Dependable Systems
dcms.cs.uni-saarland.de/ethics_21/
Sarah Sterz, Kevin Baum, Prof. Holger Hermanns

Training Exercises E6 (Codes of Ethics)

with Example Solutions

With Solutions

Issue 1: ***Get familiar with different CoEs***

Read all of the following Codes of Ethics thoroughly:

- Ethical Guidelines of the German Informatics Society (`https://gi.de/ethicalguidelines/` (English) or `https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien/` (German))
- ACM Code of Ethics and Professional Conduct (`https://ethics.acm.org/`)
- IEEE-CS/ACM Software Engineering Code of Ethics (`https://www.computer.org/web/education/code-of-ethics`)
- IEEE Code of Ethics (`https://www.ieee.org/about/corporate/governance/p7-8.html`)
- Ten Commandments of Computer Ethics (`http://computerethicsinstitute.org/publications/tencommandments.html`)
- CCC Hacker Ethics (`https://www.ccc.de/en/hackerethics`)

Then answer the following questions:

(a) In what aspects to the codes differ?

(b) How relevant and useful do you think they are?

Case Studies from Gotterbarn and Miller

All of the case studies and the parts of their suggested solution that are concerned with the ACM Code of Ethics in this section are direct quotes from

> Gotterbarn, D., & Miller, K. W. (2004). Computer ethics in the undergraduate curriculum: Case studies and the joint software engineer's code. Journal of Computing Sciences in Colleges, 20(2), 156-167.

What do different codes of ethics tell you about how to decide in these cases? You do not have to apply every code to every case, but you should use every code at least once.

Issue 2: *Acme Software Company*

George Babbage is an experienced software developer working for Acme Software Company. Mr. Babbage is now working on a project for the U.S. Department of Defense, testing the software used in controlling an experimental jet fighter. George is the quality control manager for the software. Early simulation testing revealed that, under certain conditions, instabilities would arise that could cause the plane to crash. The software was patched to eliminate the specific problems uncovered by the tests. After these repairs, the software passed all the simulation tests. George is not convinced that the software is safe. He is worried that the problems uncovered by the simulation testing were symptomatic of a design flaw that could only be eliminated by an extensive redesign of the software. He is convinced that the patch that was applied to remedy the specific tests in the simulation did not address the underlying problem. But, when George brings his concerns to his superiors, they assure him that the problem has been resolved. They further inform George that any major redesign effort would introduce unacceptable delays, resulting in costly penalties to the company. There is a great deal of pressure on George to sign off on the system and to allow it to be flight tested. It has even been hinted that, if he persists in delaying the system, he will be fired. What should George do next?

Sketch of a Solution 2:

ACM Code of Ethics In this case, Carl Babbage must contend with issues of physical safety that is dependent on software reliability. If we look at this case too narrowly, we might think that the safety of the test pilot is the exclusive safety concern. Although Mr. Babbage does have responsibilities towards the pilot, test pilots know about the risks inherent in their profession, and the test pilot may be quite willing to fly the plane despite Babbage's misgivings. However, the test pilot is not the only one endangered if the software is faulty; anyone under the plane is endangered if things go awry. Especially if the test flight might fly over populated areas (and remember that instability might lead the plane in unplanned directions before crashing), many people under the plane are unlikely to have given their consent to "testing" the software. Carl's responsibilities to those people are a vital part of our analysis. Clause 1.03 makes public safety a priority concern for a software engineer. It is exactly this concern that is central to George's decision. George clearly recognizes this obligation, and the obligation in clause 1.04 to disclose his professional opinion that the software has not been sufficiently certified as safe. Unfortunately, George's superiors have not supported his decision about the software, and are trying to convince him to sign off on the software despite his reservations. His superiors have put George in a difficult position. Clearly, the Code sections above confirm Mr. Babbage's ethical duty to refuse to sign off on the software before he is reasonably sure of its safety. (We note that for almost all complex software, we can never be entirely sure software is reliable and safe. It is a professional judgment whether or not the software is "safe enough." [8]) By pressuring George to sign off, his superiors are forcing George to choose between his loyalty to his employers (and his continued employment) and his obligation to public safety. As McFarland points out, this is an untenable position. [7] It is hoped that the existence of, and support for, an effective ethics code can help someone in this position; but it is still difficult.

So far our analysis has concentrated on Mr. Babbage and his dilemma. But the Joint Code also requires his managers to act ethically. The clauses in section 5 of the Code prohibit managers from forcing

a software engineering employee to violate the code. The Code also makes managers responsible for ensuring that there are processes to ensure the reduction of risks. The managers might object that they have adequate processes, and that the process was followed. Simulation testing revealed problems, and those problems were addressed. The managers are not convinced that Mr. Babbage's suspicions are well founded, and are not willing to jeopardize the project based on his misgivings. The wording of clause 1.03 in the Code is an important part of our analysis of this case. That clause states that software engineers should approve software only if they have a "well-founded belief that it is safe" (our emphasis). The idea of a well-founded belief is key to the dispute between George and his superiors. Perhaps George is right about the software, but perhaps his managers are right. Although the case does not offer many details about George's misgivings, he apparently did not present sufficient evidence to his superiors about the remaining problems in the software. (If the managers were convinced about the seriousness of the remaining problems, it seems unlikely that they would approve a test flight that would likely end in a costly disaster.) Perhaps this dilemma could be resolved to the satisfaction of all parties if the managers agreed to a short term delay not for a major redesign, but for further testing to either confirm George's suspicions, or convince George that the managers are correct, and that the test flight should go on. This resolution would be far better than George signing off on a system he thinks is deficient, and far better than George being fired for not doing so. The standard supported by the Code is to have the burden to demonstrate that the software is safe before deployment instead of having to prove it unsafe before deployment is halted.

Ethical Guidelines of the German Informatics Society To decide what George should do next the following two sections of the "Ethical Guidelines of the German Informatics Society" seem to be most decisive:

Section 4: Powers of Discernment GI members sharpen their powers of discernment to render themselves better equipped to contribute to design processes with individual and collective accountability. This presupposes not only a willingness to call into question and to make judgments about individual and collective actions in public discourse, but also the ability to acknowledge the limits of one's own powers of discernment.

Section 9: Courage of Convictions GI members staunchly advocate for the protection and safeguarding of human dignity, even when this is not explicitly mandated by laws, contracts or other norms, or when these stand in direct opposition to the protection and safeguarding of human dignity. This applies even in situations in which GI members' obligations to clients conflict with their responsibility to third-party stakeholders.

Section 4 draws George's attention to the fact that he first has to check in great detail whether he has the technical competence to be able to assess that a danger emanates from the system if it is not fundamentally optimised. He has the opinion that the system should not be used in its current form because it is not safe. If George comes to the result that he has the required technical competence, then he is obliged by Section 9 not to allow the system for a test flight until it has been thoroughly revised. This also applies if this results in financial losses for the company or if he loses his job.

IEEE-CS/ACM Software Engineering Code of Ethics To decide what George should do next the following three principles of the IEEE-CS/ACM Software Engineering Code of Ethics seem to be most decisive:

1. PUBLIC – Software engineers shall act consistently with the public interest.

4. JUDGMENT – Software engineers shall maintain integrity and independence in their professional judgment.

5. MANAGEMENT – Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.

The reasoning here works almost analogously to that concerning the Ethical Guidelines of the German Informatics Society. According to the 4th principle George has to check his professional competence and then make a decision with integrity. George's assessment is that the system is not safe and poses a danger to the pilot and others involved. Since he has committed himself to ethical compliance through Principle 5, he may not agree to the introduction of the system – without revision.

Ten Commandments of Computer Ethics We could employ commandment 9 "Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.", though it is not really clear whether those consequences count as social consequences. One could also employ commandment 10 "Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans. " here to argue that George should insist that the system should be redesigned. A fault in the system can lead to disastrous consequences of not only the pilot dying but also the people at the place where the plane crashes (if there are such people). Furthermore, this also hold even if he loses his job, because judging his job to be more important than the lives of other humans does not respect those humans.

Issue 3: ***Database: Levels of Security***

Leikessa Jones owns her own consulting business, and has several people working for her. Leikessa is currently designing a database management system for the personnel office of ToyTimeInc., a mid-sized company that makes toys. Leikessa has involved ToyTimeInc management in the design process from the start of the project. It is now time to decide about the kind and degree of security to build into the system. Leikessa has described several options to the client. The client has decided to opt for the least secure system because the system is going to cost more than was initially planned, and the least secure option is the cheapest security option. Leikessa knows that the database includes sensitive information, such as performance evaluations, medical records, and salaries. With weak security, she fears that enterprising ToyTimeInc employees will be able to easily access this sensitive data. Furthermore, she fears that the system will be an easy target for external hackers. Leikessa feels strongly that the system should be more secure than it would be if the least secure option is selected. Ms. Jones has tried to explain the risks to ToyTimeInc, but the CEO, the CIO, and the Director of Personnel are all convinced that the cheapest security is what they want. Should Jones refuse to build the system with the least secure option?

Sketch of a Solution 3:

ACM Code of Ethics Ms. Jones has competing duties to the people who hired her, the people who work at the company, to her consulting firm (including the people who work for her) and to herself. The Joint Code makes it clear that Ms. Jones must be careful about the issue of privacy; as a steward of sensitive data, she should not lose sight of that responsibility. In our first case, Carl Babbage was most concerned with avoiding physical harm to people; Ms. Jones is concerned with a different kind of harm. Both kinds are important. At the same time, Ms. Jones needs to balance the need for security

with the economic interests of the company that hired her to do this work. Professionals have to make subjective judgments to balance cost and the customer's needs; there cannot be perfect security, and there are never infinite resources. This tension between finite resources and attaining the highest quality policy is a common cause for ethical conflicts.

However, in this case Ms. Jones made a mistake by offering a security "option" to the company that, apparently on later reflection, she thought was inadequate. By not informing the company up front about the necessity and cost for adequate security, she has created a difficult situation, both for ToyTimeInc and for herself. In order to fulfill her obligation to the company employees, she must admit her mistake and remove that insecure system as a viable option, insisting on better security. Although the employees of ToyTimeInc haven't been consulted (at least according to this short description), they clearly will be affected by the decisions ToyTimeInc and Jones make. One possible objection to Ms. Jones not mentioning the low-security option is that she wouldn't be allowing ToyTimeInc to make an informed decision. But according to the Code, Ms. Jones is responsible for building systems that are beneficial to the public. If the low security system isn't good enough, then she shouldn't pretend that it is. An engineer designing a bridge should not be compelled to include the possibility of building it with shoddy materials in cost estimates. If the company refuses to upgrade the security, Ms. Jones should probably remove herself from the project if staying in the project will force her to deliver a system she thinks is unethically insecure. (Clause 1.01 is central here.) There are two objections to this suggestion. First, the company will have to find someone else to do the work, and this seems unfair to the company since they were (we assume in good faith) simply agreeing with one of Ms. Jones' suggestions. While this is unfortunate for the company and for Ms. Jones, Ms. Jones' duty to protect sensitive information to a reasonable level of security cannot be brushed aside. A second objection is that if Ms. Jones leaves the project, the company is likely to hire someone else (who perhaps has less ethical scruples) to deliver the job with the unacceptable level of security. Although that may be true, that possible outcome does not absolve Ms. Jones of her responsibility to be an ethical professional. Ms. Jones is first and foremost responsible for her own actions; the next professional hired to take her place will have to wrestle with these responsibilities, but Ms. Jones cannot let that possibility tempt her to dodge her own responsibilities. There is another effect if Ms. Jones delivers the less secure system. She will have harmed the profession of software engineering by allowing a degradation of the standards for quality software. Such acts will, one software engineer at a time, reduce society's trust in software engineering as a whole. If ToyTimeInc insists on building the system with inadequate security, Clause 2.05 becomes important. That clause requires Ms. Jones to keep information confidential, where such confidentiality is consistent with the public interest (our emphasis). If she thinks the security is sufficiently bad, her obligation to the employees of ToyTimeInc (see clause 1.04) will take priority of the obligation for confidentiality in clause 2.05. Another possible solution for Jones is for her to tell ToyTimeInc that she and her consulting company will build in better security, but only charge ToyTimeInc for the cheaper option. This will hurt her financially, and may adversely affect her employees. But since Jones made the mistake of offering inadequate security is an "option," she may decide it is best for her professional reputation (and the long term success of her consulting firm) for her to absorb this loss. This option clearly fulfills her obligation to ToyTimeInc employees, although it is less clear that she has been fair to her own employees who may be harmed by the decision if her company loses money on the ToyTimeInc contract.

Ethical Guidelines of the German Informatics Society To decide whether Jones should refuse to build the system with the least secure option the following section of the "Ethical Guidelines of the German Informatics Society" seems to be most decisive:

Section 9: Courage of Convictions GI members staunchly advocate for the protection and safeguarding of human dignity, even when this is not explicitly mandated by laws, contracts or other norms, or when these stand in direct opposition to the protection and safeguarding of human dignity. This applies even

in situations in which GI members' obligations to clients conflict with their responsibility to third-party stakeholders.

In this case, according to Section 9, Ms. Jones should clearly refuse to implement the system with the weakest security tool. Since she is aware that customer data can be misused in this way and only financial interests, in particular those of ToyTimeInc, speak in favour of such an introduction.

IEEE Code of Ethics The first paragraph "to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, and to disclose promptly factors that might endanger the public or the environment;" and paragraph 9 "to avoid injuring others, their property, reputation, or employment by false or malicious action; " can be employed here to judge that Leikessa should refuse to build the system. Employing the system, arguably, can harm the customers' safety, welfare, property or reputation when their data get hacked.

Ten Commandments of Computer Ethics We can easily employ commandment 9 "Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing." here to argue that Leikessa should refuse to build the system with the least secure option. With a low security, the system could harm the customers of ToyTimeInc because their data could be hacked.

CCC Hacker Ethics A plausibly relevant principle is: "Make public data available, protect private data." Building the system would not protect the employees' private data. Consequently, Leikassa should not build it.

Issue 4: ***Conflicts of Interest***

Juan Rodriguez is a private consultant who advises small businesses about their computer needs. Juan examines a company's operations, evaluates their automation needs, and recommends hardware and software to meet those needs. Recently, Juan was hired by a small, private hospital interested in upgrading their system for patient records and accounting. The hospital had already solicited proposals for upgrading the system, and hired Juan to evaluate the proposals they'd received. Juan carefully examined the proposals on the basis of the systems proposed, the experience of the companies that bid, and the costs and benefits of each proposal. He concluded that Tri-Star Systems had proposed the best system for the hospital, and he recommended that the hospital should buy the Tri-Star system. He included a detailed explanation for why he thought the Tri-Star bid was the best. Juan did not reveal to the hospital that he is a silent partner (a co-owner) in Tri-Star Systems. Was Juan's behavior unethical? We will assume for our discussion that Juan evaluated the bids in good faith, and sincerely believed that Tri-Star had given the best bid.

Sketch of a Solution 4:

ACM Code of Ethics Not all case studies require sophisticated analysis; clause 4.05 clearly labels Mr. Rodriguez's actions as wrong. Mr. Rodriguez did not fulfill his professional obligations when he

neglected to disclose his conflict of interest to the hospital. Notice that his sincerity about the superiority of the Tri-Star bid is not a central issue here. The central issue is the trust Tri-Star has invested in Juan. If Mr. Rodriguez had disclosed his part ownership in Tri-Star to the hospital, and the hospital had still hired him to evaluate the bids, then Juan could have attempted to do a professional job of evaluation. (Some people might find that difficult, but it is at least theoretically possible.) However, the Code clearly prohibits Juan from taking this job without first giving the hospital the opportunity to judge for itself whether or not they wanted to hire Mr. Rodriguez despite his interest in Tri-Star.

IEEE-CS/ACM Software Engineering Code of Ethics To decide whether Juan's behavior was unethical the following two principles of the IEEE-CS/ACM Software Engineering Code of Ethics seem to be most decisive:

2. CLIENT AND EMPLOYER – Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.

6. PROFESSION – Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.

With regard to the second principle, Juan is clearly acting in the interest of his clients and himself – his employer – and is not contradicting any public interests. The important thing here is that he does not put his own interests before the interests of his clients, which he does not do. In addition, Juan promotes the integrity of his profession by providing the hospital with the best possible offer, in good conscience. Accordingly, he does not act unethically.

IEEE Code of Ethics Although Juan complies with paragraph 3 "to be honest and realistic in stating claims or estimates based on available data;" because he really believes Tri-Strar to be the best option, he does not comply to paragraph 1 "to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;", because he does not disclose his conflict of interest. Therefore, his behaviour is unethical.

Ten Commandments of Computer Ethics There are no commandments that declare Juan's behaviour as unethical. He neither does harm (commandment 1), nor does he steal (commandment 4) nor does he do anything else forbidden by one of the commandments. So, his behaviour is not unethical.

Issue 5: ***Want more?***

If you want more case studies, take a look at the ACM-website, where you can find many interesting cases: `https://ethics.acm.org/code-of-ethics/using-the-code/`