12.AI Programming, ethics

The Association for Computing Machinery (ACM) is the world's largest educational and scientific computing society. It has its own Code of Ethics and another set of ethical principles that were also approved by the IEEE as the standard for teaching and practicing software engineering. These codes are Code of Ethics and Professional Conduct and the Software Engineering Code of Ethics and Professional Practice, respectively, and some of their guidelines are presented below:

From the Code of Ethics and Professional Conduct (ACM):

- **Contribute to society and human well-being.** Programmers should work to develop computer systems that can reduce negative consequences to society, such as threats to safety and health, and that can make everyday activities and work easier. It is “an obligation to develop to high standards” (Savage).
- **Avoid harm to others.** Computer systems have an indirect impact on third parties. They can cause loss of information and resources that might result severely harmful for users, the general public, or employers. Therefore, software developers should minimize the risk of harming others due to coding errors, or security issues, by following standards to design and test systems (Code of Ethics and Professional Conduct).
- **Be honest and trustworthy.** This principle encourages programmers to be honest and aware of their limitations in knowledge and education when writing computer systems. Also, if a programmer knows there is something wrong with a computer system, they should report it immediately to avoid undesirable consequences.
- **Give proper credit for intellectual property.** It is mandatory for every software developer to never use and take credit for someone else's work, even when it has not been protected by a copyright law, patent, etc. They must recognize and fully credit other people's works, and they should use their own ideas to develop software.
- **Respect the privacy of others.** Computer systems are wrongly used by some people to violate the privacy of others. Software developers should write programs that can protect users’ private information and that can avoid other undesired people to have unauthorized access to it (Code of Ethics and Professional Conduct).

- **Honor confidentiality.** Unless required by law or any other ethical guideline, a programmer must keep secret any additional information related to their employer that arises from working in a project.

From Software Engineering Code of Ethics and Professional Practice (IEEE, ACM):

- **Approve software only if they have a well-founded belief it is safe and meets specifications.** Programmers cannot assume that a system is ready to use only because it performs the tasks needed. They should make sure these systems are also safe and meet every specification required by the user. If programs are not safe, users are unprotected from hackers that could steal important information or money. Therefore, several tests should be performed in order to ensure a system's security before approving it.
- **Accept full responsibility for their own work.** If a program presents errors, the software developer should accept full responsibility for their work, and should work on revising, correcting, modifying, and testing it.
- **Not knowingly use software that is obtained or retained either illegally or unethically.** If a computer system will be used as a base for the creation of another, then permission to do so should be asked by the programmer. This principle prohibits using any other software for any purpose if the way it was gotten is not clear or is known to be illegal or unethical.
- **Identify, define, and address ethical, economic, cultural, legal and environmental issues related to work projects.** If a programmer notices and identifies that working on a project will lead to any kind of problems, then the programmer should report it to their employer before continuing.
- **Ensure that specifications for software on which they work satisfy the users' requirements and they have the appropriate approvals.** Software developers should come to their employers to ask for the correspondent approval to the system they are creating before continuing working on the next part. If it doesn't meet the requirements, then a modification to the source code of the system should be made.
- **Ensure adequate testing, debugging and review of software.** Programmers should perform the appropriate tests to the pieces of software they work with, and should check for errors and

system security holes to make sure that the programs are well implemented.

- **Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.** Programmers are exposed to be participants in illegal activities to get money. They get involved in them due to threats, economic issues, or simply because they want to obtain easy money by taking advantage of their knowledge about how computer systems work. This guideline prohibits programmer involvement in such unlawful actions.
- **Improve their ability to create safe, reliable, and useful quality software.** Since technology advances faster year by year, and so does virtual criminality, the need of well-structured and designed programs is increasing. Computer systems get old and limited by new ones and new devices. Programmers should "further their knowledge of developments in the analysis, specification, design, development, maintenance, and testing software and related documents" (Software Engineering Code of Ethics and Professional Practice) in order to create better pieces of software.

Ethical Programming

Ethical programming involves understanding that every piece of code, no matter how innocuous it may seem, has the potential to significantly impact society. Take for instance the influence of algorithms on social media. They can lead to the spread of fake news, influence elections, or even incite hate and violence. These potential consequences highlight the necessity of ethics in programming.

An ethical programmer considers not just the technical aspects of programming, but also the social and societal implications. This means that we must consider factors such as privacy, fairness, inclusivity, and transparency when designing and developing software. We need to ask critical questions such as: Who might be disadvantaged by this product? Whose privacy could be infringed upon? Does the end user have control over their data?

Incorporating these considerations into our work allows us to create technology that serves society rather than harms it. Ethical programming is also closely tied to sustainability in the IT sector. For example, by considering the energy efficiency of our code, we can contribute to a greener planet.

The recruitment world

World In the recruitment world, this is also increasingly coming to the fore. The ability to reason ethically and the willingness to take responsibility for the social impact of a product are qualities that are increasingly valued in potential candidates. When attracting and selecting talent, we therefore look not only at technical competencies but also at these ethical considerations.

Teaching and promoting ethical programming should play a central role in IT education and training. However, this is no easy task. Ethics are complex and subjective, and there's no 'one-size-fits-all' solution. Nevertheless, we can take steps to foster ethical awareness and critical thinking in our sector, for instance, by making ethics and societal impact a fixed part of the curriculum.

At its core, ethical programming is about taking responsibility for our technological creations. It's an essential part of our role as IT professionals to develop technology that is not only innovative and efficient but also ethically responsible and socially beneficial. It's not just a question of 'can we build this,' but also 'should we build this.'

In a world that is increasingly driven by technology, the ethical dimension of programming becomes ever more important. It's up to us to ensure that the technologies we create and implement truly benefit society as a whole.

The Essence of Ethical Coding

Coding, in essence, is a form of communication with a computer, instructing it to perform certain actions. Ethical coding is about ensuring that these instructions do not lead to harm, injustice, or inequity. It entails following a set of principles that guide responsible conduct in the creation and use of software. These principles include respect for privacy, honesty, fairness, and a commitment to doing no harm.

This function collects and returns user data when called. Ethical considerations arise when we ask questions like:

What kind of data are we collecting?

Why are we collecting this data?

Is the user aware and have they consented to this data collection?

How is the data being stored and protected?

Unethical coding would ignore these questions, potentially leading to misuse or violation of user privacy.

Why Ethics in Coding Matters

The need for ethical coding is underscored by the increasing influence of software in everyday life. Applications that we use daily are powered by lines of code, and these code decisions can greatly impact users.

For instance, consider a simple AI model that uses machine learning to make decisions about loan approvals:

This function uses a trained model to decide whether a loan application should be approved. Ethical issues arise if the model discriminates against certain groups, for example, based on their race or gender. If the underlying data used to train the model is biased, the model's decisions will also be biased. This can have real-world consequences, such as unfair denial of loans to deserving applicants. Ethical Guidelines for Coding

So, how can we ensure ethical coding? Here are some guidelines that can be followed:

User Consent and Data Privacy

Always ensure that user data is collected and used with full consent. Respect the privacy of users and take measures to protect their data. For example, if you are designing a form for user registration, it would be unethical to collect more information than necessary, especially without informing the user.

This form collects the first and last name of a user, which seems innocuous. However, without the user's consent and without a clear indication of how this data will be used and stored, it is ethically wrong to collect such information.

Fairness and Non-Discrimination

Ensure your code and the systems it powers do not discriminate or promote unfair practices. This is particularly important in AI and machine learning, where biased data can lead to unfair outcomes.

Honesty and Transparency

Be honest about what your code does and maintain transparency, especially in areas that affect user dataand privacy. This could involve providing clear documentation and user agreements detailing how data is collected, used, and stored.

In this code, a privacy policy is clearly stated and can be called to inform the user about data use.

Accountability

Take responsibility for your code and the impact it has. If your code causes issues or harm, be willing to acknowledge this, learn from it, and rectify the mistake.

In this function, accountability is shown by handling errors that may occur during the data deletion process and taking corrective action.

Ethical Challenges in Coding

While the guidelines above are helpful, implementing ethical coding is not without challenges. These include:

Handling of Biases

As we discussed earlier, coding can inadvertently lead to bias, particularly in machine learning applications. It is vital to critically assess the data used in training models to ensure they are not reinforcing existing societal biases.

Privacy versus Personalization

There is a constant tug-of-war between providing personalized user experiences and maintaining user privacy. Striking the right balance is a significant ethical challenge for coders.

Accessibility

Ensuring that your applications are accessible to all users, including those with disabilities, is not only an ethical requirement but often a legal one as well.

Incorporating Ethics into Coding Education

In light of the importance of ethical coding, it should be a part of coding education. Students should be introduced to ethical dilemmas in coding and taught how to address them.

This could be done through practical exercises and discussions. For example, students can be given a coding task that involves handling user data, and then asked to discuss the ethical considerations involved.

From time to time you hear people in the developer community talk about how we should be more ethical. This usually revolves around A.I. and if a driverless car should prioritize passengers or pedestrians. Yet today I'm going to tell you a story about how I refused to work on a project I felt violated my code of ethics.

I worked in a call-center of a non-profit medical research facility that helped people stop smoking. The idea is that they'd call looking to quit and the agents would help them find a way that best suited their needs. I worked with a small development team to create a new call-center application.

I was there almost a year when one of the managers sent me an email asking to create a small application. I was getting a lot of requests at the time because everyone knew we contractors were being let go at the end of the month due to budget concerns.

I was so shocked by what I read that I had to reread the email three times to make sure I understood what they were asking. I called the manager to clarify what exactly they wanted, I'd hoped I misunderstood the email.

Nope!

They wanted me to take a list of known U.S. Department of Housing and Urban Development (HUD) addresses and compare that to where our active callers lived. If they lived at a known address the application would report them to our HUD contact.

Let me break that down. You can't smoke in HUD facilities it's against the rules. They wanted an application to report someone trying to get help with their addiction. Which meant they'd get in trouble with their landlord or HUD.

What did I do? Did I immediately speak out against this unjust idea? Did I march into the manager's office and make a passionate plea for the people we're supposed to help? No, I put the project off citing I was too busy with other things at the time.

I didn't address the issue, I didn't make anything better, and it didn't stop the project. Two weeks before I left I got another email from someone higher up in management. They told me that this project should be my new and only priority.

I didn't know what to do. For the next week, I feined researching the API they wanted me to use to buy myself some time. I did actual research and learned

about it I just didn't do it with any seriousness. I planned to run down the clock as it were.

Then in the last week, I got a phone call from the person higher up in management I mentioned earlier. They wanted to know what was taking so long and proposed I set up a meeting to go over the details. There was a long pause after he asked when I was free the next day. I felt backed into a corner and decided the only way out was to finally do the right thing and voice my objections.

He didn't say much while I told him how I felt about the project and the negative impact it would have on the people who relied on us to help them. When I finished he reiterated the importance of the project and how we'd already promised HUD it would be ready by the next quarter. He didn't address anything I'd said during the call, he asked me again when I was free. I took a moment to collect myself and told him that I wouldn't be moving forward with the project. It was unethical and I couldn't be a part of it. Not that I was that eloquent.

After a heated retort he made it clear that I was jeopardizing my job. I told him I was leaving on Friday anyway because I was a contractor. I thanked him for his time, why I don't know, and hung up the phone.

I didn't hear from him or anyone in management after that. I assume they got someone else to make the application or let the idea fade away.

If you made it this far then congrats and thank you. This was kind of a long story but one I felt I needed to tell. I tried to make it as short as I could but a lot happened during all this.

In a way, I'm grateful it happened because it showed me where the line is that I won't cross. Though at the same time I'm not happy with how I handled it. I wonder what I would've done if I were a permanent employee instead and had more to lose.

Potential for Abuse

One significant ethical consideration related to semiconductor device programming is the potential for abuse of the devices. For example, in the realm of computing, programming a semiconductor device to hack into a computer system or access sensitive information without permission is clearly unethical. Similarly, programming a semiconductor device to facilitate identity theft or other forms of fraud is also unethical.

Hacking and Cybersecurity

Another ethical consideration related to device programming is the potential for malicious actors to exploit vulnerabilities in these devices to cause harm. For example, if a semiconductor device used in a critical infrastructure system, such as a power grid or water treatment plant, is vulnerable to hacking, it could potentially be manipulated to cause widespread disruption or damage; or programming a device used in a medical device to malfunction or deliver incorrect treatment could have serious consequences for the patient. Similarly, programming a semiconductor device used in transportation systems (such as self-driving cars) to malfunction could lead to accidents and harm to both passengers and bystanders.
Additionally, programming errors or vulnerabilities in semiconductor devices used in personal devices, such as smartphones or laptops, could leave individuals vulnerable to cyber-attacks such as data breaches or theft of personal information. It is important for manufacturers, developers, and operators to ensure that these devices are properly secured and tested for vulnerabilities to minimize these risks, and to have a plan in place to mitigate the damage of a successful attack.

Bias

A third ethical consideration related to semiconductor device programming is the potential for discrimination or bias. For example, programming a semiconductor device used in hiring or promotion decisions to favor certain groups or individuals based on characteristics such as race or gender could be considered unethical. Similarly, programming a semiconductor device used in

credit or loan decisions to unfairly disadvantage certain groups or individuals could also be considered unethical.

Skynet

Certainly, one ethical consideration related to semiconductor device programming, albeit perhaps more far-fetched, is the potential for the development of artificial intelligence (AI) systems that are capable of autonomous decision-making. This is similar to the concept of Skynet, a fictional AI system in the Terminator franchise that becomes self-aware and turns against humanity. As the capabilities of semiconductor devices and AI systems continue to advance, it is important to consider the potential consequences and ensure proper safety measures and regulations are in place to prevent negative outcomes.

In order to address these ethical considerations, it is important for those involved in semiconductor device programming to consider the potential consequences of their actions and to ensure that their programming is ethical and responsible. This may involve implementing safeguards and controls to prevent abuse or misuse of the devices, as well as regularly reviewing and evaluating the programming to ensure that it is not causing harm or discrimination.

Ultimately, the ethical considerations of device programming highlight the need for ongoing dialogue and discussion about the responsible use of technology. By considering the potential consequences of our actions and making ethical choices, we can ensure that the benefits of semiconductor devices are maximized while minimizing any negative impacts.

What does the word ‘ethics’ mean? The dictionary defines ethics because of the moral principles that govern the behavior of a gaggle or individual. But, not every people in society need to live an absolutely moral life. Ethics are actually the unwritten code of conduct that every individual should follow. These codes are considered correct only by the members of that particular profession. Similarly, for computer users, computer ethics is a set of principles that regulates the use of computers. Computer ethics address issues related to the misuse of computers and how they can be prevented. It primarily imposes the ethical use of computing resources. It includes methods to avoid violating the unauthorized distribution of digital content. The core issues surrounding computer ethics are based on the use of the internet, internet privacy, copyrighted content, software, and related services, and user interaction with

websites. The Internet has changed our lifestyle. It has become a part of our life. It allows us to communicate with a person from another part of the world. collecting information on any topic, social meets, and many other activities. But at the same time, some peoples are always trying to cheat or harm others.

Advantages of using the internet:

The Internet offers the facility to communicate with a person in any part of the world.

We can easily collect information related to any topic from the world wide web on the internet.

Various types of business are carried out through Internet, which is referred to as e-commerce. From booking railway tickets and flight tickets or tickets for movies to purchasing any type of merchandise or commodities, are possible via the Internet.

The Internet allows social networking, that is, it provides the ability to share our information, emotions, and feelings with our friends and relatives.

Disadvantages of using the internet:

A group of people is trying to get personal information (like bank detail, address, contact details, etc,) over the Internet and uses that for unethical benefits.

Malware or viruses are becoming quick access to different networks and ultimately are causing harm to personal computers(PC) or computers connected to the network.

Some people run deceitful businesses over the Internet, and the common people very often become victims of them.

People use the internet for cyberbullying, trolling, etc.

Ten commandments of computer ethics:

The commandments of computer ethics are as follows:

Commandment 1: Do not use the computer to harm other people's data.

Commandment 2: Do not use a computer to cause interference in other people's work.

Commandment 3: Do not spy on another person's personal data.

Commandment 4: Do not use technology to steal personal information.

Commandment 5: Do not spread misinformation using computer technology.

Commandment 6: Do not use the software unless you pay for this software.

Commandment 7: Do not use someone else's computer resources unless he authorized to use them.

Commandment 8: It is wrong to claim ownership of a work that is the output of someone else's intellect.

Commandment 9: Before developing software, think about the social impact it can of that software.

Commandment 10: While computers for communication, always respectful with fellow members.

Internet Security

The internet is an insecure channel for exchanging information because it features a high risk of fraud or phishing. Internet security is a branch of computer security specifically associated with the utilization of the internet, involving browser security and network security. Its objective is to determine measures against attacks over the web. Insufficient internet security can be dangerous. It can cause many dangerous situations, like starting from the computer system getting infected with viruses and worms to the collapse of an e-commerce business. Different methods have been devised to protect the transfer of data over the internet such as information privacy and staying alert against cyber attacks.

Information Privacy: Information privacy is the privacy or protection of personal information and refers to the personal data stored on a computer. It is an important aspect of information sharing. Information privacy is also known as data privacy or online privacy. Some Internet privacy involves the right of personal privacy and deals with the storing and displaying of personal information on the internet. In any exchange of personal information over the internet, there is always a risk involved with the safety of personal information. Internet privacy may be a cause for concern especially when online purchases, visiting social networking sites, participating in online games or attending

forums. Privacy issues can arise in response to information from a good range of sources, such as:

- Healthcare records
- Financial institution transactions
- Biological traits
- Residence records
- Location-based service

The risk involved in internet privacy is sometimes dangerous. In the process of data transfer over the internet, if a password is revealed, a victim's identity may be deceitfully used.

Some important terms:

Spyware: An application that obtains data without the user's consent.

Malware: An application used to illegally harm online and offline computer users

Virus: It is a small program or software which is embedded with a legitimate program and designed to harm your system.

Worms: It is a self-replicating program that spread across networks due to the poor security of the infected computers.

Trojan horse: Trojan horse is a program that allows the hackers to gain remote access to a target system.

General steps to protect our system from risks:

To minimize internet privacy violation risks, the following measures need to be taken:

Always use preventive software applications, like anti-virus, anti-malware, etc,

Avoid exposing personal data on websites with low-security levels.

Avoid shopping from unreliable websites

Always use strong passwords consisting of letters, numerals, and special characters.

Always keep your operating system updated.

Always on the firewall.

Unethical computing practices:

Now we discuss some unethical computing practices:

1. Cyberbullying: When people bully other people by the use of electronic communication (like the web, telephone, etc). it's referred to as cyberbullying. Cyberbullying has been done by friends, classmates, relatives, any other unknown persons. Sending harmful emails to a person creates fake websites to make fun of or to make harm a person by distributing the same fake information about a person posting and distributing fake images of a person. These are some common ways of cyberbullying.

In most cyberbullying cases, they do not reveal their identities. Due to cyberbullying, some bullied persons are affected emotionally or mentally. Even if those are fake information, the bullied person may become depressed or it may affect their day-to-day life. In the case of the students or kids, it may affect their study or they may lose self-esteem.

How to protect yourself from cyberbullying:

Not to respond to cyberbullying.

Never open e-mails received from unknown senders.

Keep your password secret.

Be careful, when you are posting something on a social site.

2. Phishing: An internet hacking activity used to steal user data. In this activity, an email is sent to the user which misleads him/her to believe that it is from a trusted organization. After sending the email, the attacker asks the user to visit their website, and on their website, they will ask for the personal information of the user like password, credit card information, etc. So, this is how the attacker steals the personal information of the user.

How to protect yourself from phishing:

Never open a link, attachment, etc in an email that is sent by some unknown person.

Never share your personal information in an email that is asked by an unknown person.

Always on the firewall of the computer system.

Always check your bank statements regularly to ensure that no unauthorized transactions are made. If unauthorized transactions are made in your account, then immediately report this issue to your bank.

3. Hacking: It is an unethical activity in which a highly skilled technical person(or commonly known as a hacker) enters another person's computer without the permission of the user and steals important data/project/applications from the computer or sometimes destroys the information from the system.

How to protect yourself from hacking:

Never connect your system to free Wi-Fi or a free network.

Always use strong passwords consisting of letters, numerals, and special characters.

Before installing any application in your system, always check permission and authenticity.

Always keep your operating system updated.

Always use preventive software applications, like anti-virus, anti-malware, etc,

4. Spamming: It is an unethical activity in which bulk unwanted e-mail is set to you from a strange or unknown source. Sometimes, due to bulk emails, your mail server gets full and mail bombing activity happens. Spam mail is generally used to deliver viruses, worms, trojan horses, malware, spyware, etc. to attack the user.

How to protect yourself from spam:

To prevent spam mail, install filtering or blocking software.

In your mailbox, if you find suspicious mail, then immediately delete that mail(without opening).

Always keep your software updated.

Never open the link that is sent by an unknown person.

5. Plagiarism: Plagiarism is stealing or copying someone else's intellectual work (can be an idea, literary work or academic work, etc.) and representing it as your own work without giving credit to the creator or without citing the source of information.

How to protect yourself from plagiarism:

While writing, always writes in your own words.

Always use a plagiarism checker before the update.

If you are taking someone else's work, then always give the credit to the original author in an in-text citation.