Chapter 3 Discussion: Software Development problems. - Group B

Methods of development are in flux, and open source software is a fairly new concept to the world of software engineering. An article at the website InvestInTech, Pros & Cons of Open Source in Business, explores the benefits and caveats of using Free and Open Source Software, and leaving the reader to decide whether the pros outweigh the cons. One initial promise of credibility is the use from large corporations such as Amazon, IBM, and Google. Each of these companies are seen as a leader in the software world, and many would like to follow in their footsteps. The reliability of open source software comes from the multitudes of developers that can contribute to its constant evolution, guaranteeing reliability from professionals with interest in the project. However, should interest wane in the software, it could become orphaned and no longer updated, making it somewhat risky to depend on over a long period of time. In this time frame, cost may seem non-existent as the software is free, but it is worth noting that there is no obligated or dedicated support for such software, resulting in potentially unexpected labor or contracting costs. Even though the software may be powerful, it may not be designed for the unskilled end-user due to coming from a number of developers with specific intentions and solutions in mind. The final risk to open source software is a malicious developer that may attempt to sneak in malware to the project. Though it may usually be caught, there’s no guarantee of the software’s security. It is ultimately up to an individual or team to decide which avenue to take when it comes to the use of open or closed source software.

Many are aware of the startling amounts of information a company may gather on its consumers, but a lesser known fact is the lengths that those companies can and will go to obtain it. In the video Data Mining, by ABC’s The Checkout, examples are explored that reveal an undesirable truth to the world of private data gathering. Companies such as Target have developed ways to analyze a consumer’s search and purchase history to determine if and how pregnant they are. Some methods aim to gather data when the consumer isn’t aware, such as a GPS acquiring a voice signature of its user. Others perform this trickery in a way that promise to benefit the consumer, such as a rewards card that is designed to obtain and sell information. The Checkout suggests ways that one can minimize the invasion of companies by turning off location services, not signing up for rewards, and preventing some tracking through using cash for purchases and software that disguises one’s search history, such as a Virtual Private Network.

Apple’s CEO, Tim Cook, expresses that it should not actually be the responsibility of the consumer in the Time article You Deserve Privacy Online. Here’s How You Could Actually Get It. Cook pushes for legislation that should be derived from his four principles of consumer privacy. The first is a right to personal data gathering being as minimal as possible. The second is a right to know what that information is and why it is being held. The third is the right to access, change, and delete that information being stored. The fourth and final principle provides a right to data security, implying that a consumer should be protected from data auctions and breaches. It never should have been the responsibility of the consumer to address this issue, but it is one that must be tackled to guarantee user privacy in a world being more technologically connected by the day.

Marketing first began as a way to direct the attention of consumers to a product, but through online tracking has become a way to make you the advertisement. In its video Online Advertising, CrashCourse explains how advertising initially attempted to capture a contextual environment for its ads, placing where they expect consumers to be. Thanks to the internet, now a website can track someone and have its advertising follow you wherever they go online. Websites now collect information on what a consumer clicks, watches, comments, and creates to determine what content would be most effective at targeting them. This results in
two consequences. Even though the user may get relevant content, websites gain rights to a user's content in such a way that they can sell and do with it as they please through a deceptively bland terms of service. Now a great deal of content will be hidden from the user in favor of what a company pays you to see. The second consequence is best quoted directly from CrashCourse’s video: “if something is free, you’re the product.” Due to all of this acquirement of data and an agreement in terms of service, websites can deliver everything about a user’s behavior to a company that would happily pay to turn a profit from targeted advertising. It is advised that all people be cautious in their online behavior as normal content and advertisements are starting to become indistinguishable from one another.

YouTube channel CrashCourse explains some of the basics of machine learning and artificial intelligence in their video [Machine Learning & Artificial Intelligence](https://www.youtube.com/watch?v=Machine_Learning_Artificial_Intelligence). Thanks to many advancements, aggregating data with the use of computers has become incredibly efficient and reliable. For the past 50 years, however, computer scientists have been working to develop systems that not only gather data, but make decisions with data as well. This can begin with as simple of an example as determining the species of a butterfly given some classifications, but can extend to more complex uses like driving cars, diagnosing patients, translating speech, and facial recognition. Despite the incredible function of these, they are considered “weak AI” as their purpose is narrowed to a single process. More sophisticated artificial intelligence has been hypothesized as “strong AI” that aims to mimic and reproduce human-like behavior. Some believe it to be impossible, but CrashCourse demonstrates that a program can gather and analyze data quicker than humans, and this data could be how humans react to stimuli, environments, or situations. A prime example of this would be IBM’s Wilson, a program featured on Jeopardy that was able to quickly receive data and output a question to match a statement given to it and other humans. This method of analyzing human knowledge and behavior is similar to how humans learn, and could produce some surprisingly human decisions from machines.

The United States Patent and Trademark Office (USPTO) has created a document detailing some of the false and illegal practices that invention promoters use to scam potential inventors. It is titled [*Protect Yourself Against Invention Promotion Scams*](https://www.uspto.gov/). Its details are important to all individuals who create their own work that they may wish to market, not exclusive to quirky as-seen-on-TV inventions. One should be wary of fees before the promotion itself, implying that one’s invention need to be analyzed for hundreds of dollars. Additionally, any and all guarantees are likely false, as no patent can ever be guaranteed through the patent office. Applying for a design patent, while similar, does not actually protect the operation of one’s product, and such advice should be avoided. A few other common practices for discerning scammers are also provided, such as not being able to contact anyone at the office, refusal of references or hired references, and insistence on forms or agreements without the approval of a personal attorney. It is important to know which legal protections one may have, as well as the requirements instilled upon invention promotion firms. Each firm must disclose the number of inventions that have evaluated, including the positive and negative results of each. The total number of contracts within the past five years must also be provided, as well as the total number of customers who received a net financial profit or licensed agreements resulting from the firm’s services. Lastly, names and addresses of previously the firm’s affiliated companies and persons are required. Each of these pieces of information are required, by law, to be made available to one seeking a contract with an invention promotion firm.

In an interview with Oregon State University’s Tom Dietterich titled [*Promise and Potential Peril*](https://www.youtube.com/watch?v=Promise_and_Potential_Peril), the professor of Computer Science covers some important topics and conversations to consider when developing and maintaining artificial intelligence (AI). He first notes that AI usually operates best when it accompanies a human, such as a Google search in which a human determines if it understood the query correctly. With this in mind, Dietterich transitions into the topic of autonomous AI. He declares that the
technology for this field must be incredibly robust in conjunction with a strong culture of high standards, safety, and testing. It is rare for developers to cover every single situation when it comes to a program, hence why apps often crash. These unanticipated situations and interactions are key to understand where, when, and how to implement AI. Dietterich is focusing on human-robot interaction at the university, and some considerations made are whether or not it is safe to interact with a particular robot. This kind of thinking places even greater importance on the development of the AI itself, and to facilitate robotic behavior that can be interpreted by humans to create the communication channel between AI and user. Teams at OSU are also focusing on other ways to improve this interaction, such as working on “soft robotics” that use materials that are less harmful to humans should something go wrong. Overall, Dietterich emphasizes how powerful AI can be in conjunction with a human, how ideally they could operate independently, but also how dangerous this situation can be without an extreme degree of care.

Reply to another student (which includes research about one aspect of their topic):

On the topic of data privacy, I discovered a report published by the Parent Coalition for Student Privacy and The Network for Public Education titled [The State Student Privacy Report Card](#). Within, each state was graded on a traditional A-F scale for how well each group of state-operated schools did in compliance with around 99 laws pertaining to student and parent data privacy. It involved what schools can and cannot do in regards to data being created and aggregated, especially with how they collect and disclose it. Seeing as to how much of an issue data privacy is for consumers, it's concerning to see the issue may trickle over to government entities and people (children, especially) who use them. Although I believe there should be more focus on organizations and companies that abuse the collection and sale of data, I think protection and prevention is the next step. It's worth noting that not one state received an A in this report card.