Technology Ethics

Rashid, Muhammad Mustafa

University of Detroit Mercy, University of California Davis

19 December 2020

Muhammad M Rashid

Technology Ethics

University of Detroit Mercy, University of California Davis

Table of Contents

INTRODUCTION

Technology Ethics is defined as the application of ethical thinking to the practical concerns of technology. In recent years with the rapid development of technology this field has reached prominence because new innovative technologies give us more power to act. Hence, in the past where our actions were limited by our weakness, in this day and age of technological advancement they are voluntarily constrained by our judgement and hence ethics. In recent years many new ethical questions have arisen due to innovations in medical communications, weapons technology, and workplace technologies. Therefore, for example, there used to be no brain death criteria as we do not have the technological prowess to ask that questions, but in this day and age with the technological prowess of being able to artificially maintain circulation and respiration this question has become much more serious. In the same way the rise of media communications gives rise to new questions when it comes to social media and we are still coming to terms with access to the information of so many people. Many issues have arisen such a fake news and how things can quickly go wrong on social media, and how criminals may have access to information of private individuals due to data breeches and hacks of company databases. (Green, n.d.)

The changes in technology come with disruptions and raise many ethical questions representing powerful risks. Therefore, these disruptions give rise to questions and demand us to critically think before accepting these changes as permeant in our lives. We do have a choice as to how we implement and integrate these technologies into our lives. Furthermore, our intellect and existing systems allow us to govern these technologies by laws and regulations and other agreements. Hence, it is required for us to ask fundamentally important questions as we navigate this new field and to evaluate what is right and what is wrong, what is good and what is evil.

Hence, as long as there is technological progress there will be need and growth of technology ethics, and hence as Chief Information Technology it is imperative to understand the different ethical and legal positions that arise due to technological advancement. (Green, n.d.)

IT ETHICS

Perhaps the best way to start the discussion on IT Ethics is through the framework developed by the Association of Computing Machinery. The Association of Computing Machinery (ACM) is one of the earliest organizations to provide guidance in the form of ethical content and form. The ACM has written an ethical code by which many IT professionals abide by. This Code of Ethics referred to as Code covers four basic categories containing key principles The Code of Ethics covers four specific categories containing key principles and appropriate action items to follow. (Machinery, 2020)

Table 1 Selection of the ACM Code of Ethics and Professional Practice

1. GENERAL MORAL IMPERATIVES.

1.1 Contribute to society and human well-being.

1.2 Avoid harm to others.

1.3 Be honest and trustworthy.

1.4 Be fair and take action not to discriminate.

1.5 Honor property rights including copyrights and patent.

1.6 Give proper credit for intellectual property.

1.7 Respect the privacy of others.

1.8 Honor confidentiality.

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.

2.3 Know and respect existing laws 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.

2.6 Honor contracts, agreements, and assigned responsibilities.

2.7 Improve public understanding of computing and its consequences.

2.8 Access computing and communication resources only when authorized to do so

2.9 Design and implement systems that are robustly and usably secure

3. 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 responsibility 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.

3.6 Use case when modifying or retiring systems.

3.7 Recognize and take special care of system that become integrated into the infrastructure of society

4 COMPLIANCE WITH THE CODE

A computing professional should…

4.1 Uphold, promote and respect the principles of the Code.

4.2 Treat Violations of the case as inconsistent with membership in the ACM

The Code of Ethics provided for by ACM provides for a comprehensive outline from which to start our inquiry into the IT Ethics. (Machinery, 2020)

When it comes to business of all sizes but especially small business that utilize Information Technology, there are four area of critical concern and hence; piracy, data protection and privacy, ransoms and ransomware, ethics and AI. (Weedmark, 2018)

PIRACY

Evolution in information of technology removes ethical dilemmas IT Managers and CTO's face. Software piracy is such a case, but even with the advancements in technology worldwide piracy is still an issue. IT is estimated that 37 percent of software on personal computers is unlicensed according to Forrester Groups 2018 BSA Global software survey. With time this problem is not as severe as before. It is again estimated that malware costs companies nearly $359 billion a year hence it makes financial sense to use licensed software. Furthermore, with proper software management, companies can increase profits by as much as 11 percent per year.

The legal implication of unauthorized software use should be clear as it is very daunting. According to the US Copyright Act, illegal reproduction of software is subject to civil damages of as much as $100,000 per title infringed plus criminal penalties including fines of as much as $250,000 per title infringed and imprisonment of up to five years. Given these high stakes, the consequences are certainly not worth the risk. (Weedmark, 2018)

If we for a moment set aside the legal risks of software piracy and look at it from an ethical perspective, we would begin by examining the principles of fairness and justice. Companies devote a large portion of their earning to the creation of new software products. The programmers, writers and all of the highly skilled labor involved deserve to be compensated for their efforts just as we expect fair compensation for ours. We all prefer to have a world where respect for our own property and for the property of others is the norm. Furthermore, if we apply the virtue approach to ethics, we apply the concepts of honesty, trustworthiness, faithfulness and integrity and soon discover that piracy of software does not fall into any of these categories. (Shoup)

Therefore, what are the best practices that an IT Manager of CTO can adopt in case of piracy? The first step is to get rid of any pirated software so that you are not viewed as a role model that supports pirated software. Secondly find the resources to purchase the software that is needed for the workplace. This comes with many advantages, such as user support, ability to avoid legal penalties and most importantly setting a standard and acting ethically. Furthermore, many companies have developed written employee policies about the use of software and this practice should be adopted and studies carefully. A great resource is for developing such a policy is the following: The Software Publishers Association. (Shoup)

DATA PROTECTION AND PRIVACY

With the advancement in Information Technology one of the biggest problems that have surfaced is Data Protection and Privacy. Hence, customer and employee data protection from being exposed to the public or from being hacked is of vital importance in this day and age. However, the line between the cost of protection of digital information has become blurred in the recent years. Firewalls, encryption technologies, virtual private networks, security specialists all require a significant amount of capital. According to Foresters 2018 report on ethics and consumer action, 79 percent of US adults use tools to protect their digital privacy and security online. The survey also estimates that regulations such as California’s Consumer Privacy Act and the GDPR also continue the consumer push-back against companies that do not protect data or use data responsibly. (Weedmark, 2018)

The EU's General Data Protection Regulation (GDPR) is a great starting point regarding the data privacy in global organizations. The GDPR isn't just about protecting sensitive information against hackers and leaks. The GDPR, also focuses on data privacy for business. Therefore, for organizations that are subject to the GDPR there are two broad categories of compliance: data protection and data privacy. Data protection means keeping data safe from unauthorized, and data-privacy means empowering users to make their own decision about who can process their data and for what purpose. The GDPR is the toughest privacy and security law in the world. Though it was drafter and passed by the EU it imposes obligation onto organizations anywhere so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25th, 2018. The GDPR has the ability to levy harsh fines against those who violate its privacy and security standards with penalties reaching into the tens of millions of euros. (GDPR, 2020)

The GDPR is a signal from the Europe on the stance on data privacy and security at a time where more and more people are entrusting their personal information to cloud services while at the same time the number of data breaches is at an all-time high. Some of the important legal terms of the GDPR.

- Personal Data – Is any information that relates to an individual who can be directly or indirectly identified.
- Data Processing – Any action performed on data whether automated or manual
- Data Subject – The person whose data is processed. These are your customers or site visitors.
- Data Controller – The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

- Data Processor – A third party that processes personal data on half of a data controller. The GDPR has special rules for these individuals and organizations. (GDPR, 2020)

Data Protection Principles.

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.
4. **Accuracy** — You must keep personal data accurate and up to date.
5. **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles. (GDPR, 2020)

Accountability

- Designate data protection responsibilities to your team.
- Maintain detailed documentation of the data you’re collecting, how it’s used, where it’s stored, which employee is responsible for it, etc.
- Train your staff and implement technical and organizational security measures.

- Have Data Processing Agreement contracts in place with third parties you contract to process data for you.
- Appoint a Data Protection Officer. (GDPR, 2020)

Data Security

- Data is to be handled securely by implementing "appropriate technical and organizational measures:
- Technical measures include, two factor authentication and end-to-end encryption.
- Organizational measures include staff training, data privacy policy and limiting access to personal data.
- In case of a data breach there is a 72 hour window to inform the subject or face a penalty. (GDPR, 2020)

Data Protection by Design and by Default.

From now on everything you do in your organization must "by design and by default consider data protection. This means that you must consider the data protection principles in the design of any new product or activity. Hence, for example you're launching a new app for your company. You have to think about what personal data the app could possibly collect from users, then consider ways to minimize the amount of data and how you will secure it with the latest technology.

Data Processing. The processing of person data is also a legal issue. It can only be processed when one of the following justifications are provided.

1. The data subject gave you specific, **unambiguous consent** to process the data. (e.g. They've opted in to your marketing email list.)
2. Processing is necessary to execute or to prepare **to enter into a contract** to which the data subject is a party. (e.g. You need to do a background check before leasing property to a prospective tenant.)
3. You need to process it **to comply with a legal obligation** of yours. (e.g. You receive an order from the court in your jurisdiction.)
4. You need to process the data **to save somebody's life**. (e.g. Well, you'll probably know when this one applies.)
5. Processing is necessary **to perform a task in the public interest** or to carry out some official function. (e.g. You're a private garbage collection company.)
6. You have a **legitimate interest** to process someone's personal data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data. (It's difficult to give an example here because there are a variety of factors you'll need to consider for your case. (GDPR, 2020)

Consent. There are now strict rules about what constitutes consent from a data subject to process their information.

- Consent must be "freely given, specific, informed and unambiguous."
- Requests for consent must be "clearly distinguishable from the other matters" and presented in "clear and plain language."

- Data subjects can withdraw previously given consent whenever they want, and you have to honor their decision. You can't simply change the legal basis of the processing to one of the other justifications.
- Children under 13 can only give consent with permission from their parent.
- You need to keep documentary evidence of consent. (GDPR, 2020)

Data Protection Officers. The conditions to appoint a Data Protection Officer.

1. You are a public authority other than a court acting in a judicial capacity.
2. Your core activities require you to monitor people systematically and regularly on a large scale. (e.g. You're Google.)
3. Your core activities are large-scale processing of special categories of data listed under **Article 9** of the GDPR or data relating to criminal convictions and offenses mentioned in **Article 10**. (e.g. You're a medical office.)

People's Privacy Rights: The GDPR recognizes a litany of new privacy rights for data subject which aim to give individuals more control over the data they loan to organizations. As an organization, IT Manager or a CTO, it is important to understand these rights to ensure you GDPR compliment. (GDPR, 2020)

Data Subjects privacy rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure

5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling. (GDPR, 2020)

RANSOMS & RANSOMWARE

In recent years the ethical problems in information technology have been complicated even further with a rise of ransomware attacks. Hackers infiltrate a computer network and take control of it and then demand a payment for a code that will release it. If you don't pay the ransom, you may lose all the data stored in the network. Even if you have the data backed up the time and expense of restoring our network may be more than the cost of paying the ransom. Business owners and IT managers who pay the ransom do so knowing that it will encourage hackers to do the same thing in an another organization. In 2016 the ride-sharing service Uber is an example of a ransom attack where Uber paid $100,000 ransom to hackers who accessed the personal data of 57 million people including information about the Uber drivers and their customers. The ethical and legal dilemma that arose was Uber's negligence in not telling the public. It wasn't until a a year (Stanford, Stanford, 2020) later that the ransom was revealed. This resulted in a court hearing and record fine of $148 million. (Weedmark, 2018)

Ransomware incidents can have serious consequences for business processes and organizations leaving them without the data needed to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pa and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased with some demands exceeding $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and prorogate ransomware across entire networks. These actors also increasingly use tactics such as deleting system backups, that make restoration and recovery more difficult and less feasible for impacted organizations. (Industry, 2020)

Ransomware Prevention Best Practices

Be Prepared: Maintain offline encrypted backups of data. Maintain regularly updated ‘gold images’ of critical systems. Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred. In addition to system images applicable source code or executable should be available. Create maintain and exercise a basic cyber incident response plan. (Industry, 2020)

Ransomware Infection Vector: Internet-Facing Vulnerabilities and Misconfigurations. Conduct regular vulnerability scanning to identify and address vulnerabilities especially those on internet facing-devices to limit the attack surface. Regularly patch and update software and Oss to the latest available versions. Ensure devices are properly configured and that security features are enabled. Employ best practices for use of RDP and other remote desktop services and audit systems. (Industry, 2020)

Ransomware Infection Vector: Phishing. Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity. Implement filters at the email gateway to filter out emails with known malicious indicators. To lower the chance of spoofed emails from valid domains implement Domain-based Message Authentication. Consider disabling macro scripts for Ms Office. (Industry, 2020)

Ransomware Infection Vector: Precursor Malware Infection: Ensure antivirus and anti-malware software and signatures are up to date. Use application directory allow listing on all assets to ensure that only authorized software's can run, and all unauthorizes software is blocked from executing. Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs to ransomware. (Industry, 2020)

Ransomware Infection Vector: Third Parties and Managed Service Providers: Take into consideration the risk management and cybergenic practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MPS's have been an infection vector for ransomware impacting client organization. Understand that adversaries may exploit the trusted relationship your organization as with third parties and MSPS. (Industry, 2020)

ETHICS AND AI

AI Ethics has become a business imperative for many a boards and C-Suites. A very important question that is being asked by is. What does responsible AI looks like and who owns it? The other question that is asked is if artificial intelligence (AI) will help us or hinder us? AI as a problem-solving tool offers a great promise. On the other hand, the emergence of AI has also exposed many problems such as cyber-attacks, social manipulation, completion for financial incentives and more warn of a dark-side to AI-Ethics. Hence, if an organization seeks to transform itself using AI ethical risks that arise are of a critical concern. (Weedmark, 2018)

AI is the term that is used to encompass technologies that can mimic intelligent human behavior. There are four major AI categories that are of increasing use nowadays.

1. Machine Learning. The ability of statistical models to develop capabilities and improve their performance over time without the need to follow explicitly programmed instructions.
2. Deep Learning: A complex form of machine learning used for image and speech recognition and involving neural networks with many layers and abstract variables.
3. Natural language processing (NL): A Technology that powers voice-based interfaces for virtual assistants and chatbots a well as querying data ses by extracting or generating meaning and intent from the text in a readable stylistically neutral and grammatically correct form.
4. Computer vision: A technology that extracts meaning and intent out of visual elements whether characters (in the case of document digitization) or the categorization of content in images such as faces, objects scenes and activities. (Deloitte, 2020)

Ethics deals with what is good and band and with moral duty and obligation as well as the principles of conduct governing and individual or a group. In the field of commerce, the ethical mindset supports value-based decision and what is not only good for the business but what's good for the organization's employees, client's customers, and communities, in which it operates. Hence, when we bring these two definitions, we come to the definition of AI Ethics which refers to the organization constructs that delineate right and wrong. These constructs include corporate values, policies and code of ethics, and hence form the guiding principles applied to AI technologies. (Deloitte, 2020)

According to Stanford, the field of AI ethics and robotics is a very young field within the field of applied ethics, with significant dynamic, but few well established issues and no authoritative overviews. A promising outline has been constructed by the European Group on Ethics in Science and New Technologies 2018 and we are beginning to see the societal impact. (Deloitte, 2020)

The following ae the emerging areas in AI Ethics according to Deloitte:

- Technology, data and security; looking at the organizations approach to the AI lifecycle from an ethical perspective, including the ways it builds and tests data and models into AI-enabled solution.
- Risk Management and Compliance; finding out how the organization develops and enforces policies procedures and standards for AI solutions.
- People, skills, organizational models, and training; understanding and monitoring how the use of AI impacts the experiences of both employees and customers.
- Public Policy, legal and regulatory frameworks, and impact on society; developing a place in the business environment, this includes the level of acceptance AI has in government and culture. (Deloitte, 2020)

AI Ethics Risks:

- **Research and Design;** The solutions inherent risks (such as a computer vision application that captures and potentially misuses customers or employees images or other personally identifiable information.)
- **Build and Train;** the organization lacks appropriate ways to secure consent from individuals whose data is used to train the AI model.
- **Change and operate**. A chatbot (an Ai application that can include cognitive language capabilities, learns behaviors that are inappropriate or offensive to customers.

Furthermore, Stanford has identified 10 areas of AI that are major concerns and are open to debate.

1. Privacy and Surveillance,
2. Manipulation of Behavior
3. Opacity of AI systems
4. Bias in Decision Systems
5. Human Robot Interaction
6. Automation and Employment
7. Autonomous Systems
8. Machine Ethics
9. Artificial Moral Agents
10. Singularity (Stanford, Stanford, 2020)

CONCLUSION

Information technology is essential to the lives of people around the globe and is a global phenomenon. These technologies many different types of forms and exists in every facets of our lives. All these technologies have some computational power at their core and humans' interface with them mostly through applications and operating systems. These technologies are opening up many new ways for humans to interact with each other as well as advances in communication, Information technology has also had a major impact on philosophical discussion of logic, ethics and law giving rise to new sub-fields in fields of applied ethics, logic and law. Moral challenges are ever present in the fields of Information Technology and this summary focuses on four major areas: piracy, data protection and privacy, ransoms and ransom ware and AI ethics. These four serves as a major starting point into the field of Information Technology Ethics and are essential for IT Managers and CTO's. According to Stanford, further moral challenges include information recording, communication and accessing information, organizing and synthesizing information, cultural issues, social media networking, online and virtual games, transparency, artificial life, and information technologies role in moral discovery, moral systems and moral agents. Through-out the summary many of these issues are addressed although briefly and require a much more sophisticated discussion and exploration which is yet to come as the field of Information Technology advances and grows. (Stanford, Stanford, 2020)

Bibliography

Deloitte. (2020). *Deloitte* . Retrieved from Deloitte : https://www2.deloitte.com/us/en/pages/regulatory/articles/ai-ethics-responsible-ai-governance.html

GDPR. (2020, September). *GDPR*. Retrieved from GDPR: https://gdpr.eu/what-is-gdpr/

Green, B. P. (n.d.). *Santa Clara, Technology Ethics*. Retrieved December 2020, from Markulla Center of Applied Ethics: https://www.scu.edu/ethics/focus-areas/technology-ethics

Industry, C. S. (2020, September). *Ransomware Guide.* Retrieved from Cyber Security and Infrastructure Security Industry: https://www.cisa.gov/publication/ransomware-guide

Machinery, A. o. (2020). *Association of Computing Machinery*. Retrieved December 2020, from Association of Computing Machinery: https://www.acm.org/code-of-ethics

Shoup, T. E. (n.d.). *Santa Clara University .* Retrieved from Santa Clara University : https://www.scu.edu/mcae/publications/iie/v8n3/faqs.html

Stanford. (2020). *Stanford* . Retrieved from Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/it-moral-values/

Stanford. (n.d.). *Stanford* . Retrieved from Stanford : https://plato.stanford.edu/entries/ethics-ai/

Efraim, Turban, Pollard Carol, Wood Gregory, Information Technology for Management, 11th Edition.

Weedmark, D. (2018, November). *Small Business Chron*. Retrieved from Small Business Chron: https://smallbusiness.chron.com/ethical-dilemma-use-information-technology-18366.html