Assignment #8

*CS106E Spring 2018, Young*

In this assignment we take a look at privacy and artificial intelligence. As with previous weeks, this homework consists of reading articles and reflecting on them.

This assignment is due before the start of class Wednesday June 6th – submit it on Canvas before 1:30pm. Additional Administrative Details can be found at the end of this document.

Reading Reflections

Below are a number of articles related to recent privacy and AI issues. Select (4) of the topics and write a short summary and reflection on each. Reflections can include the implications of the issue, your personal stance, and what safeguards could be put in place to mitigate the issue. Each response should be ~250 words, or one page double spaced.

**The General Data Protection Regulation**

https://www.eugdpr.org/the-regulation.html

This regulation is the reason you have been receiving so many emails about updated privacy policies. It is a landmark in online privacy that enforces stricter regulations on companies handling the data of EU citizens.

**Ethics of Autonomous Driving**

https://news.stanford.edu/2017/05/22/stanford-scholars-researchers-discuss-key-ethical-questions-self-driving-cars-present/

https://www.smithsonianmag.com/innovation/ethical-challenges-self-driving-cars-will-face-every-day-180968596/

With a recent slew of accidents involving autonomous or semi-autonomous vehicles, perhaps it is time to re-examine the ethical issues of a computer-controlled vehicle.

**Surveillance in China via Mass Facial Recognition**


China is beginning to implement mass surveillance in its cities by integrating traffic cameras, security cameras, and even private cameras.

**Chinese Social Credit System**


China also plans to implement a social credit system which rates its citizens, granting various privileges for high ratings and penalties for low ratings.
Deepfakes: Generation of Realistic Video via Machine Learning
Neural networks are able to generate realistic video by swapping two people’s faces, raising the question of what can really be trusted anymore.

Bias in Artificial Intelligence
Artificial intelligence systems are a product of the data used to train them. When the training data is biased, this leads to biased systems, such as a racist chatbot and facial recognition systems that struggle with dark skin tones.

Target Pregnancy Prediction
https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html
Target’s machine learning algorithms embarrassingly revealed a woman’s pregnancy.

In-Store Tracking via WiFi Signals and Facial Recognition
https://www.theguardian.com/technology/2016/jan/21/shops-track-smartphone-uk-privacy-watchdog-warns
By combining WiFi location and facial recognition on CCTV footage, stores are able to track movements of customers around a store with pinpoint accuracy.

Big Data and National Security
National security is increasingly concerned with collecting and processing enormous amounts of data, leading to concerns about the rise of a surveillance state within the US.

Equifax Breach
The Equifax breach led to the exposure of more than 143 million Americans’ personal information. While certainly not the largest breach in history, the nature of the data leaked, as well as the fact that many of the affected people are not customers of Equifax, leads to many questions about what right companies like Equifax to be holding data like this.

Ashley Madison Breach
https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked
The Ashley Madison breach led to the exposure of the personal information of users registered on Ashley Madison, a site used to facilitate extramarital affairs. Besides the obvious implications of having one’s association with Ashley Madison revealed, there are also concerns about scenarios in which a victim may have their information falsely inserted into the leaked data.
Facebook and Cambridge Analytica
https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Cambridge Analytica was a consulting firm primarily dealing in data mining and analysis to guide political campaigns. Recent revelations that Cambridge Analytica acquired the data of 87 million Facebook users draws into question both the role Cambridge Analytica had in the 2016 election and whether Facebook should also be held responsible for allowing this data to be used.

Tor
https://www.torproject.org/about/overview.html.en
https://www.wired.com/story/the-grand-tor/
https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

Tor is an anonymous communication system initially developed by the US government. It is often speculated that Tor was made public in order to allow intelligence communication to blend in with regular Tor traffic, as an anonymous network used solely by the intelligence community wouldn’t be very anonymous.

Cell Phone Tracking Around The World

Cell phone communication, as a general rule, is not secure unless explicitly encrypted. This has the consequence of allowing the intelligence community to gather information on targets via a device that people carry around and use for large parts of the day.

Administrative Details

For this assignment, put all reflections in a PDF document. Remember to write both your name and your partner’s name (None if no partner).