Justin Daniel Robinson
PHIL 335E

Case Analysis on CSR

Introduction

In September 2017, the Equifax data breach became a focal point of global scrutiny due to its sheer scale and the nature of the data compromised. Equifax, one of the major credit reporting agencies, experienced an unprecedented security failure that exposed the personal and financial information of approximately 147 million Americans. The data exposed in this breach was not merely superficial contact information; it included highly sensitive details such as names, Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers. This exposure opened the door to a plethora of risks for the affected individuals, ranging from identity theft and financial fraud to a variety of other cybercrimes.

The repercussions of this breach were extensive and potentially long-lasting, raising serious concerns about the security measures adopted by corporations entrusted with vast amounts of personal data. The incident served as a catalyst for a broader discussion about the ethical obligations of corporations in the digital age, where data privacy and protection are paramount. These discussions also delved into how companies balance their pursuit of profit against their ethical and social responsibilities—a balance that was notably questioned in the wake of the breach.

In this detailed analysis, I explore the ethical implications of the Equifax data breach through the lens of Deontological ethics, particularly focusing on Kantianism, which

emphasizes duty, rights, and justice. From a Kantian perspective, Equifax's failure to protect consumer data can be viewed as a violation of a moral duty, making the breach not only a legal failing but profoundly unethical. I argue that by neglecting the security of sensitive information, Equifax caused significant harm to the public, which is morally reprehensible. This breach highlights the crucial need for stringent ethical standards in corporate practices, especially for entities holding sensitive personal information. Through this analysis, I aim to underline the importance of ethical integrity in the stewardship of personal data and to advocate for more robust regulatory frameworks to prevent such breaches in the future.

Friedman's Perspective

Milton Friedman, a notable economist, strongly advocated that a corporation's primary duty is to its shareholders. In his influential piece, "The Social Responsibility of Business Is to Increase Its Profits," Friedman argued against the then-emerging notion that companies should participate in socially responsible activities not directly related to their bottom line. He maintained that corporate executives, as agents of the shareholders, should focus primarily on maximizing shareholder value. He also contended that only individuals, not corporations, can bear social responsibilities, and thus the concept of "corporate social responsibility" is fundamentally flawed. According to Friedman, businesses indirectly contribute to social welfare by pursuing profit maximization within legal and ethical boundaries.

From Friedman's viewpoint, Equifax's primary obligation was to its shareholders, meaning the company should have primarily focused on the breach's financial consequences, such as potential lawsuits, loss of consumer trust, regulatory fines, and the resulting decline in stock value. The ethical failure in preventing the breach is significant because it not only harmed consumers but also directly affected the company's profitability and shareholder value. The breach and Equifax's delayed and insufficient response can be seen as a failure in their duty to safeguard shareholder interests.

However, Friedman's profit-centric stance requires understanding the broader implications in today's interconnected world. In an age where data is a key asset, companies like Equifax are not only financial entities but also custodians of vast personal data. This dual role complicates a straightforward profit-focused approach. Focusing solely on short-term profitability without considering data security could lead to long-term financial and reputational harm. Moreover, in the information age, maintaining consumer trust is crucial; losing it can have lasting financial consequences. Therefore, even within Friedman's framework, there's a strong case for businesses to prioritize data security as both an ethical obligation and a strategic necessity for long-term profitability.

Kantianism/Deontology emphasizes duty, rules, and obligations over consequences. From this perspective, Equifax had a definite responsibility to protect its consumers'

personal data, a duty extending beyond legal requirements to moral imperatives based on the principle of treating individuals as ends in themselves, not merely as means to an end. Equifax's failure to sufficiently safeguard consumer data violated this fundamental duty. Even when viewed through Friedman's profit-maximizing lens, Equifax's actions (or inactions) leading up to the breach can be considered shortsighted. Long-term investment in cybersecurity and a prompt, transparent response to the breach were crucial not only ethically but also economically.

Anshen's Perspective

Melvin Anshen offers a viewpoint contrasting Friedman's focus on profit. In "Changing the Social Contract: A Role for Business," Anshen argues that businesses exist within a larger societal framework and have a "social contract" with their communities, encompassing societal expectations and responsibilities beyond legal obligations. Anshen believes that as societal values and expectations evolve, so should this social contract, requiring companies to adapt and maintain their status as responsible corporate citizens. This means profit maximization, while necessary, should not be the sole focus. Businesses have a responsibility to consider the wider impact of their actions on society, stakeholders, and the environment.

According to Anshen, Equifax's handling of consumer data and the subsequent breach violated its social contract with society. As businesses like Equifax hold significant power due to the data they possess, this power comes with increased responsibility to

protect various stakeholders' interests, especially consumers. The breach and Equifax's initial lackluster response indicate a failure to uphold their part of the social contract, putting millions at risk of identity theft, financial fraud, and demonstrating a disregard for the broader societal implications of their actions.

Anshen's concept of the social contract underscores the dynamic and evolving relationship between businesses and society. As technology reshapes our world, society's expectations of businesses also change. In the digital age, where personal data is a cornerstone of many business models, society expects companies not only to provide services and products but also to act as stewards of the data they collect. This stewardship involves

Conclusion

The Equifax data breach serves as a stark illustration of the ethical responsibilities that corporations must uphold in our data-driven society. Analyzing the incident through Milton Friedman's theoretical framework, one could argue that Equifax's approach to the breach was notably flawed. Despite a primary focus on profit maximization, the breach posed significant risks to long-term shareholder value. This indicates a critical misalignment between immediate financial strategies and sustainable shareholder interests, highlighting a need for a more holistic approach to corporate governance that considers long-term impacts alongside short-term gains.

On the other hand, Melvin Anshen's perspective broadens the scope of corporate accountability by emphasizing a spectrum of responsibilities that go beyond mere profit generation. Anshen advocates for a corporate role that is dynamically integrated with societal needs and expectations. In the case of Equifax, this perspective sheds light on the ethical lapses in their response to the breach, illustrating a failure to fulfill their broader social responsibilities. The delayed and inadequate response not only exacerbated the consequences of the breach but also demonstrated a disregard for the profound trust placed in them by consumers and society at large.

The Equifax incident underscores the complex challenges that entities holding sensitive data face in the digital age. While data breaches might be viewed as an unfortunate but inevitable aspect of the digital landscape, the scale and the nature of the Equifax breach reveal deeper systemic issues within corporate structures and the frameworks that govern them. This situation highlights the critical need for stringent data protection regulations and robust internal systems designed to safeguard consumer data effectively.

Such systemic failures provoke essential questions regarding the ethical obligations of businesses in an era where data is not only a strategic asset but also a fundamental aspect of individual privacy and security. My analysis emphasizes the importance of recognizing and adhering to these moral duties, especially as businesses navigate the complexities of a rapidly evolving digital environment. Achieving a balance between profit motives and ethical responsibilities is not only intricate but also essential for

companies that aim to thrive and maintain credibility in this modern context. This balance requires a reevaluation of current practices and a commitment to integrating ethical considerations into the strategic decision-making processes of businesses, ensuring they can navigate the challenges of the digital age responsibly and successfully.