Daniel DeCarlo

Box# 107

CIS 101

Prof. James

Do corporations have a responsibility to protect the data of its users?

Technology is rapidly changing and with the change of technology so is our culture. Technology is becoming integrated in our everyday lives and some of those tasks require that we put in personal information so we can have access to the technology. Most social media programs require that we include an email address, our names, birthdays, and other personal information. They might as well ask for peoples social security numbers with all the personal questions they ask. The collection of this information is stored on the company’s servers and the data is backed up. As companies collect data and store it there are people who can hack those servers and collect the personal data that the company collected. This breach of hackers and the theft of personal data can really affect our lives and can expose sensitive information. Companies that collect personal data from its users have the responsibility to protect the data because the customers are trusting the company to use it for good.

Data is always being collected by companies and is seen as a valuable resource because the data collected includes interests and other valuable things that reflect your personality. The article by Angela Carmichael, Why it’s important to safeguard your customer data and protect your brand discusses the value of data. Carmichael states “The personal information of consumers is the new oil of the digital world. Everything runs on data. But while the business that collect and process data have become increasingly valuable and powerful, recent events prove that even the world’s biggest brands are vulnerable when they violate their customers trust.” Carmichael is saying that data is a form of gaining power and the more data you have the more access you have to an individual which means you can sway them into doing something. Also this valuable data that can be used to persuade people to buy something or think a certain way can be used for good or can be used for evil, it depends on the person who has that data. Companies should protect the data they collect from individuals because if that data gets into the wrong hands, it can make the unethical people have power in the digital world. When a company says that they have been hacked and the data has been stolen it makes the company look unprofessional. The opposite is true if the company protects the data and prevents hacks and the customers trust the company more. The protection of data can be seen as a hotel. If a family is going to stay at a hotel for a vacation and they leave the room to go shopping they are trusting that the hotel will keep their valuables safe. The hotel makes sure they have enough security to protect the family’s possessions. If the security fails the family will feel violated because their stuff was stolen and someone had entered where they temporary lived. Companies are required to protect the data because it can damage the company’s image.

Companies are gathering all of this data and they are recommending different products and making our experience on their software more enjoyable. Companies do have many ways of securing the data and protecting their companies from hackers and people who breach the company. The article Companies Need to Take Responsibility for Protecting Sensitive User Data by Todd Feinman it states “Organizations in all industries must stop working under the assumption of “if” and instead, build strategies around ‘when’ a data breach will occur. The bad guys are only getting better at what they do…when companies rely too heavily on securing the perimeter instead of managing the items within the perimeter, they’re setting themselves up for a more damaging breach.” The companies should always be prepared for a cyber-attack and they should treat a drill like an actual emergency and come up with new ideas how to stop the attack. If there is an attack there should be a plan on how to prevent another one and security should keep increasing. Feinman is stating that companies need to figure out ways to protect data from within the company instead of protecting the outside of the company. This is a true statement because employees could accidently leak data or can purposely steal data. Having protection on the inside is important because having a strong perimeter and a strong internal system can really prevent attacks and can protect data.

One field of the cyber world that is always trying to get breached is the banking world. Today most individuals use electronic banking to fulfill their financial needs and errands. It’s easy to cash a check or check a balance on a phone. The banking apps require a lot of sensitive information and there are ways to protecting that data. Banking websites ask verification questions that only the customer would know the answer to. The article what is the Responsibility of Business to Prevent Identity Theft by George N. Root III discusses the idea of banking and how the data needs to be protected. Root states “A company should keep up-to-date protection on their computer database to prevent information from being compromised, and the company should also limit what information is exposed to access through the Internet. The firewalls that protect customer data should be updated on a regular basis, and there should be multiple layers of protection encrypted on each database.” The banking/credit card companies should have security that is brand new and is stronger than the previous version. Also the multiple layers per data base connects to the paragraph above when it discusses having to protect data from within. The more layers of security there are the less likely someone is going to get in and exploit the personal data of consumers. Root also brings up the idea that companies should only require information that is needed for the certain task being performed. Having less personal information on a database reduces the damage done by hackers. If there isn’t a lot of personal data on the servers that can hurt the company and the clients then it won’t impact the company. If a company has a large amount of data and they became hacked then people’s personal files are out in the world and their privacy has been violated. Having a limit and multiple layers of security should be included in a company’s business plan because it will protect them and the consumer.

# Facebook has been one of the reasons why people are now concerned with data security and whether or not companies should protect personal data. It was revealed that Facebook was selling data to a company called Cambridge Analytica without the consent of the users. Also the data sold was used to sway people in the upcoming election. This act committed by Facebook was unethical and it violated the privacy of the Facebook users. Facebook allows users data to be private and the user can share with anyone they want because they give permission to share what data they want. The article *Facebook's Zuckerberg Outlines Steps to Protect User Data* contains a comment made by Mark Zuckerberg the CEO of Facebook. The article states “We have a responsibility to protect your data, and if we can’t then we don’t deserve to serve you,” Zuckerberg said. “I’ve been working to understand exactly what happened and how to make sure this doesn’t happen again.” The CEO of Facebook is saying that their company should protect personal data and that it is included in the service they provide. Companies that collect data shouldn’t allow other companies to see it and sell it to make profits off of your personal life and information. The example of Facebook is a reason why companies should protect data because if they don’t then it ruins the trust built between the company and the customer.

The data of users is something that needs protection from hacker which is why companies have the responsibility to do so. The protection of people’s data can help protect lives and can keep people’s right to privacy remain intact in an age where technology is becoming more and more active in life.

# Works Cited

Carmichael, Angela. *Why it's so important to safeguard your customer data and protect your brand*. 9 may 2018. https://business.financialpost.com/executive/why-its-so-important-to-safeguard-your-customer-data-and-protect-your-brand. 15 November 2018.

Feinman, Todd. *Companies need to take responsibility for protecting sensitive user data*. 2 Feburary 2015. https://www.entrepreneur.com/article/242355. 15 November 2018.

Frier, Sarah. *Facebook's Zuckerberg Outlines Steps to Protect User Data*. 21 March 2018. https://www.bloomberg.com/news/articles/2018-03-21/facebook-s-zuckerberg-outlines-steps-to-protect-data-after-leak. 15 November 2018.