possible benefits, of using softbots on the Internet – specifically the risks of using EMAILFUNDER. All of these participants appear to have focused primarily upon the possible profits and benefits, and insufficiently upon the risks. Failure to include a common sex-related word in the list of "words to avoid," as well as the likely existence of a serious software "bug," are indications that the CharityBot.com software engineers were careless. Also, given Joe Biggheart's worries about the appropriateness of software-written email, he should have established a means of checking messages before they were sent. For example, he could have arranged to have each new version of the message sent to his own email and approved by him before his softbot was permitted to send the message to thousands of targeted people.

Aristotelian points Given what has been said above, it is likely that the CharityBot.com software engineers failed to achieve the kind of professional excellence that results from virtues like *reliability*, *responsibility*, and *persistence*. They seem, instead, to have indulged in the vices of *unreliability*, *irresponsibility*, and *lack of persistence*. Joe Biggheart, on the other hand, exhibited virtuous qualities like *generosity* and *compassion*, but he also apparently lacked sufficient *persistence* and *responsibility*. In addition, he should have had the *courage* to pursue his worries in spite of the annoyance they caused to the workshop leaders.

Kantian points Staff members of CharityBot.com appear to have lacked proper respect for their clients and the people who are likely to be affected by their products. They did not take Joe Biggheart's concerns seriously when he expressed doubts about the reliability of software-generated messages or about possible privacy violations. They created and sold software that can be used systematically and effectively to invade people's privacy. They showed more concern for their own profits than for the dignity and worth of their clients and the people affected by their products. Joe Biggheart, on the other hand, did show respect and concern for the children and families served by his charity; although he (perhaps foolishly) trusted the people at CharityBot.com too much; and he allowed his focus upon fundraising and his fear of offending others to overshadow his respect and concern for recipients of his softbot's email.

7. Draw some key ethical conclusions

Given all that has been said above, we are now in a position to draw some conclusions:

- A. The primary cause of the disaster appears to be a number of ethical shortcomings at CharityBot.com. The software engineers, workshop leaders, and others in the company seem more concerned with profits than with the quality of their products and services. They don't have proper respect for their clients or the people affected by their products. They are willing to create and profit from products that seriously invade people's privacy. They appear to have no company policies that demand excellence, reliability, responsibility, and concern for the dignity and worth of persons. They place concern for company profits above the public welfare.
- B. A contributing cause of the disaster appears to be a lack of sufficient care and attention by the staff of the Children's Anti-Cancer Fund. The organization either lacked or failed to enforce policies that demand excellence and responsibility in carrying out one's duties. Joe Biggheart, in particular, even though he obviously cared about children with cancer and their families, appears to have had an attitude that was too casual when dealing with possible risks to the projects for which he was responsible. And he didn't have the courage or integrity to pursue his worries about quality and privacy.

8. Draw some lessons for the future

Items A and B above are the primary ethical conclusions of this case analysis. In addition, there are some lessons that can be learned:

- Privacy will continue to be a major issue in computer ethics. The ease with which softbots on the Internet can gather personal information and assemble it into revealing profiles shows the continuing need for privacy in the information age. (See James Moor, "Towards a Theory of Privacy in the Information Age" in chapter 11 below.)
- As softbots and other software agents become more sophisticated, they are empowered to make more and more "decisions" on their own, and also to perform many more "actions" without consulting their human creators. There seems to be an urgent need for the development of "agent ethics" to help regulate the behavior of computerized agents (See Eichmann 1994).

- Because the Internet is truly global and connects most countries of the world, it has become possible to act "locally" on one's home computer or office computer and nevertheless have a worldwide impact. When a person (or robot) is acting on the Internet, whose laws apply and whose values should be respected? Should everyone in cyberspace be subject to all the laws and rules of all the countries of the world? Could there be such a thing as a "global ethics"? (See Krystyna Gorniak-Kocikowska, "The Computer Revolution and the Problem of Global Ethics" in chapter 15 below.)

References

- Bynum, T. W. and Schubert, P. (1997). "How to Do Computer Ethics: A Case Study – The Electronic Mall Bodensee." In M. J. van den Hoven (ed.), *Computer Ethics: Philosophical Enquiry – Proceedings of CEPE'97*. Erasmus University Press, pp. 85–95 (also available at <http://www.computerethics.org>).
- Eichmann, D. (1994). "Ethical Web Agents." *Proceedings of the Second International World Wide Web Conference: Mosaic and the Web*, Chicago, IL, October 18–20, pp. 3–13. (Accessed on June 29, 2002 at the following web site: <http://archive.ncsa.uiuc.edu/SDG/IT94/Proceedings/Agents/eichmann.ethical/eichmann.html>.)
- Maner, W. (2002). "Heuristic Methods for Computer Ethics". In J. H. Moor and T. W. Bynum (eds.), *Cyberphilosophy: The Intersection of Philosophy and Computing*. Blackwell Publishing (see also <http://csweb.cs.bgsu.edu/maner/heuristics/toc.htm>).
- Moor, J. H. (1985). "What Is Computer Ethics?" In T. W. Bynum (ed.), *Computers and Ethics*. Blackwell Publishing, pp. 266–75. (Published as the October 1985 issue of *Metaphilosophy*.) (Also available at <http://www.computerethics.org>)

Basic study questions

1. What is "pattern recognition" and why does Bynum say that it is much like perception?
2. What does Bynum mean when he says that he wants his case analysis method to be "natural and effective"?
3. While discussing Moor's "What Is Computer Ethics?", Bynum raises four key questions. What are these questions?
4. Why, according to Bynum, are people so sensitive to offending others?
5. What are the different kinds of "policies for conduct" that, according to Bynum, people normally use to make decisions about what they ought to do?
6. What is Aristotle's account of how people develop good ethical judgment?
7. What, according to Bynum, is "the ethical point of view"?
8. According to Bynum, when developing a detailed description of a case, one should avoid inventing "facts not specified or strongly implied." Why?
9. What three strategies, according to Bynum, can help you "tap into your own ethical knowledge and skills"?