Zaki Ahmed

Professor Narayanasami

CS 3354.007

28 January 2025

Homework 01

**Case 1: Uber Data Breach Concealment Scandal**

In October of 2016, two hackers accessed a private GitHub repository using the credentials of Uber employees. They then were able to access the data stored on an AWS account and gained a substantial suite of rider and driver information, stealing personal data from a total of 57 million accounts. The hackers secured the names, email addresses, and phone numbers of 50 million Uber riders and about 7 million drivers globally, with about 600,000 U.S. driver’s license numbers. No Social Security numbers, credit card information, or any other types of data were taken according to Uber.

Uber managed to keep the consequences of this theft to a minimum by paying a ransom of $100,000 to the hackers, on the condition that they delete the data and do not leak news of any breach. Uber kept quiet on this offense for over a year, only revealing that this incident occurred in November of 2017. Though the former CEO, Travis Kalanick, knew of this attack only a month after its occurrence, he did not disclose news of it to the public. Dana Khosrowshahi, who took over as CEO of Uber in September of 2017, disclosed the cyberattack to the public in an emailed statement, entirely unprompted.

Several notable companies have been victims of data theft, like Equifax, Yahoo, and Target and to significantly worse degrees, but the concerning element of this case are the lengths to which Uber took to conceal the event. Unfortunately, this was not Uber’s first time concealing a data breach, being fined in January 2016 for failing to divulge another incident in 2014. It was not the first time engaged in unethical practices either; the U.S. government has probed into the company making illicit software and stealing another company’s intellectual property. This compounding of unethical behavior by Uber—specifically hiding a second data breach from the public for over a year—drew significant backlash from both the public and the media. A significant portion of their existing customers lost trust in the company, as did many potential customers. As mentioned earlier, the current CEO revealed the October 2016 cyberattack completely voluntarily, without any pressure from an external organization. In his email, he pledged to learn from past mistakes and to make security a priority for the company. The actions he took by himself included firing the standing Chief Security Officer, Joe Sullivan, firing his senior lawyer, Craig Clark, replacing the Chief Legal Officer, Salle Yoo, with Tony West, hiring a former general counsel at the NSA, Matt Olsen, as an adviser, hiring a cybersecurity firm to investigate the hack, and providing drivers with stolen licenses with free credit protection monitoring and identity theft protection. With regards to external bodies, the National Crime Agency of the U.K. also ran an investigation into the scale of the data breach.

Uber was in direct violation of ACM Code 1.2. An example of harm directly mentioned in the ACM Code of Ethics is “disclosure of information”; Uber failed to disclose news of the 2016 data breach, going so far as to conceal it entirely for over a year. Hand in hand with this, Uber was in violation of ACM Code 1.3 as well. Offering bribes is explicitly stated to be dishonest conduct in violation of the Code, and Uber paid the hackers $100,000 as hush money, a clear example of a bribe. This point also illustrates the fact that the public good was not Uber’s central concern during their programming work. They purposely attempted to sweep this event under the rug because their central concern was public image and reputation—their users’ safety was among the lowest of their concerns. Uber was in violation of an oath to respect privacy, codified in ACM Code 1.6. They did not take proper precautions to protect the personal data of their users which resulted in the two hackers gaining unauthorized access to their internal database. This detail violates Code 3.7 as well. Because Uber did not recognize and take special care of the systems that house sensitive information, especially after their first data breach, they suffered a second, more brutal attack. Altogether, Uber was in violation of Code 3.4. By violating so many crucial points in the ACM Code of Ethics, they were not supporting policies or processes that reflected the principle of the Code in the slightest.

Source: <https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data>

**Case 2: Apple Batterygate**

“Batterygate” refers to a low point, in 2017, in Apple’s career where it was discovered that the company had been intentionally reducing the performance of iPhones with degraded batteries. This was done without any disclosure or explanation, nor were there any options provided to the user to toggle this performance reduction.

Anecdotes of people experiencing impaired performance on their iPhones with continued use had already been circulating, but with the 2017 iOS updates, this experience became an epidemic. Complaints kept gradually building until independent researchers from Geekbench empirically discovered that iPhones with deteriorated batteries experienced significant CPU slowdown, at which point frustrations boiled into a complete outrage. Apple faced substantial public backlash, with a vast portion of their customer base losing complete trust in the company and even lodging class-action lawsuits regarding the matter. Apple compromised their reputation by mishandling the most significant component of their business model—customer trust. The mounting pressure finally elicited a response from the company, with the CEO, Tim Cook, himself issuing an apology letter to the customer base. Vowing to learn from the mistakes of this disaster and make amends, Cook revealed plans to allow users customization over their device’s battery health and performance. Additionally, Apple offered significantly reduced-cost battery replacements for any iPhones affected, providing some alleviation to embittered customers.

Apple directly violated Code 1.2; by forcibly slowing down iPhones with poor battery health without informing customers, the company caused many to believe their phones became obsolete. This resulted in consumers purchasing completely new smartphones, instead of merely getting their battery serviced, and thereby causing notable financial harm. Apple was most egregiously violating Code 1.3—an oath to be honest and trustworthy. They failed to disclose to their customers the implementations within their iOS updates and simply imposed many iPhone models to be borderline unusable. This practice did not reflect honesty from the company and demonstrably resulted in an exceptional dip in customer trust. Related, the final principles Apple was in violation of was Code 3.6 and 3.7. Within the section of the former, the ACM explicitly mentions that if any changes to a system are risky or impractical, users should be promptly notified. In Apple’s Batterygate updates, they failed to notify those with affected iPhones that they would diminish their phone performance and enforced it without their consent. This leads into infringing upon Code 3.7. Smartphones have become so thoroughly integral to modern society; it is evident that Apple failed to recognize or take the special care required for their iPhones. Were they aware, they would not have rolled out their 2017 updates.

Ultimately, Apple owned up to their mistakes and provided a decent remedy to their blunder, but only after being thoroughly pressured by the public and researchers. Though Batterygate marks a permanent blemish on the company’s career, it also marks a general turning point for not only Apple, but the tech industry as a whole. Apple became much more transparent with the contents of iOS updates, and governments enacted stricter consumer protection regulations to implement safeguards from planned obsolescence and hold companies more responsible for their actions.

Source: <https://medium.com/@AppleByte/when-apple-lied-to-millions-99da0dd4435c>