Assignment on Challenges at the Intersection of Law and Technology for CS50L

Total points 9/10 ?

Starting in 2021, all assignments in CS50L are out of 10 points. A score of 7 points or better (70%) is required to be considered to have "passed" an assignment in this course. Please do not resubmit an assignment if you have already obtained a passing score. You don't receive a final grade at the end of the course, so it will have no bearing on your certificate, and it will only slow down our graders!

Unlike CS50x, assignments in this course are graded on a set schedule, and depending on when you submitted, it may take up to three weeks for your work to be graded. Do be patient! Project scores and assignment status on cs50.me/cs50l (e.g. "Your submission has been received...") will likely change over time and are not final until the scores have been released.

Email *

maz786@outlook.com

Name *

Mazafer Ul-Raqib

edX Username *

Mazafer

What is your GitHub username?

You only need to tell us if you are concerned about checking your progress in the course and/or you want a free CS50 Certificate after you satisfy all of the requirements of the course. If you do not already have a GitHub account, you can sign up for one at https://github.com/join. You can then use this account to log in to cs50.me/cs50l to track your progress in the course (your progress will only show up after you have received at least one score release email from CS50 Bot, so do be patient!). Don't worry about seeing a 'No Submissions' message on submit.cs50.io, if you find that. The course collects submissions using Google Forms, and only the gradebook on cs50.me/cs50l is important! If you do decide to provide us with a GitHub username, BE CERTAIN IT IS CORRECT. If you provide the wrong username, you will not be able to see your scores.

https://github.com/maz786

This course is graded by human graders, and has a ZERO TOLERANCE plagiarism and collaboration policy. If *any* of your answers are copied and pasted from, or obviously based on (a) an online source or (b) another student's work in the course, in *any* of the course's ten assignments, you will be reported to edX and removed from the course immediately. There is no opportunity for appeal. There are no warnings or second chances. *

It is far better, we assure you, to leave an answer blank rather than risk it. This may be an online course, but it is offered by Harvard, and we're going to hold you to that standard.

● I understand this policy and agree to its terms; I hereby affirm that I will not plagiarize any answers or collaborate with any other students in this course .

✓ In "Reflections on Trusting Trust," how does Ken Thompson illustrate the idea that a computer can "learn"? 1/1

https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf. Note that the Figures 2.1 and 2.2 are out of order in the original paper!

In "Reflections on Trusting Trust," Ken Thompson uses the example of a Trojan horse that a malevolent programmer inserts into a computer system's software to demonstrate the idea that a computer may "learn." A programme known as a "Trojan horse" has a trustworthy appearance but secretly contains harmful code that can jeopardise the system's security.

According to Thompson, a computer needs to be able to run code and draw conclusions from that execution in order to be able to "learn." This means that even if it is unfamiliar with the specifics of the code it is running, the computer must be able to trust it.

Thompson uses the example of a malevolent programmer creating a Trojan horse to infiltrate the software of a computer system to demonstrate this idea. This Trojan horse is intended to alter the system's compiler, which is a programme that converts code that can be read by humans into code that can be read by machines and executed by computers.

The Trojan horse programme functions as a "back door," a covert entryway that permits illegal access to the system, in the system's software. The Trojan horse programme executes when the compiler is run, changing it to incorporate a secret code that enables the malicious programmer to enter the system without authorization.

This scenario serves as an example of how a computer can "learn" by being able to run code and make decisions in response to that execution. In this instance, the computer has become infiltrated because it has come to trust the Trojan horse application.

Thompson does point out that this situation is not just confined to Trojan horses and malicious malware, though. He contends that any software system that is intricate enough to be practical would also be intricate enough to have flaws and weaknesses that an attacker may take advantage of.

Thompson suggests a multi-layered approach to trust, in which certain system components are segregated and are only trusted to carry out particular duties, to reduce this risk. This lessens the chance that the system will be compromised by a single vulnerability.

Overall, Thompson's "Reflections on Trusting Trust" serves as an example of how a computer may "learn" by running code and drawing conclusions from that running. It also emphasises how important it is to exercise caution when asking a computer to execute code because such code can have flaws or other issues that jeopardise the system's security.

✓ Machines lack the ability to think critically, so how does "machine bias" come to be? What are some consequences of it in the legal system? 1/1

Machines are incapable of independent cognition and judgement, which prevents them from being able to think critically. They lack the capacity to weigh the implications or effects of their actions in the same way that a human would because they are programmed to carry out specific jobs based on the instructions they are given.

As a result, when robots are created or taught using biassed data or methods, they are more likely to exhibit "bias." A machine learning method, for instance, may provide biassed results when used with new data if it was trained on a dataset that was skewed or unbalanced in some way. Numerous negative effects, such as prejudice and unfair treatment of people or groups, may result from this.

Machine bias can have major repercussions in the legal system. For instance, if a machine learning algorithm is used to forecast a criminal offender's chance of recidivism and the algorithm is trained on data skewed against particular groups (like racial or ethnic minorities), it may give biassed predictions that result in unfair treatment of those people. Even if the offender is not at a higher risk of committing a new crime, this could involve harsher punishments or more frequent surveillance.

Other aspects of the legal system, including the use of facial recognition technology to identify suspects, are subject to machine prejudice. The technology may provide inaccurate or biassed findings if it is trained on a dataset that is not representative of the population, which could result in false positives and potentially improper convictions.

It is crucial for designers and developers to be aware of potential sources of bias in their data and algorithms and to take actions to reduce or eliminate those biases in order to avoid the possibility of machine bias. In order to understand and assess the decision-making process, this may entail employing more representative and diversified datasets as well as accessible and comprehensible methods and systems.

✓ The Intel Management Engine interacts with your system via the BIOS. Read up on what a BIOS is, and in a few sentences in your own words, describe its function. 1/1

A chip on a computer's motherboard has firmware called the BIOS (Basic Input/Output System). Its primary duties include loading the operating system from the hard drive into the computer's main memory and initialising and testing the hardware components of the system during the boot process.

Many Intel chipsets contain the Intel Management Engine (IME), a separate processor. It functions independently of the primary CPU and operating system as a hardware-based component. It utilises its own firmware and Minix, which is its own operating system.

Various types of system management tasks, including power management, hardware monitoring, and remote management, are provided by the IME. The Baseboard Management Controller and other hardware elements, such as the BIOS, allow it to connect with the rest of the system (BMC).

The BIOS initialises the IME and gives it control during the boot process. The IME then assumes control and completes a set of initialization and testing procedures all on its own. The BIOS then takes over and continues the boot process and loads the operating system when the IME has finished its responsibilities.

The IME keeps running in the background and does its numerous management tasks after the operating system has finished booting. Through remote administration tools, it can also be accessed and managed by system administrators or service personnel.

✓ When we use the term "net neutrality", what exactly do we mean? 1/1

Net neutrality is the idea that Internet service providers (ISPs) should permit access to all material and applications without discriminating against or restricting any particular websites or services, regardless of the content's source. As a result, ISPs shouldn't be permitted to deliberately impede or limit access to any website or service or charge a premium for quicker access to specific websites.

The principle behind net neutrality is that everyone should have equal access to the same information and resources on the Internet, creating a level playing field. This is significant because many people now depend on the Internet as a primary source of information, a means of communication, and a portal to a wide range of services.

The fact that it encourages competition and innovation is one of the main justifications for net neutrality. Without net neutrality, ISPs might block or stifle access to particular websites or services, giving their own products or those of businesses willing to pay for speedier access an unfair advantage. This might reduce consumer choice and impede competition.

The significance of net neutrality for the freedom of expression is a further justification for the policy. Without net neutrality, ISPs can potentially restrict access to particular opinions or censor particular types of content, which would be detrimental to free expression and the free interchange of ideas.

The protection of net neutrality may be at danger in a number of ways. One method is the development of "fast lanes" or "paid prioritisation," where Internet service providers (ISPs) charge websites or content providers for consumers' speedier access. A two-tiered Internet might result from this, giving those who can afford to pay for speedier access a competitive advantage over those who cannot.

The practise of "zero-rating," in which ISPs provide access to some websites or services for free but charge for others, poses a further risk to net neutrality. As a result, only a small number of websites or services might be broadly accessible to people, while others might be effectively restricted or made less accessible.

Several initiatives have been made to uphold net neutrality, both domestically and internationally. The Federal Communications Commission (FCC) in the United States approved net neutrality regulations in 2015, but these regulations were eventually abolished in 2017. Net neutrality has been the subject of continuous discussions and legal disputes in the US, and it is still a contentious and contentious issue.

Numerous initiatives have been made to advance net neutrality and safeguard Internet freedom on a global scale. Strong net neutrality regulations have been established by the European Union, and nations like Canada and India have also taken action to prevent ISPs from discriminating against particular websites or categories of material.

In general, the principle behind net neutrality is that everyone should have equal access to the same information and resources on the Internet and that ISPs shouldn't have the power to ban or slow down access to specific websites or services. This is critical for safeguarding free speech while also encouraging competition and innovation.

✓ In no more than three sentences, explain why a developer may be inclined to license her code under the MIT license or something similar (such as the BSD-3 or BSD-4 license). 1/1

The fact that MIT and BSD licences are liberal, allowing users to use the software for any purpose and distribute it however they see fit, may influence a developer to use them. This is because the original copyright notice and licence terms must still be included. Additionally, these agreements do not demand that users distribute any software modifications they make. This enables the software's creator to maintain ownership of their creation while also enabling unrestricted usage and distribution by others.

Gottschalk v. Benson

Read the United States Supreme Court opinion Gottschalk v. Benson, an early opinion on the patentability vs. copyrightability of software and algorithms. The next question relates to the algorithm in question in that opinion.

https://caselaw.findlaw.com/us-supreme-court/409/63.html

✗ Convert 010100010010 from BCD to hexadecimal. 0/1

Recall that the place values for hexadecimal numbers are ...256, 16, 1, rather that decimal's ...100, 10, 1. Recall also that we typically preface hexadecimal values with "0x".

0x512 ✗

Correct answers

0x200

200

✓ In no more than three sentences, how does a genetic algorithm operate? 1/1

An optimization technique called a genetic algorithm takes its cues from the course of natural evolution. Recombination, mutation, and selection are used to iteratively improve a population of potential solutions in order to make them better each time. The most successful candidates are more likely to be chosen for reproduction at each iteration, and the offspring are then employed to replace the population's less suitable individuals. Until the population reaches an acceptable level of fitness, or until a predetermined number of iterations have been carried out, this process is repeated.

✓ The "Guns, Limbs, and Toys..." article presents a hypothetical 10-parts framework for dealing with legal issues created by 3D printing. Based on your studies in this course and others, select any two (2) of those parts. For one, identify a reason why that part of the framework should be workable. For the second, identify a reason why that part of the framework should NOT be workable. 2/2

There is not a specific right answer that we are looking for with respect to any of the ten parts; rather, we want you to dig into them a bit deeper into identifying unarticulated benefits or detriments with this proposed approach. Feel free to really flex your legal muscle here. https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1408&context=mjlst (Pages 826-830 in the original document). Please be sure to explicitly identify which two (2) parts you are choosing by identifying them with their corresponding number from the article ((1) through (10)) and be sure you are making explicit whether you believe that part to be WORKABLE or NOT WORKABLE in your write-up.

The article "Guns, Limbs, and Toys..." offers a fictitious 10-part structure for addressing legal difficulties brought on by 3D printing. Part (2), "Building a comprehensive 3D printing database," and Part 9, "Building a system of licencing and certification," are the topics I'll be covering.

I'll start by explaining why building a comprehensive database for 3D printing, which is part of the architecture, should be feasible. According to this section of the architecture, a database should be established that contains the blueprints and technical details for each 3D-printed product. Because it permits the traceability of 3D printed things, this component of the framework ought to be feasible. The database would make it possible to track down an issue with a 3D printed object, such as a flaw or malfunction, and determine who created it in the first place. By highlighting designs that have previously created concerns, this would make it easier to find and fix any problems and maybe even prevent them from happening again.

I'll now go over why developing a system for certification and licencing in section (9) of the architecture would not be feasible. According to this portion of the framework, a system should be established for certifying and licencing 3D printed items, much to how traditional produced goods are controlled. This aspect of the framework could not be feasible since it might be challenging to successfully enforce. Traditional manufacturing often has a centralised manufacturing process that can be monitored, making it simpler to oversee and implement licence and certification requirements. As a result of 3D printing, it is more challenging to monitor and enforce licence and certification requirements because things can be made by individuals or small organisations using their own equipment.

Additionally, it could be challenging to keep up with and properly control new designs and materials given the quick speed of technological innovation in the field of 3D printing.

✓ Do you think we should treat potential crimes or civil infractions differently based on whether they happen in augmented reality versus "reality"? What about virtual reality versus "reality"? Why or why not? 1/1

There is now substantial discussion over how potential criminal or civil offences that take place in virtual or augmented reality should be handled differently from those that do so in "reality." The nature of the infraction, the harm done to people or society, and the likelihood of enforcement are only a few of the variables to take into account when deciding how to address such instances.

The possibility that crimes or violations committed in virtual or augmented reality may not have the same repercussions as those committed in "reality" is one justification for treating them differently. For instance, a virtual theft could not cause the same level of monetary loss or psychological distress as a real theft. The victim of an augmented reality assault might not sustain any physical injuries. Some people think that less harsh penalties should be applied to these kinds of offences as a result.

Others counter that crimes or transgressions committed in augmented or virtual reality can nonetheless have serious repercussions. Virtual theft, for instance, might result in the loss of virtual assets that may have real-world worth. Virtual bullying or harassment, for instance, can lead the victim to experience severe mental pain. Additionally, it is frequently possible to identify the perpetrator of crimes or infractions that take place in virtual or augmented reality, making enforcement easy.

The type of the offence is another thing to take into account. Whether they take place in virtual or augmented reality, some crimes or transgressions, like murder or sexual assault, are widely seen as significant acts that need to be punished. Other acts, such virtual vandalism or the theft of virtual goods, can be considered less serious and hence call for a different course of action.

Ultimately, the ideals of justice and fairness should be used as a guide for deciding how to handle crimes or transgressions that happen in virtual or augmented reality. This may entail taking into account the harm brought on by the offence, the likelihood of enforcement, and the possible outcomes of various actions. To choose the best course of action, it might also entail asking professionals and the impacted community for their opinions.

Debrief

About how many MINUTES would you say you spent on this assignment in total? *
Just to set expectations for future students.

666

This form was created inside CS50.

Google Forms