Lecture Overview

- ACM Software engineering code of ethics
- Analysis of the code
- Case studies
- A Few Other Codes

Preamble of the Code

Computing professionals’ actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good. The ACM Code of Ethics and Professional Conduct (“the Code”) expresses the conscience of the profession. The Code is designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. Additionally, the Code serves as a basis for remediation when violations occur. The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration. Each principle is supplemented by guidelines, which provide explanations to assist computing professionals in understanding and applying the principle.

Preamble of the Code

Section 1 outlines fundamental ethical principles that form the basis for the remainder of the Code. Section 2 addresses additional, more specific considerations of professional responsibility. Section 3 guides individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM member, and principles involving compliance with the Code are given in Section 4. The Code as a whole is concerned with how fundamental ethical principles apply to a computing professional’s conduct.

Preamble of the Code

The Code is not an algorithm for solving ethical problems; rather it serves as a basis for ethical decision-making. When thinking through a particular issue, a computing professional may find that multiple principles should be taken into account, and that different principles will have different relevance to the issue. Questions related to these kinds of issues can best be answered by thoughtful consideration of the fundamental ethical principles, understanding that the public good is the paramount consideration. The entire computing profession benefits when the ethical decision-making process is accountable to and transparent to all stakeholders. Open discussions about ethical issues promote this accountability and transparency.

General Ethical Principles

1.0 GENERAL ETHICAL PRINCIPLES
- 1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
- 1.2 Avoid harm.
- 1.3 Be honest and trustworthy.
- 1.4 Be fair and take action not to discriminate.
- 1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
- 1.6 Respect privacy.
- 1.7 Honor confidentiality.

Professional Responsibilities

2.1 Strive to achieve high quality in both the processes and products of professional work.
2.2 Maintain high standards of professional competence, conduct, and ethical practice.
2.3 Know and respect existing rules pertaining to professional work.
2.4 Accept and provide appropriate professional review.
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
Professional Responsibilities

2.6 Perform work only in areas of competence.
2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.
2.8 Access computing and communication resources only when authorized or when compelled by the public good.
2.9 Design and implement systems that are robustly and usably secure.

Professional Leadership Principles

3.1 Ensure that the public good is the central concern during all professional computing work.
3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.
3.3 Manage personnel and resources to enhance the quality of working life.
3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.
3.5 Create opportunities for members of the organization or group to grow as professionals.

Professional Leadership Principles

3.6 Use care when modifying or retiring systems.
3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.

4. Compliance with the code

4.1 Uphold, promote, and respect the principles of the Code.
4.2 Treat violations of the Code as inconsistent with membership in the ACM.
4.3 Remain objective when evaluating software or related documents
4.4 Do not engage in deceptive financial practices
4.5 Disclose conflicts of interest
4.6 Do not participate in decisions in which you, your employer, or your client has a potential conflict of interest

Analysis of Preamble

- No mechanical process for determining if an action is right or wrong
- Should not take an overly legalistic view of the Code
  - If Code doesn’t forbid something, that doesn’t mean it is morally acceptable
  - Judgment required
- Code reflects principles drawn from multiple ethical theories

Origin of Virtue Ethics

- Aristotle
  - Happiness results from living a life of virtue
  - Intellectual virtue: developed through education
  - Moral virtue: developed by repeating appropriate acts
  - Deriving pleasure from a virtuous act is a sign that the virtue has been acquired
- Some virtues: Benevolence, courage, fairness, generosity, honesty, loyalty, patience, tolerance
- A person of strong moral character
  - possesses many virtues
  - knows right thing to do in each situation
**Strengths of Virtue Ethics**

- Provides a motivation for good behavior
- Provides a solution to the problem of impartiality
  - Some virtues are partial (e.g., generosity)
  - Other virtues must be impartial (e.g., honesty)

**Virtue Ethics Complements Other Theories**

- Virtue ethics may not work as a stand-alone theory
- It may be a good complement to utilitarianism
- Allows rationale for action to be considered
- Solves problem of moral luck that plagued act utilitarianism

**Alternative, Discipline-Independent List of Fundamental Principles**

- Be impartial.
- Disclose information that others ought to know.
- Respect the rights of others.
- Treat others justly.
- Take responsibility for your actions and inactions.
- Take responsibility for the actions of those you supervise.
- Maintain your integrity.
- Continually improve your abilities.
- Share your knowledge, expertise, and values.

**Case: Malware**

Rogue Services advertised its web hosting services as “cheap, guaranteed uptime, no matter what.” While some of Rogue’s clients were independent web-based retailers, the majority were focused on malware and spam. Several botnets used Rogue’s reliability guarantees to protect their command-and-control servers from take-down attempts. Spam and other fraudulent services leveraged Rogue for continuous delivery. Corrupted advertisements often linked to code hosted on Rogue exploiting browser vulnerabilities to infect machines with ransomware.

**Analysis**

Consider: In deciding whether to proceed with the attack, the security response team needs to consider the impact on stakeholders that include Rogue’s clients, those affected by the malware hosted on Rogue’s systems, and others who rely on the services of Rogue’s non-malicious clients. While the worm is intended to disrupt the malware hosting, it could disrupt the operation of non-malicious clients or escape Rogue’s network, spreading to other ISPs. The worm could also prove to be ineffective and fail to achieve its aim, though alerting Rogue’s malicious clients in the process. More information about Rogue’s non-malicious clients would be beneficial, particularly whether they understood the nature of and risks caused by Rogue’s malicious clients.
**Analysis**

Analyze: Allowing Rogue’s malicious clients’ service to continue impacts the rights of individuals they harm, whereas Rogue’s retailer clients have rights relating to the integrity and preservation of their data and business. Furthermore, Rogue’s clients should have had transparent information of the risks associated with their business model. The most relevant portions of the Code are Principles 1.2 and 2.8, as the worm authors must consider whether the intentional harm to Rogue’s systems is justified to support the public good.

**Analysis**

Review: Rogue’s policy of non-interference with their clients, coupled with their refusal to cooperate with takedown requests, shaped the choices of the security response team. Cooperation by Rogue or a more robust legal framework by their host country would have provided more options for a resolution that did not risk such harm.

**Analysis**

Evaluate: This case highlights a key nuance of Principle 1.2. Given that the worm was designed with the specific intent of causing harm to Rogue’s systems, the authors are obligated to ensure the harm is ethically justified. As the worm aims to shut down web services that are clearly harmful and malicious, the intent of the worm is consistent with the moral obligations identified in Principle 1.1. Additionally, the Code obligates the authors to minimize unintended harm by limiting the worm’s effects solely to Rogue’s systems. Rogue’s other (non-malicious) Malware Disruption Rogue Services advertised its web hosting services as “cheap, guaranteed uptime, no matter what.” While some of Rogue’s clients were independent web-based retailers, the majority were focused on malware and spam. Several botnets used Rogue’s reliability guarantees to protect their command-and-control servers from take-down attempts. Spam and other fraudulent services leveraged Rogue for continuous delivery. Corrupted advertisements often linked to code hosted on Rogue exploiting browser vulnerabilities to infect machines with ransomware. Clients could rightfully object if their data is harmed, so the worm should include additional precautions to avoid this unintentional harm.

**Analysis**

The worm also highlights the guidance in Principle 2.8. The worm will clearly access Rogue’s systems in ways that are not authorized—destroying data in the process—but targeting known malicious software demonstrates a compelling belief that the service disruption was consistent with the public good. While there is a legitimate concern that such a worm could be manipulated as a precedent for someone seeking vigilante action, this case suggests how a computing professional should approach this work, by resorting to malicious actions only when other approaches are unsuccessful.

**Case: Linking Public Data Sets**

Quinn is a member of a medical research team studying the role of genetic factors in psychological disorders, particularly focusing on how different variants influence social behavior. To facilitate this work, Quinn built a tool that linked three anonymized data sets: an anonymized set of genetic test results accessible only by medical researchers, a publicly available anonymized database of clinical diagnoses, and a custom database of public social networking posts.

To preserve anonymity, the tool replaced all personally identifiable information in the social networking posts with quasi-identifiers. Quinn’s team was granted approval for a study by their ethics review board (ERB), on the grounds that all data was anonymous and/or public, and all users had opted in to the data collection.

**Case: Linking Public Data Sets**

While testing the tool, Quinn discovered a bug that incorrectly linked some records of multiple individuals as a single person. Given that the data sets were all anonymized, the team had accepted that such erroneous matches were likely to occur. The bug increased the expected number of such matches, but only slightly; as such, the bug was classified as low priority. Quinn raised concerns that there may be other such bugs and suggested that the source code be released under an open source license to facilitate peer review of both the tool and the overall research.
Consider: Before releasing the code, Quinn and the team need to consider the impact on relevant stakeholders, particularly individuals whose records are contained in the data sets. When data sets are linked, re-identification of individuals is a common risk, which could lead to harm. Quinn would need to evaluate the merged data according to established anonymization metrics. Even more problematic, Quinn would need to consider how the merged data sets could be linked with other unknown data collections to break the existing anonymity.

Analyze: Quinn’s team had a moral (and almost certainly a legal) responsibility to protect the human subjects of their research. Although they worked with their ERB as part of this process, making the tool publicly available—even while keeping the existing data private—introduces unpredictable risks of data re-identification. Individuals who opt into such data sets could not be expected to anticipate the risk of using their data in this way. The most relevant portions of the Code are Principles 1.2 and 1.6, though several other principles apply.

Review: Prior to releasing the source code in any way, Quinn’s team should consult with their ERB regarding the risks. It is possible that the ERB members lack the technical expertise to determine that releasing the code is tantamount to releasing the merged data. Additionally, Quinn should consider alternative ways to do such peer review, such as making the code available only on request and under restricted terms.

Evaluate: Principle 1.2 warns against the harms that can be caused by data aggregation; Principle 1.6 re-emphasizes this point by stressing that merging data can strip privacy guarantees in the original sets. Principle 1.6 also suggests that the inaccuracies introduced by the bug must be fixed, and subjects must be adequately informed of the risks. In addition, the tool may facilitate the collection of data (such as metadata associated with the social networking activity) beyond the minimum amount necessary. Principle 2.5 also declares that the team must consider possible future risks associated with this tool and data use. In addition, Principles 2.1 and 2.4 obligate transparent communication with stakeholders, which would obligate informing both the ERB and all subjects of these risks. As such, publicly releasing the source code for this tool could cause harm and would be inadvisable.

The use of social networking posts also raises concerns in regard to Principle 2.8. Although these posts were publicly accessible, Quinn’s team had no reasonable belief that using the data in this way was authorized. Some individuals’ posts may have been made public because they did not understand the system’s privacy controls. Even those who knowingly made their posts public would not have considered that these posts would be linked to genetic records.

Quinn’s attempt to seek peer review is consistent with the intent of Principles 2.2 and 2.4. In recognizing the potential for bugs in the tool, Quinn sought input from other computing professionals; however, given the risks involved, a more discreet form that did not involve a completely public release would have been recommended. It is not clear whether Quinn had sufficient training in data anonymization techniques; if not, the guidance of Principle 2.2 suggests that Quinn should not have developed the tool without acquiring these technical competencies.
Corazón is a medical technology startup that builds an implantable heart health monitoring device. The device comes with a smart phone app that monitors and controls the device wirelessly, as well as stores a persistent record that can be shared with medical providers. After being approved by multiple countries' medical device regulation agencies, Corazón quickly gained market share based on the ease of use of the app and the company’s vocal commitment to securing patients’ information. To further expand their impact, Corazón worked with several charities to provide the device at a reduced price to patients living below the poverty line.

As a basic security mechanism, Corazón’s implant could only be accessible through short-range wireless connections, requiring the phone and implant to be in close proximity. Data transferred between the app and the device employed standard cryptographic algorithms, and all data stored on the phone was encrypted. To support on-going improvement, Corazón had an open bug bounty program inviting disclosure of potential vulnerabilities in their app.

At a recent security conference, an independent researcher claimed to have found a vulnerability in the wireless connectivity. The researcher presented a proof-of-concept demonstration where a second device in close proximity could modify commands sent to the implant to force a device reset. The attack relied on the use of a hard-coded initialization value stored in the implant device that created a predictable pattern in the data exchanges that could be manipulated. In consultation with Corazón’s technical leaders, the researcher concluded that the risk of harm with this attack is negligible, given the limited capabilities of the device.

Corazón’s consultation with the researcher also highlights a key aspect of Principle 2.5. The design and implementation of Corazón’s products exhibit a commitment to comprehensive and thorough risk analysis. Furthermore, Corazón welcomed independent security evaluation to identify additional issues that their designers overlooked. Once a potential vulnerability was discovered, Corazón acted responsibly and quickly to determine the scope of the flaw with the aim of mitigating the harm.

One area of concern regarding Corazón’s design is the use of a hard-coded value in the implant. Given the nature of the device, fixing this design choice would be difficult if it proved necessary. However, there is insufficient evidence at this point to determine the scope of the risk induced by this design.
Corazón’s on-going commitment to security and improvement also exemplifies an important aspect of Principle 3.7. Corazón’s rapid success in this specialized healthcare field is an instance of the integration of technology into the infrastructure of society. Recognizing the increased stewardship required by this Principle, Corazón began working with charities to serve individuals whose poverty may have excluded them from access.

Diane recently started a new industry research job, joining the company’s interactive technologies team. In graduate school, her advisor had collaborated with several members of the team on a few research projects, involving and highlighting Diane’s contributions whenever possible. The team had been impressed by Diane’s work and recruited her as she was approaching graduation.

Max, the team’s technical leader, had built a reputation as a brilliant yet mercurial expert in augmented reality. His team’s contributions were highly cited within the field, with Max typically claiming primary authorship as the team leader. Their work was also highlighted frequently in the popular press, always with quotes only from Max. Despite the team’s repeated successes, Max would erupt with verbal and personal attacks for even minor mistakes. He would yell at the person and berate them in internal chat forums. On multiple occasions, team members—only the women—have found their names removed from journal manuscript submissions as punishment.

Diane soon found herself the target of one of Max’s tirades when she committed a code update that introduced a timing glitch in the prototype shortly before a live demo. Infuriated, Max refused to allow Diane to join the team onstage. Feeling Max’s reaction was unprofessional and abusive, Diane approached the team’s manager, Jean, who must consider how to respond.

Max’s abusive behavior clearly violates several principles in the Code. His verbal abuse violated both Principles 1.1 and 1.2, by failing to maintain a safe social environment and failing to adhere to high standards of professional communication. By removing names from journal submissions and blocking Diane from appearing onstage, Max violated these team members’ rights to credit for their work, violating Principle 1.5. Max’s retaliation also demonstrates a violation of Principle 1.4. His punitive actions of removing names and blocking participation show a history of targeting only women team members. This behavior is a clear abuse of power that limits these team members’ fair access to the work environment.

Section 3 of the Code provides Jean with guidance on how to respond in this case. Principle 3.3 obligates leaders to provide for the psychological well-being and human dignity of the team. In addition, Principle 3.4 has leaders articulate, apply, and support policies that reflect the principles of the Code. Allowing Max’s behavior to continue unchallenged would fail to achieve this standard. Consequently, Jean must address Max’s behavior and support Diane’s objection.
Case: Malicious Input to Content Filters

The U.S. Children's Internet Protection Act (CIPA) mandates that public schools and libraries employ mechanisms to block inappropriate material that is deemed harmful to minors. Blocker Plus is an automated Internet content filter designed to help these institutions comply with CIPA's requirements. To accomplish this task, Blocker Plus has a centrally controlled blacklist maintained by the software maker. In addition, Blocker Plus provides a user-friendly interface that makes it a popular product for home use by parents.

Case: Malicious Input to Content Filters

Due to the challenge of continually updating the blacklist, the makers of Blocker Plus began to explore machine learning techniques to automate the identification of inappropriate content. During the development of these changes, Blocker Plus combined input from both home and library users to aid in the classification of content. Pleased with their initial results, Blocker Plus deployed these techniques in their production system. Furthermore, Blocker Plus continued to collect input from users to refine their learned models.

Case: Malicious Input to Content Filters

During a recent review session, the development team reviewed several recent complaints about content being blocked inappropriately. An increasing amount of content regarding gay and lesbian marriage, vaccination, climate change, and other topics not covered by CIPA, had been added to the blacklist. Initial investigations into these incidents suggested that some activist groups had exploited Blocker Plus's feedback mechanism to provide input that corrupted the classification model.

Analysis

Blocker Plus is a system designed to block content legally designated as harmful to children. While this filtering constitutes a form of censorship, children are considered a protected vulnerable class. To reduce the impact on adults, CIPA also mandates that these filters must be disabled on request. Given that Blocker Plus is complying with U.S. federal regulations to facilitate socially responsible uses of computers, the system is consistent with Principles 1.1 and 2.3.

Analysis

Given the complexity and risk involved in Blocker Plus's use of machine learning techniques, Principle 2.5 calls for extraordinary care. Principle 2.9 suggests that Blocker Plus should have included better protections against the intentional misuse by the activist groups. Blocker Plus’s deployment of machine learning causes harm by suppressing information of legitimate public interest and safety, as well as by discriminating based on sexual orientation, raising concerns for both Principles 1.2 and 1.4.

Analysis

In addition, Blocker Plus provides an example of a system becoming integrated into the educational infrastructure of society. Principle 3.7 emphasizes that the developers of such systems have an added responsibility to provide good stewardship and Blocker Plus must correct these issues.
Linux Code of Conflict

As a reviewer of code, please strive to keep things civil and focused on the technical issues involved. We are all humans, and frustrations can be high on both sides of the process. Try to keep in mind the immortal words of Bill and Ted, "Be excellent to each other."

Code of Conflict

Contributor Covenant

"This week people in our community confronted me about my lifetime of not understanding emotions. My flippant attacks in emails have been both unprofessional and uncalled for. Especially at times when I made it personal. In my quest for a better patch, this made sense to me. I know now this was not OK and I am truly sorry." -- Linus

Contributor Covenant

Microsoft

Letter from Satya Nadella


Is it consistent with our core values and the Standards?
We expect you to think through the issues and to use available resources to help including our core values and the Standards.

Is it Legal?
We are not expecting you to be a lawyer or legal expert. We do expect you to ask questions and seek guidance if you are not sure.

Am I comfortable with others finding out about my decision?
If you would not be comfortable with friends, family, and co-workers, it probably is not the right thing to do.
If you cannot answer yes, or are not sure, do not make the decision or take the action until you get additional help and guidance.

Not on Board

"Sometimes, it looks like we're replacing in-your-face incivility with knife-in-the-back incivility."

"We've known that it's being used politically, instead of encouraging meritocracy. I don't understand why these people don't come down on this like a ton of bricks. It's toxic culture, and it will poison the projects that adopt it. Contributors will leave, politicians will remain. Until you can stick a fork in it."

"If feelings get in the way of results this amounts to self-sabotage by the community as a whole. I'm a slightly abrasive person, and I do my best to make sure I'm polite, but sometimes things get in the way. I got a little cranky, but that's because I have personal problems that make it harder to be nice all the time. My inability to be a perfect person 100% of the time shouldn't put me in jeopardy of not being able to participate in the community. Targeted harassment? Ban it, obviously. Some hurt feelings because of something being given the bent of "toxic masculinity" when it doesn't exist? GTFO."

"All of this is so unbelievably worrying. How can they not see what they are doing? Meritocracy is the very foundation OSS is built upon. I would understand adopting a mild and very basic CoC in order to encourage positive and productive collaboration. But such an ideological piece from this unbelievably toxic author... Linus, what the fuck are you doing?! You're letting everyone down!"

Coddling of the American Mind?

"Something strange is happening at America’s colleges and universities. A movement is arising, undirected and driven largely by students, to scrub campuses clean of words, ideas, and subjects that might cause discomfort or give offense."

The coddling of the American mind

Codes of Conduct: Questions

● Are codes of conduct even effective or practical? Are they really necessary?
● Is it fair to require people to refrain from actions or speech which they consider non-offensive but others might find offensive?
● Do we have a right to not be offended? Should we be protected from offensive speech or actions?