

4. *Treat others justly.*

Everyone deserves fair wages and appropriate credit for work performed. Do not discriminate against others for attributes unrelated to the job they do. Do not penalize others for following the Code. (Supports clauses 5.06, 5.07, 5.08, 5.09, 5.10, 5.11, 5.12, 7.03, 7.04, 7.05, 7.07, and 8.07.)

5. *Take responsibility for your actions and inactions.*

As a moral agent, you are responsible for the things you do, both good and bad. You may also be responsible for bad things that you allow to happen through your inaction. (Supports clauses 1.01, 3.04, 3.05, 3.06, 3.07, 3.08, 3.10, 3.11, 3.14, 3.15, 4.02, and 7.08.)

6. *Take responsibility for the actions of those you supervise.*

Managers are responsible for setting up work assignments and training opportunities to promote quality and reduce risk. They should create effective communication channels with subordinates so that they can monitor the work being done and be aware of any quality or risk issues that arise. (Supports clauses 5.01, 5.02, 5.03, and 5.04.)

7. *Maintain your integrity.*

Deliver on your commitments and be loyal to your employer, while obeying the law. Do not ask someone else to do something you would not be willing to do yourself. (Supports clauses 2.01, 2.04, 2.08, 2.09, 3.01, 3.02, 3.09, 4.03, 4.04, 6.06, 6.10, 6.11, 8.08, and 8.09.)

8. *Continually improve your abilities.*

Take advantage of opportunities to improve your software engineering skills and your ability to put the Code to use. (Supports clauses 8.01, 8.02, 8.03, 8.04, 8.05, and 8.06.)

9. *Share your knowledge, expertise, and values.*

Volunteer your time and skills to worthy causes. Help bring others to your level of knowledge about software engineering and professional ethics. (Supports clauses 1.08, 6.01, 6.02, 6.03, 6.04, 7.01, 7.02, and 7.06.)

In the following section, we use these fundamental, discipline-independent principles to facilitate our analysis in four case studies related to computing.

9.5 Case Studies

Throughout this text we have evaluated a wide range of moral problems. Our methodology has been to evaluate the moral problem from the point of view of one or more of these theories: Kantianism, act utilitarianism, rule utilitarianism, social contract theory, and virtue ethics.

Another way to evaluate information technology-related moral problems is to make use of the Software Engineering Code of Ethics and Professional Practice. We follow a three-step process:

1. Consult the list of fundamental principles and identify those that are relevant to the moral problem.
2. Search the list of clauses accompanying each of the relevant fundamental principles to see which speak most directly to the issue.
3. Determine whether the contemplated action aligns with or contradicts the statements in the clauses. If the action is in agreement with all the clauses, that provides strong evidence the action is moral. If the action is in disagreement with all the clauses, it is safe to say the action is immoral.

Usually, the contemplated action is supported by some clauses and opposed by others. When this happens, we must use our judgment to determine which of the clauses are most important before we can reach a conclusion about the morality of the contemplated action.

In the remainder of this section, we apply this methodology to four case studies.

9.5.1 Software Recommendation

SCENARIO

Sam Shaw calls the Department of Computer Science at East Dakota State University seeking advice on how to improve the security of his business's local area network. A secretary in the department routes Mr. Shaw's call to Professor Jane Smith, an internationally recognized expert in the field. Professor Smith answers several questions posed by Mr. Shaw regarding network security. When Mr. Shaw asks Professor Smith to recommend a software package to identify security problems, Professor Smith tells him that NetCheks got the personal computer magazine's top rating. She does not mention that the same magazine gave a "best buy" rating to another product with fewer features but a much lower price. She also fails to mention that NetCheks is a product of a spin-off company started by one of her former students and that she owns 10 percent of the company.

Analysis

From our list of nine fundamental principles, three are most relevant here:

- Be impartial.
- Disclose information that others ought to know.
- Share your knowledge, expertise, and values.

Searching the list of clauses identified with these fundamental principles, the following ones seem to fit the case study most closely:

- *1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.*
Professor Smith was deceptive when she mentioned the most highly rated software package but not the one rated to be a "best buy."
- *1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.*

9.5.2 Chil

SCEN

Anal

Lo

re

- 4.05. *Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.*
- 6.02. *Promote public knowledge of software engineering.*
Professor Smith freely provided Sam Shaw with valuable information about network security.
- 6.05. *Not promote their own interest at the expense of the profession, client or employer.*
Professor Smith did not tell Sam Shaw that she had a personal stake in the success of the NetCheks software. She did not tell him about the “best buy” package that may have provided him every feature he needed at a much lower price.

Mr. Shaw was asking Professor Smith for free advice, and she provided it. When she freely shared her knowledge about network security, she was acting in the spirit of clauses 1.08 and 6.02, and doing a good thing.

However, Professor Smith appears to have violated the other three clauses, at least to some degree. Most important, she did not reveal her personal interest in NetCheks, which could lead her to be biased. The fact that she did not mention the “best buy” package is evidence that she was neither evenhanded nor completely forthcoming when she answered Mr. Shaw’s question about software packages.

Perhaps Mr. Shaw should have heeded the maxim, “Free advice is worth what you pay for it.” Nevertheless, the ignorance or foolishness of one person does not excuse the bad behavior of another. Professor Smith should have revealed her conflict of interest. At that point Mr. Shaw could have chosen to get another opinion if he so desired. ~

9.5.2 Child Pornography

~ SCENARIO

Joe Green, a system administrator for a large corporation, is installing a new software package on the PC used by employee Chuck Dennis. The company has not authorized Joe to read other people’s emails, Web logs, or personal files. However, in the course of installing the software, he accidentally comes across directories containing files with suspicious-looking names. He opens a few of the files and discovers they contain child pornography. Joe believes possessing such images is against federal law. What should he do?

Analysis

Looking over the list of nine fundamental principles, we find these to be most relevant to our scenario:

- Be impartial.
- Respect the rights of others.
- Treat others justly.
- Maintain your integrity.

We examine the list of clauses associated with these four fundamental principles and identify those that are most relevant:

- 2.03. *Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.*
Somebody has misused the company's PC by using it to store images of child pornography. By this principle Joe has an obligation to report what he discovered.
- 2.09. *Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.*
While revealing the existence of the child pornography may harm the employee, possessing child pornography is illegal. Applying this principle would lead Joe to disclose what he discovered.
- 3.13. *Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.*
Joe discovered the child pornography by violating the company's policy against examining files on personal computers used by employees.
- 5.10. *Provide for due process in hearing charges of violation of an employer's policy or of this Code.*
Simply because Chuck had these files on his computer does not necessarily mean he is guilty. Perhaps someone else broke into Chuck's computer and stored the images there.

Our analysis is more complicated because Joe violated company policy to uncover the child pornography on Chuck's PC. Once he has this knowledge, however, the remaining principles guide Joe to reveal what he has discovered to the relevant authorities within the corporation, even though management may punish Joe for breaking the privacy policy. There is the possibility that Chuck is a victim. Someone else may be trying to frame Chuck or use his computer as a safe stash for their collection of images. Joe should be discreet until a complete investigation is completed and Chuck has had the opportunity to defend himself.

9.5.3 Antiworm

SCENARIO

The Internet is plagued by a new worm that infects PCs by exploiting a security hole in a popular operating system. Tim Smart creates an antiworm that exploits the same security hole to spread from PC to PC. When Tim's antiworm gets into a PC, it automatically downloads a software patch that plugs the security hole. In other words, it fixes the PC so that it is no longer vulnerable to attacks via that security hole [4].

Tim releases the antiworm, taking precautions to ensure that it cannot be traced back to him. The antiworm quickly spreads throughout the Internet, consuming large amounts of network bandwidth and entering millions of

computers. To system administrators, it looks just like another worm, and they battle its spread the same way they fight all other worms [5].

Analysis

These fundamental principles are most relevant to the antiworm scenario:

- Continually improve your abilities.
- Share your knowledge, expertise, and values.
- Respect the rights of others.
- Take responsibility for your actions and inactions.

Examining the list of clauses associated with each of these fundamental principles reveals those that are most relevant to our case study:

- *1.01. Accept full responsibility for their own work.*
Tim tried to prevent others from discovering that he was the author of the antiworm. He did not accept responsibility for what he had done.
- *1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.*
The antiworm did something good by patching security holes in PCs. Tim provided the antiworm to the Internet community without charge. However, system administrators spent a lot of time trying to halt the spread of the antiworm, a harmful effect.
- *2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.*
Tim's "client" is the community of Internet PC owners who happen to use the operating system with the security hole. While his antiworm was designed to benefit them, it entered their systems without their knowledge or consent. The antiworm also consumed a great deal of network bandwidth without the consent of the relevant telecommunications companies.
- *8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance, and testing of software and related documents, together with the management of the development process.*
- *8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.*
- *8.06. Improve their knowledge of this Code, its interpretations and its application to their work.*
Tim followed the letter of the first two of these three clauses when he acquired a copy of the worm, figured out how it worked, and created a reliable antiworm in a short period of time. The experience improved his knowledge and skills. Perhaps he should invest some time improving his ability to interpret and use the Code of Ethics!


According to some of these principles, Tim did the right thing. According to others, Tim was wrong to release the antiworm. How do we resolve this dilemma? We can simplify our analysis by deciding that Tim's welfare is less

important than the public good. Using this logic, we no longer consider the fact that Tim improved his technical knowledge and skills by developing and releasing the antiworm.

That leaves us with three clauses remaining (1.01, 1.08, and 2.03). From the point of view of clause 1.01, what Tim did was wrong. By attempting to hide his identity, Tim refused to accept responsibility for launching the antiworm. He has clearly violated the Code of Ethics in this regard.

When we evaluate Tim's action from the point of view of clause 1.08, we must determine whether his efforts were directed to a "good cause." Certainly, Tim's antiworm benefited the PCs it infected by removing a security vulnerability. However, it harmed the Internet by consuming large amounts of bandwidth, and it harmed system administrators who spent time battling it. Because there were harmful as well as beneficial consequences, we cannot say that Tim's efforts were directed to a completely good cause.

Finally, let's evaluate Tim's action from the point of view of clause 2.03. Even though the antiworm was completely benevolent, Tim violated the property rights of the PC owners, because the antiworm infected their PCs without authorization. Hence Tim's release of the antiworm was wrong from the point of view of this clause.

To summarize our analysis, Tim's release of the antiworm is clearly wrong from the point of view of clauses 1.01 and 2.03. It is also hard to argue that he satisfied the spirit of clause 1.08. We conclude that Tim's action violated the Software Engineering Code of Ethics and Professional Practice. 

9.5.4 Consulting Opportunity

SCENARIO

Acme Corporation licenses a sophisticated software package to many state, county, and city governments. Government agencies have the choice of three levels of service: the bronze level provides online support only; the silver level adds phone support; and the gold level includes training classes taught on the customer's site. The gold level of support costs \$20,000 a year more than the silver level.

Jean is one of the Acme employees who works in the support organization. Mostly, Jean provides phone support, but from time to time he teaches an on-site class. In fact, Jean created many of the instructional materials used in these classes. Because of the recession, quite a few government agencies have dropped from the gold level of support to the silver level, and some members of Jean's training group have lost their jobs. Jean has a family to support, and he is wondering if his position will soon be eliminated as well.

The state government of East Dakota is one of the many customers that no longer pays Acme Corporation for on-site training. One day Jean gets a call from Maria, who works for the East Dakota state agency using the software package. Maria offers to pay Jean \$5,000 plus expenses to run a five-day training class that covers the same material as the official course taught by Acme.

Jean accepts the offer, but he does not inform anyone at Acme Corporation of his decision. Working at home on evenings and weekends, he develops his own set of instructional materials. He takes a week of paid vacation from work, travels to East Dakota, and teaches the class.

Analysis

From our list of fundamental principles, quite a few are relevant here:

- Be impartial.
- Take responsibility for your actions and inactions.
- Disclose information that others ought to know.
- Maintain your integrity.
- Continually improve your abilities.

Examining the clauses associated with each of these fundamental principles, the ones that most closely fit this case study are as follows:


- *2.08 Accept no outside work detrimental to the work they perform for their primary employer.*
Employers provide employees with weekends off and paid vacations so that they can rest from their labors and return to work refreshed and able to perform at a high level. You could argue that Jean's consulting work was detrimental to his "day job" at Acme Corporation because it filled his evenings and weekends and kept him from getting a proper vacation.
- *3.04 Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.*
Based on his prior experience at Acme, Jean was certainly well qualified to develop the instructional materials and teach the class in East Dakota. He has fulfilled this obligation of the Code.
- *4.05 Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.*
By accepting the consulting job with the East Dakota state government, Jean created a conflict of interest between himself and Acme Corporation. Namely, it is in Jean's interest if East Dakota does not purchase the gold level of support, but it is in Acme Corporation's interest if East Dakota does buy the gold level of support. Jean violated this clause by not disclosing his consulting job to Acme Corporation.
- *6.05 Not promote their own interest at the expense of the profession, client or employer.*
By agreeing to teach the class in East Dakota, Jean put his own interest above that of his employer. Clearly, the East Dakota state government recognized a need to have some on-site training. If Jean did not accept the consulting job, the East Dakota government may have gone back to the gold level of support from Acme.

- 8.04 *Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.*
By creating his own set of instructional materials, Jean probably developed an even better understanding of the software package and its capabilities. There is a good chance he came up with some insights about better ways to teach others how to use the software. This additional knowledge will make Jean a more valuable employee of Acme Corporation.

You could argue that Jean is actually helping Acme Corporation. Governments are dropping the gold level of support because it is simply too expensive, but phone support and online support aren't enough. If these agencies cannot find another source of on-site training, they may stop using Acme's software altogether. By providing East Dakota with affordable on-site training, Jean was helping ensure that East Dakota would remain a customer of Acme Corporation, albeit at the silver level.

You could also argue that Jean's work for East Dakota improved his knowledge of the software package and his ability to teach others how to use it, making him a more effective phone support person at Acme.

However, it's unlikely upper management at Acme Corporation will be convinced by these arguments, particularly since Jean did not disclose the offer from East Dakota before accepting it. Jean's decision is much more likely to cause management to question his loyalty to his company and his fellow employees. If the company learns about his consulting work, Jean may well be the next person laid off.

To conclude our analysis, Jean's actions were wrong and unwise. He violated clauses 2.08, 4.05, and 6.05 of the Software Engineering Code of Ethics and Professional Practice, and he may have put his full-time job in jeopardy. 

9.6 Whistle-Blowing

All four case studies presented in the previous section involve the actions of a single individual. It is easy for us to assign moral responsibility to that person and to discuss how things might have turned out better if he or she had acted differently. Often, however, a product or decision is the cumulative result of the work of many people within a larger organization. Suppose somebody within the organization perceives a danger to the public but is unable to persuade the rest of the organization to make needed changes to eliminate that danger. Should that person go outside the organization with the information?

A **whistle-blower** is someone who breaks ranks with an organization in order to make an unauthorized disclosure of information about a harmful situation after attempts to report the concerns through authorized organizational channels have been ignored or rebuffed [6]. Sometimes employees become whistle-blowers out of fear that actions taken by their employer may harm the public; other times they have identified fraudulent use of tax dollars [7].

9.6.1 M

Fr
civ

Or
bo
to
ro
(Fi

rec
nec
evi
ing
wer
for
shu
red

disc
unu