Noah Baker

ITP 125 – Final Paper

One of the most significant issues in my life involves keeping one person away from me. The current measures for doing so only go into effect after contact has been made between me and the individual – there is no preventative guard. That being said, I think it is possible to develop a system which lets me know of their whereabouts. This is when an ethical dilemma comes into play.

Setting boundaries is one of the hardest aspects of developing a just security system. The NSA has had major trouble in the recent past with justifying intense monitoring of personal data for security measures. When does knowing a detail about someone become an invasion of privacy? This is the key question I deal with in developing a system to monitor another person without invading their privacy. This brings me to a complex question that I neither have the understanding of development tools used in security or the industry knowledge to understand or know the answer to: Can I gather personal information about a person that is unjust for me to have knowledge of such that the system does not allow me to access said information, yet is able to interpret that information in order that I am warned in a preventative manner? I would love to dig deeper into this question and work on tools that do just security! One way to deal with this is locking the information down such that no one has any way to access it. This could be done by encrypting and decrypting data within a program so that it is only interpretable to the program; never to a developer or user. This problem seems pertinent to an ever-applicable industry, so it could very well be that the ethical guidelines are being written as cybersecurity plays a bigger role in our lives. It is only my first semester taking classes and learning about cybersecurity, so writing this paper makes it clear that I have to dig deeper to understand the status of the cybersecurity industry today.

A book I began reading recently, Startup Nation, covers the innovative nature of Israel. The introductory chapter is about a green Israeli veteran who takes his skills for tracking terrorist activity to a massive corporation and sells his superior algorithm for billions of dollars. His methods are not only faster, but also more accurate. It is amazing that people are working hard to make the world a better place by developing tools that bring justice to people trying to hurt others. However, it is clear that these tools must be developed ethically and securely so that they don’t fall into the wrongs hands. That thought brings up an opportunity for development – designing a system that is able to assign a level of trust to a person. This could be based on something like responses to questions, similar to a polygraph test, but there are better ways to adequately check someone out. Clearly security can be taken in so many directions and it is something I look forward to understanding on a deeper level in the future.