Website: http://www.gphjournal.org/index.php/bm

GPH – Journal
International Journal of Business Management

Research Article

ETHICS IN DATA COLLECTION AND ADVERTISING

Raheel A. Chaudhry[1], Paul D. Berger[2]*

Bentley University Waltham, MA U.S.A.

Corresponding author: Paul D. Berger, Bentley University Waltham, MA U.S.A.

Received Date: July 22, 2019
Published Date: July 31, 2019

Introduction:-

This paper will explore the ethical connotations within the current advertising methods used by companies who want to market their products online. Specifically, the paper will focus on how customer data is collected and used via targeted advertising and what the ethics behind this method of advertising are. While marketers argue that targeted advertising using customer information results in greater consumer market efficiency, by sparking customers' interests through tailored advertisements, many consumer privacy groups have questioned the ethicality of such practices (Jules, Ari 2011). Throughout this paper, we will explore the different ways a person's data is collected online, how that data is handled and who has access to this data, as well as the amount of control an individual has over his/her own personal data. There are pros and cons to both sides of the debate, on whether people deserve the right to their own privacy, as well as the benefits an individual gains from the current data selling and online advertising business models that have become so common in the digital world. Whether the average person knows it or not, almost everything he/she does online has been collected and used as data in some way or form. This paper is not trying to make the case that all data collection is bad or that no one should have access to our personal data. Rather the paper is exploring the ways in which companies collect said data and whether or not those methods can be considered ethical. Especially in terms of collecting sensitive consumer information, it is imperative that companies take measures to ensure consumer data is well protected..

DATA REGULATION

What data on a consumer are considered up for grabs? Research shows that consumers lack sufficient knowledge about how their information will be used by these firms that collect them and so, companies must do their part in not only highlighting to customers how their information will be used, but also in taking the necessary steps to ensure data privacy (*Culnan & Clark, 2009*). If you look at it from the point of view of a corporation, anything they can legally get their hands on is fine to use for marketing purposes.

This is especially important because the laws in America are overwhelmingly in favor of the corporate side on this account and much less in favor of personal data privacy. There is no singular federal law in America that covers data privacy; instead, citizens must rely on numerous federal and state laws that protect certain aspects of data privacy, often broken down by industry. The most effective way, outside of congress passing a federal law, for data protection laws to take place in America has come down to relying on other countries or large states to pass laws on their behalf. Because of how multinational most online platforms are, the decision of one major player in the geopolitical world to pass strict data privacy laws actually ends up affecting the entire consumer base.

This can be seen in the passing of the GDPR, the General Data Protection Regulation by the EU last year, following which almost every online platform had to revise their privacy terms and conditions to unilaterally follow the GDPR, because it is not feasible to separate consumers based on their nationality online. Instead of risking violating the GDPR by having two sets of rules for different users, companies merely updated their data collection and storage terms and conditions for all users. The GDPR, which came into effect in May 2018, protects consumers through giving them rights, such as the right to access the information they give to companies, the right to ask the company to delete their data if they no longer have a relationship with the company, and 6 other rights (“*GDPR, What Is It And How Does It Impact My Business”, CRM Blog, 2019*). These rights combine to give consumers the tools they need to fight for their privacy in the current data-driven world. This method of data protection has also been taken up by California. While Americans benefited from the passing of the GDPR, in that companies overhauled their terms and conditions, only Europeans are able to make use of the rights afforded by the GDPR. California is the first state to give Americans the same opportunities. Being the largest state economy in the country, California has basically passed data protection onto the rest of the country by changing their own data protection laws. There are very few, if any, companies that do business in America but not in California. The California Consumer Privacy Act, which goes into effect in 2020, will be the first major privacy act in America, following in the footsteps of the GDPR (“*Council post: Are you ready for CCPA”, Forbes, 2019)*. If these procedures are followed and consumers are well aware of how their data is being collected and used and where it is being stored, then there is little leeway for unethical issues to take place

DATA COLLECTION

Data collection can be done in a myriad of ways. These collection methods generally fall under three broad groups: asking customers directly, indirectly keeping track of customers, and by adding other sources of customer data to your own source (“*How and Why Businesses Collect Consumer Data”, Business News Daily, 2018*). Of these three methods, the one with the most ethical leg to stand on is asking customers directly. Getting data from customers directly, with their consent, is the most ethical way to collect data. This data collection can be done through the use of surveys, reviews, sales history, and through the creation of online profiles such as an Amazon account. However, the other two data collection methods mentioned earlier are where there is more room for ethical nuance to appear. Another common method of collecting an individual's personal data is by scanning the content of his/her emails and then pushing ads to the person based on the person's mailbox. This is done by many of the bigger email companies, including Google and Yahoo, who use your own emails to target you (“*Big Data: 8 Intriguing Ways Companies Can Use Your Data” Villanova, 2019)*. Once again, the end goal of these companies might be to enhance their customer database and improve customer experience through personalized ads; yet, the method they go about getting the necessary data to fulfill these methods is not the most ethical.

One of the more common forms of indirect tracking that is used by advertisers and data companies is by tracking online searches. Everyone has experienced the online phenomenon of being targeted by ads for a product after recently purchasing a similar product. This happens through the tracking of cookies. "Cookies" refers to information saved on your browser or your phone that keeps track of where you have been browsing online. This can be used by companies to target you with ads that fit the profile built by the cookies collected, such as sending ads to a user about graduate schools if they had recently searched for "the benefits of an MBA." There has been evidence of some smaller apps taking screenshots of a smartphone and sending that information to data-collection sites. Facebook imbeds a certain program in multiple websites throughout the internet to keep track of Facebook users who go on those sites, and aggregates the data to find out all of their online search history and trends. These forms of data collection, while not the most upfront, are in a bit of a gray area in terms of how ethical they are. One could argue that users should assume that anything they look up online or search is free game for companies to track. It can also be argued that companies should make users more aware that such tracking is going on, especially for the less tech-savvy consumers who might not even know what cookies are (*"Is Your Smartphone Secretly Listening To You?." Consumer Reports, 2019).*

Another major indirect data collection method available to companies is tracking users through location services. This can be done by using the IP address of the device that a person is using to track his/her location and then use that to stylize ads just for that person. It can also be used through tracking a person's smartphone, although this requires authorization from the user to allow apps to access your location services. By using these apps to track the user's location patterns, a unique profile of each user can be developed and the individual's lifestyle, preferences, and other endeavors can all be identified through the use of geolocation tracking. This information is then monetized and sold to third parties without users' consent and is done so in a way that is inconsistent with the app's data privacy policies (*"The Power Of Place: Geolocation Tracking And Privacy", Business Law Today, 2019*). As we have seen time and again in this paper, the laws surrounding data privacy regarding locations services are a gray area that allow for a lot of wiggle room for companies to still make use of and monetize user data, while adhering to the letter of the law.

When a user opens an app, say a map app, they opt into allowing the app to access their location so that they can make use of the service. Their phone uses GPS to track the real time location of the user and sends it to an aggregator company who then sends it to the app company so that they can complete their objective of giving the user directions. This is all legal and ethical and all parties are willing participants. But what ends up happening afterward is that the aggregator companies then take the data they received from the user and sell it to unrelated third parties, who monetize the data in various different ways. The majority of smartphone users have no idea that this is happening and that their location data are being sold to different companies who then use the data for various purposes, such as selling it to law enforcement agencies so they can track individuals. Also, there is no opt out feature for this data-collection method. *"The big U.S. wireless carriers—AT&T, Verizon, Sprint, and T-Mobile—were all working with LocationSmart, sending their users' location data to the firm so that it could triangulate their whereabouts more precisely using multiple providers' cell towers. It seems no one can opt out of this form of tracking, because the carriers rely on it to provide their service"* (*"The Power of Place: Geolocation Tracking And Privacy", Business Law Today, 2019*). This form of data collection can absolutely be considered to be unethical and unnecessary. And yet, due to the "profit over everything" economy that we live in, this secondary data market is growing year by year. *"IBM claims that 90 percent of all*

consumer data that is currently in circulation was created in the last two years. This industry is expected to generate $350 million dollars annually by 2020" (*"The Power of Place: Geolocation Tracking And Privacy", Business Law Today, 2019*). As long as corporations can get away with selling user data and make large amounts of money by doing so, these practices will continue with no real oversight.

The final major form of data collection comes from adding other sources of customer data to a company's own data records. This data method makes use of the secondary data market, where companies buy and sell data from all over the world. There are companies whose sole business is collecting data and selling the data to companies. They are often referred to as "List Enhancement Bureaus" (*Roberts and Berger, 1999*). The results of this data-collection method results in more robust data records as well as an additional monetary incentive to data collection in general. The money involved in the secondary-data market is extensive and growing as more data is created and processed every year. The secondary-data market is where advertising companies get the majority of their data, thanks, in part, to data giants such as Google selling their collected data to the highest bidder. *"While Google's most visible product is a search engine, and the company has expanded into just about every facet of modern existence, it has always been an advertising and data company at heart. "When you search, they know exactly what keywords you have, what history of keywords you've used," said Shavell. "They sell those to their ad networks, and people bid on them, and that's where they continue to make most of their money."* ("*How Companies Turn Your Data Into Money." PCMAG, 2019*). With the financial incentives available to companies who collect, sell, and buy data, there is no end in sight to regulating this market and consumer-data privacy without the use of laws. While the sale of aggregated data might not be considered to be ethical or unethical, the fact that the majority of the data collected comes from rather shady means leads to the fact that this form of data collection also has some inherent problems within it.

PRIVACY CONCERNS VS. BENEFITS

While there are many red flags relating to privacy concerns when companies ask users for their information, if done in the right manner, there are several benefits that can stem from user data collection. As noted previously, by collecting data through tracking the user's search history through cookies, or monitoring the customer's past purchases, companies can use the information gathered to generate personalized ads targeted to each individual's unique preferences. Often times, companies can also identify what the individual might like based on how much time he/she spends viewing a particular product online. This can lead to increasingly targeted ads not just online but also in brick and mortar retail locations. For example, while Dunkin Donuts aims to use technology to change the ad they display in-store based on a certain customer's appearance, big supermarket chains also personalize their coupons based on the customer's previous purchases (*Johnson, Justin, 2010).* What is the benefit of going the extra mile to create such personalized marketing? By providing users with recommendations based on the collected data, companies can improve the overall online experience for the customer and strengthen their relationship with the customer. Instead of pushing standardized ads to each user, companies now have the power to make each customer feel special as they can build a unique one-to-one relationship with each individual. Additionally, when companies personalize ads, they are able to catch the eye of customers who might not have previously even been aware of the advertised products. This means that if the right ads are shown to the right people, there are higher chances that these people buy these products; thereby, companies can make more effective use of their scarce advertising resources through targeting to the right people and generating higher returns (*"Benefits Of Targeted Advertisements: A Spotify Fail." eREACH, 2013*). The benefits also vary from the point of view of the consumer. It was found that 71% of consumers prefer personalized ads because this helps reduce the

likelihood of being flooded by irrelevant ads and it is also a way to discover new products online *("Study: 71% Of Consumers Prefer Personalized Ads." Marketing Dive, 2016*).

Another secondary benefit that comes from added efficiency, and affects online advertising, is the continuous availability of free content online. Because ads are so effective and can bring in a lot of revenue for the sites means that these sites can offer their services to online users for free or for reduced costs. For example, anyone can make use of Spotify or YouTube for free by just having to deal with listening to a few ads on each video or every couple of songs. Users can also opt in to pay for ad-free services if they are so inclined. The ad revenue for these sites, especially for less well funded sites and forums, pays for the server and maintenance costs of the sites. There is no guarantee that stricter data-privacy laws being in place won't lead to less efficient advertising, which will in turn lead to less revenue for the websites who show these ads. This might, in turn, affect the user experience for these sites and even lead to many sites shutting down because they can't afford to stay open with the reduced ad revenue. There is also the monetization aspect of YouTube videos to take into account. Content creators on YouTube make money based on the number of views their videos get. The decrease in monetization from ads might result in their receiving less money for the same number of viewers as before and could affect the content creation business on YouTube. Of course, this is based on conjecture, without knowing the full breakdown of how better data privacy laws would affect the online advertising business and the profitability of ads in general.

Moving on to the negatives of this data driven world, the most obvious one is that of privacy. With the extensive ways in which data are collected and processed in the big-data world, and the value that said data has to companies, it is almost impossible to imagine a life of privacy and anonymity. In such a world, it is imperative that we ask ourselves whether an individual has the right to privacy and if it means anything to have that right when a person's data can be collected so easily. The current model of how data are collected relies on consumers opting out of having their data collected when it would be much more practical to instead have users opt in to having their data collected. And, this applies only to data collection methods that rely on user agreement; as we have discussed previously, there are many more ways that companies can collect consumer data without the user being any the wiser. Some might want to respond to this by saying that using the internet or having a smartphone is a choice and that people who use them have passively opted into an agreement that allows their data to be collected. However, this becomes less and less justifiable as the technology era continues to expand and the need for technology becomes more of a necessity than an option in the current world.

Another major concern with the wide-spread collection of data that goes on now is the risk involved in data breaches and malicious parties buying consumer data on the secondary data market. Cambridge Analytica has been in the news again recently, a perfect example of how large amounts of data collection can go wrong. Cambridge Analytica was a political consulting firm with ties to the Trump campaign for president in 2016, that came under scrutiny when it was discovered that they, with the help of a loophole in the Facebook API, had harvested the data of over 87 million people and used said data to allegedly help steer the election to Trump's favor. The actual effectiveness of their campaign can be called into question, but the fact remains that they were able to breach Facebook's security and access millions of user's data and use it to their own benefit. The sale of the data collected maliciously and used for such shady means is one of the biggest concerns that come from the increase in data collection and the reduction of personal online privacy that is

currently ongoing. Facebook, for their part in this breach, was recently fined around $5 billion dollars by the United States Federal Trade Commission, a figure which some are saying is not high enough in comparison to the damage done by the breach *("Facebook to be Fined Record $5Bn, Reports Say." BBC News, 2019).* The risk of consumer data falling into a "bad actor's" hands is a major risk in the growing secondary data market.

The final concern that must be talked about is how little people actually know about their own data being collected online. The main ethical issue at play is that average people don't really know what is happening behind the computer screens when they go on Amazon and browse products or when they search for things in Google or when they do anything that is connected to the internet. The main thing that should be advocated for is transparency in how data are collected, why data are collected, what type of data values are collected, and the ability to stop your personal data from being collected. Legislation is needed for such practices to become the norm, as we can see by the example set in the EU via the GRPR. California's own version of the law that goes into effect in 2020 is a strong next step in America but what must really be done is to have this kind of legislation done on the federal level.

CAVEATS

Whether something is ethical or not is a very nebulous discussion. There are a variety of viewpoints that can be taken in any particular instance that can change the perception of the topic of ethics. As such, it is hard to label something as ethical or unethical without finding some sort of opposition to the labeling. In this instance, there might be continuous alignment on the current data-privacy collection methods having a certain unethical nature to them. Many forms of data collection can be considered above aboard and ethical. But, many other forms of data collection can be considered to be unethical and underhanded. Hopefully, a concession can be reached with everyone agreeing that something should be done to protect data privacy in some capacity. The specifics of what should be done to make sure that the data collection is ethical, of course, up for debate and would require more intense research than what was laid out in this paper. However, some kind of change is needed as we continue to head down this path.

REFERENCES:-

1. "*Benefits Of Targeted Advertisements: A Spotify Fail." eREACH. N. p., 2013. Web. 15 July 2019.*
2. *"Big Data: 8 Intriguing Ways Companies Can Use Your Data" Villanovau N. p., 2019. Web. 15 July 2019.*
3. *"Council Post: Are You Ready For CCPA?." Forbes.com. N. p., 2019. Web. 15 July 2019.*
4. *Culnan, Mary & Clark, Cynthia. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches.. MIS Quarterly. 33. 673-687. 10.2307/20650322.*
5. *"Facebook To Be Fined Record $5Bn, Reports Say." BBC News. N. p., 2019. Web. 15 July 2019.*
6. *"GDPR: What Is It And How Does It Impact My Business?." CRM Blog: Articles, Tips and Strategies by SuperOffice. N. p., 2019. Web. 15 July 2019*.
7. "*How Companies Turn Your Data Into Money." PCMAG. N. p., 2019. Web. 15 July 2019.*

8. *"Is Your Smartphone Secretly Listening To You?." Consumer Reports. N. p., 2019. Web. 15 July 2019.*

9. *IT. "How And Why Businesses Collect Consumer Data." Business News Daily. N. p., 2018. Web. 15 July 2019.*

10. *Johnson, J. (2011). Targeted Advertising and Advertising Avoidance. SSRN Electronic Journal.*

11. *Juels, Ari. "Targeted Advertising ... And Privacy Too." Topics in Cryptology — CT-RSA 2001 (2001): 408-424. Web. 15 July 2019.*

12. *Roberts, Mary Lou, and Berger, Paul D., "Direct Marketing Management," Prentice-Hall, 2nd Edition, 1999.*

13. *"Study: 71% Of Consumers Prefer Personalized Ads." Marketing Dive. N. p., 2016. Web. 15 July 2019.*

14. *"The Power Of Place: Geolocation Tracking And Privacy | Business Law Today From ABA." Business Law Today from ABA. N. p., 2019. Web. 15 July 2019.*