

CONCERNS OF DATA COLLECTION PRACTICES

Author:

Amanda Maroun

Faculty Sponsor:

Lynn Braender

Department of Business

ABSTRACT

Big data has transformed our lives by providing us with customized online experiences, new products and services, and improved ways of doing business. While “big data” may enhance the way we live by allowing us, for instance, to understand scientific fields like medicine and climatology, it also comes with risks to our personal privacy. This paper will examine some of the issues surrounding big data; specifically with current data brokerage activities. It will discuss the current state of data collection and the practice of selling that data to third parties and how these activities open up potential and serious problems with our right to privacy. If data collection continues to go unchecked, it may reach dangerous levels that could adversely impact the way we live.

INTRODUCTION

As technology becomes integrated into our daily lives it has adapted and advanced in unprecedented ways. Individuals in corporate America have found ways to capitalize on the feature’s technology provides. In today’s data driven era, big data has turned into a profitable market for companies because it provides another stream of revenue. Data collection becomes an issue when companies benefit off customers who value efficiency and are unaware of the dangers to their privacy. Although data collection proves to be a useful tool for companies, the problem lies in the possibility of exploiting the collected data for economic gain. Consumers private information is left vulnerable and in the hands of unknown individuals. The current state of data collection requires change because an person’s right to privacy is at risk. This paper will focus on how customer data has been used for profit, the lack of knowledge people have on data collection practices, and the fact that people care about their privacy. There should be transparency with consumers and regulations set forth by the government. The purpose of this paper is to explore and explain ways that data collection practices can improve. It would be ideal to minimize the risk of data collection toward the consumer while maintaining a level of efficiency for businesses.

HOW CUSTOMERS HAVE BECOME A PRODUCT

Companies are able to receive economic benefit by selling and receiving consumer data. There is not much stopping organizations in the United States from taking advantage of selling data since there are hardly any regulations in place. Data brokers such as Acxiom, Nielsen, and Equifax specialize in the analysis, collection, and redistribution of personal information.¹ These companies sell sensitive data to businesses, advertisers, other data brokers, and the government.² Some of the information collected includes: name, age, gender, home address, telephone number, email address, marital status, age of children, sexual preference, other connected devices in the household, property ownership, political views, income details, and educational background.³ Social media websites such as Facebook, Twitter,

¹ "Why do Companies Collect, Sell, Buy or Store Personal Data," The Windows Club, accessed December 8, 2018, <https://www.thewindowsclub.com/why-do-companies-collect-sell-buy-or-store-personal-data>.

² Ibid.

³ Ibid.

A. MAROUN: CONCERNS OF DATA COLLECTION PRACTICES

Snapchat and Instagram allow its users to share pictures and messages with friends. However, the ability to use these platforms for free comes with a hidden cost. In a sense, people are paying for the free service with their data, instead of physical currency. A problem emerges when companies begin tracking movements online and using personal information to make money. In Instagram's Privacy Policy Statement, the company states, "User content and any other information collected through the service may be among the items sold or transferred".⁴ The policy continues, "We share information about you with companies that aggregate it".⁵ There is no notification or message that explains who it's being directly or indirectly sold to, how long the data will survive, and the profits generated from these practices. Beside social media websites, other large companies such as Amazon, Google, and Microsoft have been accused of gathering and selling data. In September of 2018, there were allegations against Amazon staff for selling confidential consumer data to third-party companies in China.⁶ Many online services have the opportunity to sell personal data or have begun to secretly sell it because it is profitable and there is a lack of government regulation. Companies are beginning to turn their customers into another form of profit and have created a system that constantly surveils and collects personal information. This can only be stopped with effective and proper rules in place.

The primary defense for those who support data collection is the fact that it is useful in helping businesses do a better job of providing products or services to consumers and other businesses. Data can improve efficiency and allow companies to have more relevant and valuable analytics. Consumer data is important for businesses to analyze, however, without proper oversight, data collection may jeopardize consumers sensitive information. If companies were to collect data with some level of anonymity, in other words, without identifying data, companies could still have the same data but at a smaller risk to individuals. A company only needs two data points, such as birth date and zip code, in order to identify a person. The United States could follow a model similar to the General Data Protection Regulation (GDPR) that the European Union uses. The GDPR has multiple rules within its policy which include: consent, breach notification, right to access, right to be forgotten, privacy by design, and penalties.⁷ Consent makes sure companies use clear terminology and that their data and privacy policies are in a simplified form.⁸ Breach notification requires mandatory notification of any data that is at risk of being compromised in the first 72 hours of a company becoming aware of the issue.⁹ Right to access gives individuals the power to request what data a company has on him or her and the purpose the collected data serves the company.¹⁰ The right to be forgotten allows a customer to request that their data is erased.¹¹ It is important to note that requests to erase data may not be fulfilled and are sometimes limited. Privacy by design is a regulatory law that limits the data a company has on an individual if it is not relevant to an organization's operations (focused collection).¹² For instance a clothing store does not need to know personal health details. In addition to regulating the relevancy of data, privacy by design also calls for companies to include data protection as a default setting.¹³ Many times products or services come with default settings that enable access to location, camera, and microphone. Data by privacy would ensure that these must manually be turned on. Penalties include large fines and imprisonment for infringement

4 Instagram Inc., Instagram Help Center, accessed December 9, 2018, <https://help.instagram.com/402411646841720>.

5 Ibid.

6 Agence France-Presse and James Cook, "Amazon Investigates Reports that Staff Sold Customer Data," The Telegraph, last modified September 17, 2018, accessed December 8, 2018, <https://www.telegraph.co.uk/technology/2018/09/17/amazon-investigates-reports-staff-sold-customer-data/>.

7 "GDPR Key Changes," Trunomi, accessed December 9, 2018, <https://eugdpr.org/the-regulation/>.

8 Ibid.

9 Ibid.

10 Ibid.

11 Ibid.

12 Ibid.

13 Ibid.

on the previously stated regulations.¹⁴ If the United States seriously considers the risks data collection creates and takes a course of action, data can continue to be collected with protection and purpose.

UNAWARE AND UNINFORMED

Individuals are often unaware of what is being done with their information and are overall uninformed of the data collection process. People are mindful that they directly and indirectly leave digital footprints on the web. However, many individuals do not know the extent or details of how their data is processed and how it transfers from company to company. For instance, "only 25% of people knew that their data footprints included information on their location".¹⁵ Only 14% knew that their web-surfing history was shared and 18% knew that their communication history online, such as chat logs, were accessible to others.¹⁶ In April of 2018, Mark Zuckerberg, CEO of Facebook, was in the limelight for data mining issues. It was discovered that Facebook sold user's data without their knowledge.¹⁷ If companies became more transparent with their practices then consumers would become a more informed user base. If the government set guidelines for companies to follow in regard to transparency, then there would be a general standard for all companies to use. From there, the government could monitor data collection practices and ensure that there are no loopholes.

Many may blame the consumer for being unaware and uninformed. For example, there is a terms and agreement policy in place, why don't they just read? The issue with this argument is that privacy policies are complex intentionally.¹⁸ Kristen Martin, associate professor of business ethics at George Washington University and cyber privacy expert, claims that privacy policies are purposely ambiguous and filled with jargon.¹⁹ The vagueness generalizes privacy concepts and doesn't actually explain what's going on. Even if people were to read the policy they would still be uninformed. Businesses can simplify and consolidate their privacy policies. When businesses compose financial statements for the end of the quarter, they simplify masses of complicated information so investors can quickly understand the performance of the company. The same can be done with data collection terms and agreements.

DO PEOPLE CARE ABOUT THEIR PRIVACY?

The value of privacy should be more important than short term efficiency. Since many people care about the privacy of their data, government regulation is essential in order to maintain privacy. A Harvard Business Review survey found that 72% of Americans are reluctant to share information with businesses because they want to maintain their privacy.²⁰ The issue is many Americans unconsciously take actions that show a lack of concern for their privacy. Accepting a terms and agreement policy without reading it thoroughly or thoughtlessly connecting to a foreign wi-fi network in a retail store are examples of valuing efficiency over privacy. Although people can do a better job of protecting their sensitive information, businesses should implement privacy into their policies and practices. Those who write the terms and agreement policy need to use simplified language so the common user can consent to the policy with understanding. Stores that use consumer data from wi-fi connected devices should be limited to the type of information they can view. Individuals have the power to advocate for change. If organizations do not

¹⁴ Ibid.

¹⁵ Timothy Morey, Theodore Forbath, and Allison Schoop, "With Big Data Comes Big Responsibility DATA Customer Data: Designing for Transparency and Trust," Harvard Business Review, accessed December 9, 2018, <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>.

¹⁶ Ibid.

¹⁷ Kimberly Atkins, "Facebook CEO Faces Grilling today on Data Mining," Boston Herald, last modified April 10, 2018, accessed December 12, 2018, <https://www.bostonherald.com/2018/04/10/facebook-ceo-faces-grilling-today-on-data-mining/>.

¹⁸ Stan Horacek, "Here's Why You've Been Getting so Many Privacy Policy and Terms of Service Updates Lately," Popular Science, last modified April 26, 2018, accessed December 15, 2018, <https://www.popsoci.com/gdpr-privacy-policy-update-notices#page-2>.

¹⁹ Ibid.

²⁰ Morey, Forbath, and Schoop, "With Big Data," Harvard Business Review.

A. MAROUN: CONCERNS OF DATA COLLECTION PRACTICES

want to change, the government can apply pressure on them to do so. The implementation of effective regulation and transparency measures is important because if data collection practices continue to go unchecked it will only negatively impact our right to privacy in the future.

Some may argue that customers should not worry that their data is collected and should just enjoy the benefits data collection provides. However, there is general concern by the American public on data collection. The Pew Research Center reports that 69% of adults are not confident that their activity on social media sites will remain private and secure.²¹ Another report reveals that 66% of adults are unconfident that search engine providers will keep their activity private and secure.²² Consumer apprehension shows that people do indeed care for their privacy online. Although there may be a select few who claim they “don’t care”, it does not mean that this matter should not be investigated and improved. Since data is important for businesses to remain competitive and efficient, companies should invest in encryption services. They can also destroy data after it is used, collect relevant data, and limit access to data to certain individuals in the company. If companies are transparent about their data collection practices, consumers will have more trust in the organization and would feel safer about the use of their data. For instance, Apple has taken steps to improve its transparency regarding data collection. The company has created a portal where customers can review the data Apple has collected on them.²³ Tim Cook, the CEO of Apple, has praised the GDPR and believes data privacy is a “fundamental human right”.²⁴ This has ultimately boosted Apple’s public image, and set standards for other companies to follow. Companies who implement transparency in their practices will see higher levels of customer satisfaction.

CONCLUSION

Transparency and regulation are two ways to lessen the invasiveness and risks of data collection. People have lost a sense of privacy on the internet and their sensitive data has turned into another source of profit for many organizations. Individuals also tend to be in the dark about what is truly being done with their information online. Many citizens care about their data but tend not to express their thoughts due to the lack of knowledge on the issue. Are people victim to the American corporate environment? Have they resigned to the system? Have citizens become complacent due to the lack of privacy standards online? The issues surrounding data collection can be seen as a violation to the Fourth Amendment of the United States Constitution. This amendment grants protection against warrantless searches or having anything taken away from someone without probable cause or good reason. What gives companies the right to surveil customers? Should they be able to take our information and store it, and to what extent? The dangers of data collection is a bipartisan issue that negatively affects American citizens. If companies adapt clear policies regarding data collection and if the government were to enact laws to control data collection practices, then this situation would greatly improve.

ACKNOWLEDGEMENTS

I would like to acknowledge my peers in my data privacy seminar course who have researched and presented information about data privacy issues. They have given me inspiration for this paper. My peers interviewed loved ones, analyzed social media privacy policies, and presented any other relevant findings to the class. This was useful for my analysis in this paper.

²¹ Mary Madden and Lee Rainie, "Americans' Attitudes About Privacy, Security and Surveillance," Pew Research Center, last modified May 20, 2015, accessed December 9, 2018, <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

²² Ibid.

²³ Nicholas Fearn, "Apple's Transparent Data Policy is a Lesson in How to Exploit GDPR," IT Analysis Business Insight, last modified December 10, 2018, accessed December 15, 2018, <https://www.itpro.co.uk/general-data-protection-regulation-gdpr/32509/apples-transparent-data-policy-is-a-lesson-in-how-to-exploit-gdpr/>.

²⁴ Ibid.

BIBLIOGRAPHY

- Atkins, Kimberly. "Facebook CEO Faces Grilling today on Data Mining." Boston Herald. Last modified April 10, 2018. Accessed December 12, 2018. <https://www.bostonherald.com/2018/04/10/facebook-ceo-faces-grilling-today-on-data-mining/>.
- Fearn, Nicholas. "Apple's Transparent Data Policy is a Lesson in How to Exploit GDPR." IT Analysis Business Insight. Last modified December 10, 2018. Accessed December 15, 2018. <https://www.itpro.co.uk/general-data-protection-regulation-gdpr/32509/apples-transparent-data-policy-is-a-lesson-in-how-to>.
- France-Press, Agence, and James Cook. "Amazon Investigates Reports that Staff Sold Customer Data." The Telegraph. Last modified September 17, 2018. Accessed December 8, 2018. <https://www.telegraph.co.uk/technology/2018/09/17/amazon-investigates-reports-staff-sold-customer-data/>.
- "GDPR Key Changes." Trunomi. Accessed December 9, 2018. <https://eugdpr.org/the-regulation/>.
- Horaczek, Stan. "Here's Why You've Been Getting so Many Privacy Policy and Terms of Service Updates Lately." Popular Science. Last modified April 26, 2018. Accessed December 15, 2018. <https://www.popsci.com/gdpr-privacy-policy-update-notices#page-2>.
- Instagram Inc. Instagram Help Center. Accessed December 9, 2018. <https://help.instagram.com/402411646841720>.
- Madden, Mary, and Lee Rainie. "Americans' Attitudes About Privacy, Security and Surveillance." Pew Research Center. Last modified May 20, 2015. Accessed December 9, 2018. <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.
- Morey, Timothy, Theodore Forbath, and Allison Schoop. "With Big Data Comes Big Responsibility DATA Customer Data: Designing for Transparency and Trust." Harvard Business Review. Accessed December 9, 2018. <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>.
- "Why do Companies Collect, Sell, Buy or Store Personal Data." The Windows Club. Accessed December 8, 2018. <https://www.thewindowsclub.com/why-do-companies-collect-sell-buy-or-store-personal-data>.