Word Count: 1570

Throughout the long course of human existence, adaptation and innovation have been some of the core principles that have driven society to where it is today. As a result, we have seen the birth of a myriad of technologies ranging from the creation of fire to the advanced manipulation of subatomic particles. Yet as history has shown, these technologies have the potential to not just aid society but also tear it down. Even something as simple as fire has the ability to enable the destruction of years of invention. However, the past century has given rise to a new technology that has changed societal norms drastically and may be one of the most influential technologies to date. Computer technology is like fire in that it has the potential to benefit or damage society, but perhaps on a much larger scale. The vast complexity of computer technology makes it necessary to look at the various aspects of the technology and how the creator of this technology, computer science professionals, must be responsible in order to ensure that the technologies they create results in society's betterment.

One of the first areas to look at is the relatively modern subject of machine autonomy. With the rise in autonomous devices such as driverless cars it must be considered how exactly these devices make their decision. For instance, the choice of a driverless car to hit one person over another, is an algorithm designed by the computer scientist. As such, it becomes possible for computer scientists to either unconsciously or consciously replace the user's judgment with their own via the autonomous system. It is the responsibility of the designer of such systems, the computer scientist, to ensure that the absolute replacement of the user's judgment is not an issue, and properly consider ethics in their design. A potential solution is the design systems to inform the user better rather than replacing all their decisions.

Another critical field to consider is the general safety of computer systems to the user. Many computer technologies in the world can easily affect human lives to an extreme degree. For instance a

plane navigation system can cause the death of hundreds of people if it malfunctions. In particular, if this system is not rigorously tested and approved before usage it provides an even greater risk to its users. It is an easy decision to cut corners in such a manner in favor of time and costs. Therefore, it is the role of computer scientists to overall take into consideration the safety of the users. This could be done by ensuring the good of the technology outweighs any harm, informing users of the risks, distributing the benefits and burdens of the technology, and minimizing the risk to the user through proof and testing.

As computer technology begins to pervade every aspect of our life, privacy also becomes another important issue. As our information is being controlled by software from other companies, it becomes increasingly easy for these companies to use our information to their benefit. For instance, in the case of the Barbie doll, it recorded and stored children's words and gave this intimate data to 3rd party vendors. For this reason, in the newer generations of such devices they should be subject to much higher levels of regulations on what data can be collected. They should respect people's right to solitude, intimacy, and reservation as this is what allows users to trust companies, computer scientists, and the computer technologies they create.

However, this trust in companies also applies when data is voluntarily provided by users. When user's choose to use computer technologies to store information, they trust that the computer science professionals have designed the technologies such that the security of their data is of the utmost priority. Therefore, it is a computer scientist's responsibility to ensure that they develop products that protect the user's data and do not expose them to any unwarranted risk. Passwords are a foundational example of this issue. Computer scientists often design technologies that emphasize ease of use, such as exceedingly simple passwords, password recovery systems, and passwords wallets. However, these technologies place the user at more risk, and makes it easier for confidential information to be stolen.

Therefore, it becomes necessary for computer scientists to find the balance between good security and user satisfaction.

While data privacy and security are new concepts brought about by computer technology, a concept that has existed far longer is that of intellectual property. However, the birth of cyberspace makes the conditions for intellectual property more unclear. For one, computer technology makes the act of copying very easy, as is evidenced by the vast amounts of pirated media on the internet. The more problematic issue is that computer softwares is not well defined by existing patenting laws as they are built for a function rather than with a specific structural design. As classic patent law doesn't properly apply to software, it becomes simple to repurpose other's work. Even large companies such as Facebook have abused this in the past. Ownership is important as it is what drives innovation and creation, which benefits society as mentioned before. This is why computer science professionals must develop a new category of patent to cover software and protect software ownership. Whether it is preexisting, technical, or emergent bias,

The stealing of software intellectual property has certainly gone under the radar on numerous occasions, but a much more hidden issue is the bias that is often found in computer systems. It is altogether very easy to introduce bias into a system, whether it is because of the reference material or of the creators own volition. An example of the National Resident Match Program, which systematically favored the decision of the hospital programs over the medical students in cases of conflict. Another more everyday example would be certain apps having reduced functionality for colorblind individuals. Therefore it is important for computer scientists to design systems that actively minimize bias.

In order to create such systems, however, extensive research is required, and is yet another circumstance in which computer scientists must take caution. When conducting research of any sort, it is important to consider the rights and safety of the participants. The issue, however, is that some computer technology research often puts participants into negatively aroused emotions. For instance research assessing intrusion detection or viruses may result in distressed participants, which goes against the principle of ethical research. For this reason, it is the role of computer scientists to ensure that participants have full knowledge of the study they are a part of and are able to leave the study whenever they choose to.

Overall, many of these issues stem from a lack of regulation, and arguably the most critical area for regulation is the internet. Abuse on the internet is made overly simple because of the anonymity it provides. An excellent example for this is the realm of video games. In video games, there is abundant opportunity for cheating, griefing, cyber bullying, offensive texting, and even threats. These may be considered meaningless because they are simply in a virtual world, but in reality they can definitely affect the player in real life by evoking real, harmful emotions. As such, it is a critical responsibility for computer science professionals to construct the internet and by extension video games, to protect its users from these types of problems.

Finally, one of the potentially most devastating issues with computer technology is that of cyber warfare. While many countries find a need for warfare to promote their values in the world, cyber warfare has changed the field on how war can be conducted. In the past the Just War Theory has been used as a guideline for warfare. However, the Just War Theory is inadequate for the non-physical nature of cyber warfare, which allows for abuse within warfare. For instance, the erasing of data fits within the guidelines of the Just War Theory, yet it seems common sense that this can severely damage a

population's safety. Therefore, it is the role of computer science professionals to construct a set of guidelines befitting cyberwarfare, in order to mitigate the damages that can be caused in such warfare. An example of this can be by combining the Just War theory with Information Ethics.

In conclusion, the study and application of Computer Ethics are indispensable for every computer science student aspiring to contribute to a utopian world rather than succumbing to the pitfalls of an "iron cage." The rapid evolution of technology amplifies the impact of ethical considerations, making them a cornerstone of responsible innovation. By instilling a strong foundation in Computer Ethics, students become not just proficient coders but conscientious architects of a better future. In a world where trust, inclusivity, and sustainability are paramount, ethical awareness safeguards against unintended consequences and fosters a culture of responsibility. The call for a utopian vision is not an abstract ideal but a pragmatic necessity in the tech-driven landscape. Computer science students, armed with ethical principles, play a pivotal role in shaping a society where technology serves as a force for positive transformation. This ethical lens ensures that advancements align with societal values, breaking free from the constraints of an "iron cage." In essence, the study and application of Computer Ethics empower students to be architects of progress, contributing to a harmonious and enlightened world where innovation and responsibility coexist for the greater good.