- What skills are unique to the profession of computing?

"Computing" is a broad field which encompasses concepts related to mathematics, engineering, electronics, philosophy, linguistics, etc. however these all remain distant relatives to computing. In order to be successful in computing one must be able to create, update, and test mental models of the computing systems they're working with. Additionally there's a degree of planning the systems which requires knowledge of the tools and techniques in order to create well designed systems.

- What does it mean to be a "professional?"

Being a "professional" means to do something as a career and doesn't necessarily have any bearing on actual skill/capacity. So for example someone can be so good at golf that they consistently beat Tiger Woods or whoever is the best golfer, but if they don't make money doing it they're not a "professional." Furthermore, one can be a "professional" software engineer or developer but not know basic data structures and algorithms just by having a job in the field.

- In what ways do you see the "typical" computing job as professional?, and in what ways is it not?
    There are many jobs which are indirectly related to 'computing.' For example a friend of mine worked at a company where the majority of the employees were physicists and RF engineers. One of the physicists created a model which would generate relevant charts given different user-defined variables for inputs, design considerations, etc. and in order for them to find the 'optimal' values for all the different variables they had one employee spend the better part of the week adjusting the 31 different variables using individual sliders. Although you could argue that this employee was employed in the field of 'computing' because he did create the model using tools, libraries, and code, the reality is that the majority of his week was wasted as a professional would have worked smarter by creating better tools.

- If an AI system "does harm," did it violate a code of conduct?, did anyone? Explain.
    Upon the deployment of an AI system one can easily apply a "code of conduct" for it to live by and if that standard is violated the AI's deployment can be reconsidered. One should contractually obligate the developers/subcontractors of the AI product to be responsible for violating a set of rules. Assuming breaks the rules the user would then be able to collect a settlement replacing any damages. Assuming the rules are impossible to achieve with current state of technology, either the risk vs reward ratio (ie - settlement value * rate of failure * expected lifetime / (contract rate - development cost)) would warrant the contract regardless or no one will accept the contract and the product will not be developed.

There are two classifications of harmful applications of AI, and they are not well defined, with classifications varying depending on the individual's own belief systems and faith in the technology and authority figures. The first classification is intentional use for an application which causes harm. This would be like having an AI system which detects people who are hot and sprays them with water to cool them down. The developer might imagine that it's helping people and saving lives but it's only a matter of time before someone gets wet and mad leading to lawsuits.

The second classification is for AI systems which have acceptable applications but are poorly implemented, resulting in harm. This is more difficult to hold someone accountable as the specific incorrect behaviors could be argued as the responsibility of a myriad of developers ranging from individuals at a company to developers of software libraries and operating systems who could be anonymous. However considering the majority of software is written by companies who are held accountable for any mistakes made, any **direct** harm done to the consumer is typically minimized.

- What does the rampant spread of disinformation on social media tell you about the effectiveness of codes of conduct in the computing profession?
    - Misinformation: wrong, but not malicious
    - Disinformation: Intentionally deceptive and incorrect

Among others, the Russian government has been spreading massive volumes of fake news in various forms since the cold war. It's just now that we've been able to fact check it rapidly. There are several problems at play here which are not the responsibility of computing. It is physically impossible to eliminate fake news.

If you take a look at most fact checkers today they've become completely detached from reality and arguably just as bad as the people producing the fake news in disseminating their own opinion instead of objective facts, using tactics like marking statements which are true in their entirety as "only partly true" or worse because the individuals responsible for the judgement don't like the reality or don't agree with it politically/socially/economically/etc. Another portion of the problem is the fact that the internet gives individuals the ability to publish onto the same platforms as large, edited, verified publications. Resulting in obvious violations of the norms of journalism.

One important skill which unfortunately is not taught by most schools as it's very hard to teach is digital literacy and knowing to look at the context and attempt to understand the situation more clearly before making statements or acting on the information.

One seemingly innocent example of misinformation, people on twitter will take a picture of the article title and image instead of sharing the actual article making the end reader have to independently verify the article's authenticity. Although one would argue that this is a result of the user being more likely to read a picture than click a link or restrictions of other platforms they also post to, the reality is that news companies often correct article titles, images, stories, etc. as more information is available or after discovering a breach in journalistic integrity. Many newswires have automated systems which produce articles based on events such as seismometers which trigger earthquake stories or other alert systems. Which then go to

publishers who likely don't verify the validity of the data they are given and produce a story out of it. Although none of this is malicious in intent it's results can be the same