Using Utilitarian Ethics to Analyze the Equifax Breach of 2017

STS Research Paper

Presented to the Faculty of the School of

Engineering and Applied Science

University of Virginia

By

Ethan Gumabay

February 24th, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date _____

Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

Between May and July of 2017, sensitive information of at least 143 million Americans such as names, birthdays, addresses, and social security numbers was exposed during the Equifax data breach (Gressin, 2019). Equifax, one of the three largest consumer credit reporting agencies in the United States, announced in September of 2017 that the sensitive data of almost 50% of American adults had been compromised. This left half of the American population vulnerable to credit fraud and identity theft. The attack was on a popular web-application software called Apache Struts; though the exploited vulnerability in this system was disclosed in March of 2017, Equifax had not yet implemented the patch at the time of the breach. Many scholars believe that Equifax had an obligation to patch the vulnerability immediately, and its failure to do so led directly to the largest data breach in American history (Newman, 2017). These arguments, however, are generally centered around virtue ethics, the idea that the best ethical decision is the decision which a virtuous person would make. Though it is sometimes difficult to rigidly define a virtuous individual, practicing negligent behavior certainly lies below the universal moral minimum. One of the largest supporting claims to this argument comes in the fact that Equifax did not announce the breach until September of 2017, four months after its occurrence. Virtue ethics, however, is insufficient in analyzing the Equifax breach because it fails to consider the fact that Equifax is not a single human, but instead a collective of humans, each with different ethical values.

I will analyze the Equifax breach through the lens of utilitarian ethics to demonstrate that Equifax can be held morally responsible for the breach of their system in 2017. Specifically, I will illustrate this claim by examining Equifax's actions as they relate to the overall welfare of the public. I will evaluate their adherence to the utility principle, focusing on their failure to

consider the public as a whole with regards to duration and intensity. Failing to consider these facts by evaluating Equifax's actions solely through the lens of virtue ethics puts their actions in a vacuum and overlooks the ramifications of its choices. In order to properly construct this claim, I will also need to tangentially employ the concept of actor network theory to prove that Equifax was a malicious actor and is directly responsible for the overall vulnerability of the network.

Background

Equifax is a large consumer credit reporting agency that collects data, some of which is extremely sensitive, in order to accurately track credit scores of American adults. Information is bought and sold between large companies every day, allowing companies like Equifax to collect data on millions of Americans, even if they do not directly contract Equifax for their services (Electronic Privacy Information Center, 2018). In order to house the large amounts of information necessary to function on such a large scale, Equifax maintained an internal database secure from any outside users (Bals, 2017). One software Equifax used to operate its database was called Apache Struts, a popular web application framework that allows developers to do things like build and manage sensitive databases. In Apache Struts version 2.5.x, there was a vulnerability that allowed for remote code execution (Primoff and Kess, 2018). This meant that by sending a cleverly constructed message to the web server, attackers could trick the server into executing malicious code. This effectively granted them access to the entire Equifax database, ultimately allowing them to steal sensitive data of over 143 million Americans.

Literature Review

Some scholars' analyses of the Equifax breach suggest that Equifax is not to blame for the breach, but instead the rise of technology and inherent lack of security on the internet (Primoff and Kess, 2018). Other scholars fault the public for misunderstanding credit unions themselves. An overwhelming majority of the analyses of the breach, however, employ virtue ethics in order place blame on several individuals or groups of people that were largely responsible for the apathy surrounding the detrimental vulnerability.

According to Sidney Kess and Walter Primoff from the CPA journal, the Equifax breach was a major failure of computer systems' internal control (Primoff and Kess, 2018), removing some blame from the external Equifax-specific factors. In support of this argument, Kess and Primoff argue that air gapped systems with a small number of internet-facing devices have inevitably morphed into broad, complex networks with large numbers of internet-facing devices. As a result of this, a breach such as Equifax's was ultimately inevitable and therefore simply an unfortunate result of technological evolution (Primoff and Kess, 2018). Moreover, they argue that a recent cultural shift to innovation has incentivized companies to move towards producing software as fast as possible and fixing bugs later. This is an inevitable result of the technological arms race which forces corporations to technologically keep up with their competitors, minimizing the importance of software vulnerabilities in publicly available software.

Conversely, other scholars have placed the blame, at least partially, on the public themselves for the breach. Zou and Schuab claim that they found consumers they had interviewed concerning the data breach had very little knowledge of what a credit agency like Equifax actually is, and therefore did not take sufficient protective actions to deal with the perceived risks [of a breach] (Zou & Schuab, 2018). Although Zou and Schuab claim that

Equifax was indeed at fault for the data breach, they note that the fallout was lessened by a widespread lack of understanding from consumers. The risk perception of consumers, or their subjective assessment of the probability that specific event happens and how concerned they are with the consequences, was impaired by a widespread misconception (Zou & Schuab, 2018). This misconception stemmed from a general trust in credit unions themselves combined with a lack of understanding of what personally identifying information credit unions actually have access to.

Perhaps the most popular opinion amongst scholars, however, instead places the blame on Equifax as a collective rather than the inevitable evolution of technology. Hal Berghel from the University of Nevada, Las Vegas claims that Equifax was told of the potential vulnerability in their system in early March, but neglected to patch it until mid-June once they had already been notified of the breach (Berghel 2017). Additionally, Berghel notes that a company with clear, established security policies built on industry best practices that has a trained security staff normally doesn't experience a breach of this magnitude (Berghel, 2017). Drawing attention to the clear, established security policies completely eliminates the possibility that there was any confusion on the Equifax security team regarding standard operating procedures. Moreover, directly referencing the trained security staff of Equifax suggests that the fault for such a breach lies at a higher level than the security staff, most likely the company leadership itself. Like Berghel, many scholars conclude that the breach could have been prevented with competent leadership and a effective incident response team.

Most scholars conclude that Equifax was the primary party at fault for the massive data breach it suffered in 2017, though some believe there were other factors at play which may have been inevitable. Though these scholars do blame Equifax for the data breach, they fail to

consider the overall utility of the data breach. My analysis will focus on the specific ethical violations committed by Equifax in terms of utilitarian ethics. This will ultimately shed light on the extent to which the Equifax data breach caused permanent damage to American society. Equifax at no point considered the overall welfare of society as a whole, and instead prioritized its own wellbeing.

Conceptual Framework

The morality of the Equifax breach can be analyzed using the theory of utilitarian ethics. The number of stakeholder groups involved in such a large data breach is too great to overlook the effects it had on each individual group. Utilitarian ethics is a way to quantify ordinarily qualitative effects as they effect every individual stakeholder in order to quantitatively arrive at the best ethical decision (Poel and Royyakers, 2011). In this case, the three groups affected by the breach who need to be considered in order to ethically analyze the impact are Equifax's IT staff, Equifax's executive team, and the consumers. The lens of utilitarian ethics allows me to analyze which decision would have generated the most overall good to society as a whole, which has been largely overlooked by previous analyses.

Utilitarian ethics relies heavily on the utility principle. The utility principle states that the best ethical decision for an individual or collective is that which generates the maximum amount of happiness for the largest number of people (Poel and Royyakers, 2011). This is particularly pertinent to the research outlined in this paper because there was such a large number of people impacted; roughly 56% of the adult American population felt the effects of the breach (Electronic Privacy Information Center, 2018). The utility principle will allow me to analyze the overall happiness generated by Equifax's actions, forming the crux of my argument.

Two factors which also play sizeable roles in analyzing a decision with respect to utilitarian ethics are duration and intensity (Poel and Royyakers, 2011). Duration refers to the amount of time the effects of a decision will be felt by any affected parties, while intensity refers to the overall significance of a particular decision in day-to-day life. Both of these concepts are integral in analyzing the Equifax breach because the effects of the breach are both unavoidable and indefinite for the majority of Americans. Both of these factors, however, are reliant upon the values of pleasure and pain. Pleasure and pain are objective states and can, more or less be quantified as a part of hedonistic calculus (White, 2001).

The final principle that can be used to analyze the Equifax data breach with respect to utilitarian ethics is the freedom principle. The freedom principle states that individuals and collectives are given the freedom to make the choice which gives them the greatest amount of happiness (Poel and Royyakers, 2011). This principle is what allows companies like Ford to make the decision they made to release a faulty vehicle. The decision was made which benefitted Ford, generating the greatest amount of happiness for their collective. The principle, however also specifies that the happiness generated for a single individual or collective cannot be outweighed by the pain it generates to the rest of society (Poel and Royyakers, 2011). In the case of the Ford Pinto, Ford made a decision that generated more happiness for their collective than pain to those individuals it impacted. This is particularly useful when analyzing the Equifax data breach because the freedom principle contains a very specific clause that directly states individuals and collectives must also consider the rest of society when making an ethical decision.

In what follows I will analyze the Equifax breach through the lens of utilitarian ethics. I will begin by applying the utility principle to the case, which will then be supplemented by my

analysis of intensity and duration. Finally, I will address the outlined by the freedom principle to reinforce the claim that Equifax acted unethically and is morally responsible for the data breach of their systems in 2017.

Analysis

Equifax made the unethical decision to neglect a security patch which ultimately resulted in the exposure of millions of Americans' sensitive information. The actions of Equifax's executive team indicate a clear lack of consideration for the consumers and the decisions made by Equifax repeatedly suggest that it failed to consider the welfare of society as a whole. This is a direct violation of the utility principle which clearly states that the most ethical action is the one which generates the greatest amount of happiness for the greatest amount of people. The monumental size of the Equifax data breach exemplifies the extent to which Equifax's actions impacted society. The vulnerable information stolen directly indicates that Equifax considered neither the intensity nor the duration of the effects of a potential breach.

The Utility Principle

Equifax as a collective made an unethical decision to neglect the software vulnerability present in their system. Despite knowledge of the vulnerability, Equifax prioritized the wellbeing of its reputation over the integrity of consumers' data. The number of people Equifax prioritized is limited to the number of people working for their collective, while the number of consumers was estimated to be about half of all Americans (Gressin, 2019). The utility principle states that the correct decision is the decision that generates the maximum amount of happiness for the greatest number of people (Poel and Royyakers, 2011). In utilitarian ethics, the utility principle is

the only sufficient ground for any actions for both collectives as well as individuals. Since the utility principle is considered the only grounds to make a decision, Equifax needed to consider the action which would result in the greatest overall happiness for the greatest number of people. In the breach, Equifax failed to consider the volume of Americans which could potentially be exposed during a breach due to their decision, and instead chose to preserve its own welfare.

One aspect of the Equifax breach that is often overlooked are some of the factors that did not lead directly to the breach itself, but instead increased the severity of the breach. Once the attackers were logged in as authenticated administrators, there were many instances of unencrypted personally identifiable information of Americans. Equifax decided at the start of its operation, years before the breach occurred, that they were going to house sensitive data as well as login credentials in plain English with no encryption (House of Representatives Committee on Overnight and Reform, 2018). Storing this sensitive information without any encryption indicates a complete lack of consideration for consumer privacy and a prioritization ease of access. Additionally, the decision was apparently made at the start of the operation, which indicates Equifax was consistently neglecting consumer privacy for years even before the breach. Equifax again choosing to preserve the welfare of its collective over the decision which would have generated maximum welfare for the public as a whole.

Importance of Intensity & Duration

Equifax was entirely careless with respect to both intensity and duration when neglecting to patch the software bug in their system. One of the most important factors when making an ethical decision in terms of utilitarian ethics is the intensity of the pleasure generated by the decision (Poel and Royyakers, 2011). Pleasure [or pain] will be greater or less according at least

partially to its intensity. The intensity of the pleasure the collective enjoyed by not expending the time, resources, and money on patching the Apache bug was negligible relative to the intensity of the pain felt by the victims of the data breach. The intensity of the pleasure enjoyed by Equifax was unnoticeable; it was simply an annoyance that Equifax did not subject itself to. Conversely, the intensity of identity theft or even the fear of potential identity theft is an active worry suffered by millions of Americans significantly decreasing their overall quality of life (Rash, 2017). The negligible increase in quality of life of Equifax employees obviously does not outweigh the significant decrease in quality of life suffered by half of the American public. Equifax's failure to consider the intensity of their decision is evidence of a clear and obvious violation of utilitarian ethics.

Equifax was also careless when considering the duration of their decision to neglect the Apache Struts vulnerability. Duration of the pleasure or pain experienced by society as a whole is an integral factor when making an ethical decision in terms of utilitarian ethics. (Poel and Royyakers, 2011). For Equifax, the revamping of the system following the vulnerability patch may have taken between three and five years (House of Representatives Committee on Overnight and Reform, 2018). Conversely, the victims as young as eighteen were subjected to an unrelenting fear of identity theft that would last a lifetime. In the best case this would be one or less years, in the worst cases this could mean six decades of potential risk. Based on the estimates made by Congress, the five years (1,825 days) which it may have taken Equifax to patch all of their systems does not outweigh the fear felt by half of all Americans, even if each was only impacted for a single day (143,000,000 days). Ultimately the decision made by Equifax failed to consider the duration of potential pain and pleasure, again directly evidencing its failure to make an ethical decision with regards to utilitarian ethics.

The Freedom Principle

It is possible that Equifax as a collective was simply striving for its own pleasure in an attempt to preserve its resources, time, and energy by neglecting to patch the vulnerability. The freedom principle states that each individual is permitted to strive for his or her own pleasure provided that it does not hinder the pleasure of others (Poel and Royyakers, 2011). Former Equifax CEO Richard Smith claimed that Equifax would, beginning on January 1st, 2018, allow consumers to lock and unlock their credit files when they want (C-SPAN, 2018). This new tool is a way for Equifax to delegate the power of data integrity to the consumers, relieving Equifax of the responsibility. This is in accordance with the freedom principle because it demonstrates that Equifax is in fact allowing consumers the freedom to make their own decisions with their credit information. The fallacy, however, is that this feature was not offered until January of 2018, but the breach occurred in March of 2017. At the time of the breach, Equifax was not acting in accordance with the freedom principles, instead they were prohibiting consumers from striving for their own pleasure by protecting their data, in direct violation of the freedom principle. Moreover, Equifax's decision to neglect the software vulnerability directly hindered the consumers' ability to pursue their own pleasure, once again violating the freedom principle. It is clear, then, that Equifax violated even the freedom principle in pursuance of its own pleasure, and therefore made an unethical decision through the lens of utilitarian ethics.

Conclusion

I have argued that Equifax is morally responsible for the breach it suffered in 2017 leaving millions of Americans vulnerable to fraud and identity theft for the remainder of their

lives. By evaluating the breach and all of the stakeholders involved through a utilitarian ethics lens, it has become extremely obvious that Equifax failed to make the decision which would benefit the largest amount of people. Though Equifax is frequently blamed for its breach, it is most often evaluated using virtue ethics, but I have illustrated through the use of utilitarian ethics that there is sufficient evidence to support the claim that Equifax is morally responsible for the breach. Such a finding only amplifies the need for software vulnerability detection and prevention. The Equifax breach was ultimately the result of a detected yet unpatched vulnerability in their system which could have been mitigated by a more robust vulnerability prevention device.

Word Count: 3,164

References

Bals, F. (2017, September 15). Equifax, Apache Struts, and CVE-2017-5638 vulnerability: *Synopsys.* Retrieved January 23, 2020, from https://www.synopsys.com/blogs/software-security/equifax-apache-struts-vulnerability-cve-2017-5638/

Berghel, H. (2017). Equifax and the latest round of identity theft roulette. *University of Nevada Press*, *50*(12), 72–76. doi: 10.1109/mc.2017.4451227

Electronic Privacy Information Center (2018). EPIC - Equifax data breach. Retrieved from https://ftp.epic.org/privacy/data-breach/equifax/

Gressin, S. (2019, September 25). The Equifax data breach: What to do. Retrieved January 21, 2020, from https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

C-SPAN. House Energy and Commerce Subcommittee Hearing on Equifax Data Breach. (2018). Retrieved from https://www.c-span.org/video/?434786-1/lawmakers-grill-equifax-ceo-data-breach

House of Representatives Committee on Overnight and Reform (2018, December) The Equifax data breach. Retrieved January 21, 2020, from https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

Newman, L. H. (2017, September 14). The Equifax breach was entirely preventable. Retrieved January 21, 2020, from https://www.wired.com/story/equifax-breach-no-excuse/

Poel, I. van de, & Royakkers Lambèr M. M. (2011). *Ethics, technology and engineering: An Introduction*. Chichester, West Sussex: Wiley-Blackwell.

Primoff, W., & Kess, S. (2018, December 6). The Equifax data breach. CPA Journal, November 2018 Issue, Retrieved January 22, 2020, from https://www.cpajournal.com/2018/12/06/

icymi-the-equifax-data-breach/

Rash, W. (2017, September 22). Equifax hackers enjoyed a leisurely tour inside your credit history. Retrieved February 10, 2020, from https://www.eweek.com/security/equifax-hackers-enjoyed-leisurely-tour-inside-your-credit-history

White, R. (2001, June). The principle of utility. Retrieved February 19th, 2020, from https://faculty.msj.edu/whiter/utility.htm

Zou, Y., & Schaub, F. (2018). Concern but no action. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems - CHI 18*. doi: 10.1145/3170427.3188510