
Written By: Brianna, Heather, and Nkechinyere

April 12, 2019
Introduction

Data privacy and security are becoming major concerns for individuals everywhere, as there have been several data breaches in major corporations all across the globe and even in government agencies. Data privacy and security concerns have also led to the formation of the European Union’s General Data Protection Regulation (GDPR) which aims at enforcing data protection and privacy for all individuals. The U.S. has not been left out, as there have been several cases of top management of major corporations being called to Congress for hearings. However, there isn’t any general regulation like the GDPR present in the U.S. which would increasingly become of concern to the citizens as time goes on. In other parts of the world, there are fewer data privacy regulations, and some governments encourage surveillance of their citizens.

Data surveillance is constant monitoring of peoples digital activity, and it can enable a person’s location, habits, likes, beliefs and sometimes banking information to be monitored, mostly to provide tailored advertisements to that person. Data surveillance forms the backbone of electronic commerce as major technology companies engage in data surveillance and “Big Data” has become the new “gold” in this technological era, where business analytics tools serve as a competitive advantage for companies.

The now-defunct Cambridge Analytica Ltd was a British political consulting firm that used data analysis to provide advice to political aspirants during the campaigns. The company is most famous for its role in the U.S. Presidential Election and the Leave.EU (United Kingdom’s referendum to leave the European Union), both of which are ongoing investigations in the U.S. and U.K respectively. They used Facebook data from millions of people without their consent and targeted political advertisement at people aiming to influence their opinions. This was the largest breach of individual privacy, and it had the highest impact worldwide, and it sparked the talk on data privacy regulations being put in place to protect citizens from unethical exploitation.
This paper looks at how data insecurity is favored by major corporations, and how it forms the bases of their business models. It takes a closer look at the Cambridge Analytica scandal and asks questions about what people, companies and even the government are doing to ensure that such a scandal does not repeat again. Finally, we make suggestions on what we believe is the right cause of action for everyone to take to ensure a more private and secure internet.

**Companies Favor Insecurity**

Big Data has created the opportunity for companies to make tremendous profits through targeted marketing, and companies create recommendations that are tailored to the individual needs of people. Amazon collects data from your purchases online to enable them to make tailored recommendations to consumers to increase purchases, Amazon's Alexa collects data from users to enable improved voice recognition. Facebook collects its users data to provide tailored advertisements to the users, and Netflix collects data to enable them to provide movie recommendations to consumers.

Data is gold for the twenty-first century, and all the companies are mining the data to improve their competitive advantage. Therefore, it is in the interest of the companies to ensure that there are loopholes within the internet to enable them unfettered access to the data they desire. The result of this massive digital surveillance is a promise of convenience to the end users, the promise of being able to obtain your required groceries without the inconvenience of going to the mall, and the luxury of being able to control all the gadgets in your house just by talking. However, these conveniences come with a steep price of constant surveillance, lack of privacy, and even worse, the lack of complete knowledge of what your data will possibly be used for in the future.

These issues are further complicated by somewhat outdated privacy policies and legal practices. Requirements for privacy policies vary from country to country, and even state to state in the U.S., with the strictest instance soon to be in California where a privacy policy must be easily
viewed from a link containing the word “privacy”. It does not require users to have the option to request that their data not be tracked. These differences over state or country lines can also be difficult for the average user to understand, requiring specific legal terms that people may not be familiar with—often resulting in people not fully understand the terms that they agree to. In an age where so much data is being created daily, it is a huge risk for individuals to be unaware of the risks they may be taking on in order to use a service.

Even beyond these issues with data privacy, it can be difficult even for an informed consumer to be safe with their data or to take legal action in regards to data insecurity. U.S. court systems have little legal precedent to go off of in cases of data breaches or potential data breaches, and even frequently rule that the risk of a data breach is not enough injury to be worth taking legal action over. Even if one sues over a potential data breach, a case may be rebuffed or even dismissed if no data breach actually takes place. As a result, individuals cannot sue over a data breach until the damage has already been done, thus creating little legal precedent for future cases or law making.

**Facebook and Cambridge Analytica Scandal**

Cambridge Analytica, a political consultancy firm, obtained over eighty million Facebook users’ profiles using an algorithm developed by Dr. Aleksandr Kogan, a psychology professor at Cambridge University. They used the data to create personality profiles of the users, and developed advertisements tailored to those users aimed at influencing their opinions. They were hired by several political campaigns all over the world, from the US Republican Presidential campaign to electoral campaigns in Kenya and Nigeria.

The data Cambridge Analytica collected from users included their profile information, their likes, their network of friends, and their location data, using this information to develop various clusters of people’s personality traits and target consumers with advertisements. They used a survey to mine information from not just users who agreed to take the survey, but also those in
the social network who had not agreed to give Cambridge Analytica permission to read their data - in fact, only about 270,000 users had in fact given consent. The survey claimed to only want to use the data for academic purposes, however, they sold to political campaigns for targeted advertising purposes. While at the time of the data collection, Facebook did allow for apps such as the survey to collect information from others in a user’s network, they later changed this policy to disallow that; and throughout this entire process, Facebook has not allowed data collected for academic purposes to be sold for non-academic uses.

This situation leaves one with troubling questions for future incidents. Could similar situations have already happened, unknown about without individuals like Christopher Wylie who reported the truth of the matter? Can it be determined how much of an impact these targeted advertisements had on the 2016 U.S. Presidential Election, the Brexit vote, and more? And clearly, the deterrents in place were not enough to prevent this gross misuse from happening once - so what would be enough of a consequence to ensure that it does not happen again? Some of the factors that contributed to the Cambridge Analytica situation were the company’s monetary motivation from their political clients, a lack of security - either from Cambridge Analytica themselves if they were in fact, as they claim, ignorant of how Dr. Kogan’s algorithm worked, or from Facebook in not seeing what information Cambridge Analytica truly was taking - and some degree of consumer privacy and data illiteracy. Even though consumers were not aware that the survey would take data from others in their social network, not knowing just what can be done with their data and how it can affect them is still a relevant issue here.

The scandal resulted in major losses for Facebook, as their share prices dropped by $100 billion within twenty-four hours. The CEO of Facebook, Mark Zuckerberg, issued a public apology for the situation and was invited to the U.S. Congress to answer questions on how the data was collected. The British parliament also requested that Zuckerberg appear before the parliament to answer questions concerning Facebook’s involvement in the Cambridge Analytica Scandal. However, Zuckerberg did not appear before the British Parliament, only the U.S. Congress. Facebook has begun applying the E.U’s GDPR in all countries, not just Europe, as a means to
ensure the scandal does not occur again. Cambridge Analytica, however, is now a defunct company as of May 1st, 2018.

**Lessons Learned from the Facebook and Cambridge Analytica Scandal**

The biggest lesson from the Cambridge Analytica scandal is the importance of data privacy and security; however, there are several other lessons that can be learned from the scandal, including how there are several unethical corporations that operate under disguise and provide wrong or intentionally ambiguous information to the consumers to ensure that their interests are continuously protected. Furthermore, the scandal showed the complete lack of awareness consumers have on what their data is being used for. Many consumers believe their data is only used to enhance their experience on such sites as Facebook, Google, Amazon, Twitter, etc. However, the Cambridge Analytica scandal showed that there are several other uses of consumer’s data that are not highlighted within a company’s policies and are not known to the consumers.

The Cambridge Analytica scandal also showed that there are bigger consequences of lack of privacy that users should be aware of. The typical tailored recommendations or advertisements are not the only disadvantage of unfettered data mining, the repercussions can go as far as manipulating the users' opinions to enhance a candidate’s chances at a presidential election. The ability to control the public by any corporation or government agency should be a major concern to everyday citizens as it is a violation of the rights. Although several regulations are emerging to prevent a recurrence of this scandal, there are still several countries that are lagging behind others, and there are still individuals that are not fully aware of the repercussions of lack of privacy.

There is also a major impact of this scandal on academic research, as the data was collected by Dr. Kogan allegedly for academic research. This increases the difficulty of obtaining data for legitimate academic research by institutions or professors. Thereby, increasing the delay in
discovering innovative solutions to social problems. While it is necessary to ensure all data being given out for whatever purpose is secured and anonymous, the scandal increased the reluctance of people to opt-in to giving their data for research purposes, as they are unable to differentiate real research from fake research. Furthermore, the scandal encourages major conspiracy theories concerning data analytics and big data and further emphasized the doomsday rhetoric being emphasized by anti-technologists.

**Potential solutions to data insecurity**

If the Cambridge Analytica scandal has any lesson to teach about data security, it is that major companies that allow for third-party apps need to tighten their security and quality assurance in order to protect users’ data. If Facebook had tested Cambridge Analytica’s survey before allowing users to take the survey, they may have decided that it was too much of a risk in regards to what data was being collected. Implementing such measures instead of assuming that third parties would be inherently compliant with their policies would go a long way in preventing this sort of data scraping again in the future. Since large companies, such as Facebook, handle personal data on millions of people, there is no reason to not be taking every measure to ensure that sensitive information stays safe and secure. Such efforts may require a devoted team at these large companies, or perhaps a neutral, third party entirely devoted to the task.

Furthermore, a compliance check would need to be put in place in order to ensure data protection. Corporations have proven that they cannot be implicitly trusted to maturely handle data, which necessitates some form of government policy and/or certification that companies are handling sensitive data securely. This could potentially be something along the lines of extant energy efficient or employment opportunity compliance. Luckily, there are already strides in this direction, with tech giants coming to work with Congress on making better policies in regards to data handling in light of recent technological innovation. California and the GDPR are also foraging the path towards data legislation, as well.
However, the issue of privacy illiteracy remains. With more unified privacy legislation, though, people will be able to more easily trust their understandings of what privacy policies entail. And, with the privacy legislation that Congress is working on, people would also be able to do something about violations of their privacy- or maybe even potential violations. Though data creation and use has evolved quickly, laws are beginning to catch up to the current state of affairs. These changes will be able to prevent scandals, such as with Cambridge Analytica, from happening again, especially when ensured by an ever-evolving legal system to work with future changes on the tech scene. This is another situation where having a team of people devoted to making sure that data and privacy related laws are still effective with current technologies, and that privacy is still a forefront concern in creating more of this legislation. In an ideal world, none of these issues would exist; but in a realistic world, making sure that companies that do not comply with these legislations face consequences, and making sure that these legislations exist, is a viable place to go to- and as soon as possible.

**Conclusions**

Although the companies favor insecurity for profit margins, it is not impossible to change the security of users data across the globe. The Cambridge Analytica scandal has brought forth new guidelines and procedures in the handling of data in some corporations and countries. This jump start to a concern for privacy will help propel the need for secure data practices. Introducing new legislation and promoting privacy and data understanding throughout society will lead to a more secure and informed society.

In order to measure the success of the implementation of the new data and privacy statements presented by corporations, the following guidelines should be met. The statements should: be straight-forward and understandable to an everyday user, allow users to opt-out of data sharing and be transparent about where the data travels, and ensure the privacy legislation is enforced. For those companies that refuse to adopt a new standard data and privacy policy, there should be financial ramifications and sanctions taken against the company. Implementing these guidelines
and fostering a transparent operation of data will lead to a more informed and secure society. Giving users a peace of mind and allowing them to restore the privacy that has been lost.
References


Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. WW Norton & Company; 2018 Sep 4.


Socialpinpoint “7 lessons we learned from the facebook/cambridge analytica scandal.” https://www.socialpinpoint.com/blog/7-lessons-we-learned-from-the-facebook-cambridge-analytica-scandal/