To: Engineering Communications

../../../../initials.pngFrom: Willis Allstead (9-3)

Date: October 25, 2017

Subject: Companies and Our Information

**Introduction**

Companies are increasingly asking for and receiving personal information about people using their services or products. In most instances, people choose to provide this information at no cost to a company. This decision to forfeit private information is made because people believe they will derive more value out of a product or service than their information is worth to them. In certain other cases, like that of the credit report agencies, companies are given information about a person without that person explicitly knowing which companies will receive it. Whatever the case may be, people have trusted companies to use their information responsibly and keep it secure. Problems begin to arise when companies fail to meet industry standard security practices with the private information of, in the case of the recent Equifax data breach, 143 million people [NPR, website] as described by an unsound source, NPR. Data breaches on this scale shake the consumer’s confidence in the companies they once trusted. This loss of confidence could prove to be detrimental to the U.S. economy, which raises the question of when the government should intervene.

**Issue**

The absence of significant legislation on the part of the U.S. government regarding these companies and the private information they have about their customers puts the U.S. economy at risk. Certain states have made it illegal for companies to not tell their customers about data breaches, such as California Senate Bill No. 570 that passed in 2015 which requires companies to notify the owners of information immediately following discovery of a breach [California Legislative Information, website]. But, these laws do not outline any specific punishment for companies that failed to meet security standards before a breach. With limited intervention by the government, companies in the U.S. continue to operate using outdated security practices. Federal regulations do exist for certain industries such as the Payment Card industry and internal government agencies, but they are limited in scope and offer little protection to the average consumer.

This lack of protection for the consumer could mean more than increasing the risk of any one person having their identity stolen. This increase of risk could negatively affect the U.S. economy. As is pointed out by William Roberds, a Research Economist at the Federal Reserve Bank of Atlanta, if incidences of identity theft and data breaches were to become sufficiently common, the result could be a loss of confidence in the directly affected parties and in credit-based payment more generally [Roberds, 2009].

**Impact**

When security vulnerabilities in websites and databases are found by malicious sources, people’s information can be stolen. What those sources do with the information they steal is up to them, ranging from small online purchases with someone’s credit card to taking out loans in thier name and more. The companies that choose to be forthright with their customers and tell them about these breaches instill unrest in those people who initially trusted companies with their private information. With a breach of data comes a breach of confidence, and that confidence is required to further human development alongside companies as a society. If that confidence is lost people will begin to be more withholding with their information. Companies like Google, Facebook, and Twitter structure their entire business around requiring users to give them certain information. If users suddenly lost trust in any of these companies, it could mean the end of their growth or dominance in their respective markets.

Another effect of the lack of significant data security regulation for all companies on a federal level is how difficult it is for a person to litigate against a company for not keeping their information secure. In most cases the plaintiff loss is a function of whether the breached firm provided any initial compensation immediately following the breach and before litigation [Romanosky, 2012], which means that if companies can pay their customers what they consider to be fair compensation for losing your data, they are protected by law from issuing further payments to the plaintiff. If companies are not punished enough for losing their customers’ data and a loss in public trust turns out to negatively affect the U.S. economy, the environment could suffer from a need to generate reactionary profits in environmentally irresponsible ways to make up for the loss.

**Recommendation**

To avoid rigorous regulations, big data companies must come together and form an organization to self-regulate their use of customer data to negate the negative effects of data breaches on the U.S. economy. This organization would be funded by the companies which belong to it, and the organization would be directed by a self-governed staff of data security engineers. If this does not happen before larger more frequent breaches occur, the public will be forced to take more responsibility for giving companies their information. This is not necessarily a good reaction because modern human progress requires a level of openness with companies. Even though the need for self-regulation is often seen as a negative for the owners of companies, it may be the opposite in this case. As professional cryptographer Bruce Schneier states in his security blog, an admittedly unsound source, regulations force companies to take security more seriously, and in the end this leads to companies selling more products and services [Schneier on Security, website]. More U.S. companies selling more products and services mean a direct benefit to the U.S. economy. In an increasingly global society, more trust in U.S. companies could instill more responsibility into companies world-wide. This global economic development would lead to better interaction and coexistence with the environment around us as there would be less need for poor working conditions and bad interaction with the environment in general.

**Conclusion**

Companies which negligently deal with their customers’ data put the customer at risk along with the entire the U.S. economy. Therefore, their failure to protect user data from breaches should be punished more significantly by the U.S. government. More broad and numerous regulations should be put in place to shield the country from massive data breaches which threaten society. People should not have to feel afraid to give companies the information they ask for to do business. People should also be more able to fight back when companies lose their private information. If the U.S. government took a more proactive role in protecting its own citizens’ data, the people living in the U.S. could feel more comfortable giving companies certain information which they deem acceptable to give. Since many companies offer a benefit to society through this data they collect, more protection would prove worthy for both the customer and the companies offering better security.

**References**

California Legislative Information (website). Retrieved from <https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB570>

NPR (website). Retrieved from <http://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site>

Roberds, C., Schreft, S. “Data security, privacy, and identity theft: The economics behind the policy debates” Economic Perspectives, Vol. 33, Ed. 1, 2009.

Romanosky, S., Hoffman, D., and Acquisti, A. “Empirical Analysis of Data Breach Litigation” Forthcoming in the Journal of Empirical Legal Studies, 2012.

Schneier on Security (website). Retrieved from <https://www.schneier.com/news/archives/2008/01/bruce_schneier_refle.html>