A Deeper Look into the Fairness of Diferential Privacy
(Technical Report)

A Virtue Ethics Analysis of the 2013 Yahoo Data Breach
(STS Research Paper)

An Undergraduate Thesis Portfolio

Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia, Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Youssef Errami

May 4, 2020

Table of Contents

Youssef Errami (ye4pg)

April 24, 2020

STS 4600

Socio-technical Synthesis:

My technical work and STS research are connected through the concept of privacy. Where my technical work explores the aspect of fairness with respect to privacy mechanisms, my STS research takes a look at the Yahoo 2013 data breach and analyzes the event from a morality perspective. My technical work consists of experimentation and data gathering, whereas my STS research involved researching and gathering information about the Yahoo data breach through case studies and other experts in the field. Even though my technical work and STS research focus on different aspects, both of these projects are centered around the theme of privacy.

My technical work takes an experimental approach to analyzing privacy mechanisms. This capstone research project focuses on the fairness of differential privacy by analyzing the members of data sets who were exposed by attacks. Differential privacy is a mathematical definition of privacy that is used throughout the privacy-preserving machine learning field. This leads into what I am working on, which is finding out if certain members of a dataset protected by a differential privacy mechanism are exposed strictly because of some characteristic about their data. Throughout the project, I analyzed aspects of the exposed data points in order to determine whether these aspects could have been the reason they were exposed. This research project started in hopes of shedding light on the aspects of fairness with respect to differential

privacy and even though there was nothing conclusive found from this project, it is a step in the right direction towards figuring out the connection between fairness and differential privacy.

My STS research involves analyzing the 2013 Yahoo data breach and the actions that Yahoo and its engineers took that led to them being hacked. My research focused on finding out whether Yahoo can be held morally responsible for the event that took place that led to the biggest data breach in history. I analyzed the morality of Yahoo using a virtue ethics framework in tandem with Prichard's eleven 'Virtues for Morally Responsible Engineers'. My claim is that the actions and decisions Yahoo made throughout its engineering teams reveal notable shortcomings and that they are morally irresponsible. My paper explores this idea in order to help other companies and software engineers learn from the possible mistakes Yahoo made and the moral implications these decisions had so that they don't end up having their own security issues that lead to massive data breaches.

Working on both of these projects alongside each other greatly increased the quality of both projects. My technical work gave me hands-on experience when it comes to dealing with cutting edge privacy mechanisms that high profile companies use currently researching and possibly using on their own databases. My STS research helped me see the importance of protecting user's private information. This allowed me to learn more about how prevalent these data breaches are and it gave me an example of a potential use case my technical work could be used for. In summary, working on both my STS research and technical projects at the same time has allowed me to explore the field of privacy and has allowed me to develop a passion for this field as well.