Data Profits vs. Privacy Rights: Ethical Concerns in Data Commerce

Amiah Armstrong
Old Dominion University

Data Profits vs. Privacy Rights: Ethical Concerns in Data Commerce

Amiah Armstrong

Old Dominion University

COVA CCI Undergraduate Research Program

April 12, 2024

Abstract

In today's digital age, the collection and sale of customer data for advertising is gaining a growing number of ethical concerns. The act of amassing extensive datasets encompassing customer preferences, behaviors, and personal information raises questions of its true purpose. It is widely acknowledged that companies track and store their customer's digital activities under the pretext of benefiting the customer, but at what cost? Are users aware of how much of their data is being collected? Do they understand the trade-off between personalized services and the potential invasion of their privacy? This paper aims to show the advantages and disadvantages of consumer data commerce. It examines the dynamics between consumers and their dwindling expectation of privacy, taking a dive into the implications of User Agreements and closely analyzing the controversies surrounding it. Possible solutions to address these ethical concerns that can be immediately implemented in today's practices are also provided.

What and how is data being collected?

Customer data collection is not a new phenomenon. Companies have long been utilizing this strategy to maximize corporate profits. One example of this involves the retail corporation, Target, which used data analytics to anticipate whether their customers were expecting a child. This specific demographic was identified based on those customers' interactions with products that, when purchased together, indicated a high likelihood of them being pregnant. Subsequently, those individuals were sent tailored, pregnancy-related coupons (Hochheiser, 2015). Another example involves the transportation network company, Uber, and their infamous "Ride of Glory" controversy. In a now deleted blog post on their official site, Uber revealed that they track their customer's one-night stands. To prove that fact, data was released to show that Boston, San Francisco, and Washington D.C. had the highest frequency of such rides (CBS, 2014). Both of

these instances increased user personalization: Target by tailoring advertisements specifically to the needs of pregnant women and Uber by improving service during peak times. There are countless other examples of companies collecting and analyzing the patterns of their customers, known and unknown. But by doing this, they push past the line of customer comfortability, raising concerns about ethical data usage.

In the past, data collection primarily relied on traditional methods such as customer surveys, feedback forms, and loyalty programs, all designed to gain insights into consumer preferences. However, the introduction of the e-commerce and social media platforms has led to a period in which copious amounts of data are being produced at an astonishing rate. Companies now have the ability to track online activities, monitor purchasing patterns, and analyze social interactions in real-time.

There are four types of data companies collect. There is Personal Data, which relay details about individual customers. Some examples are name, date of birth, and credit card information. There is Engagement Data, which tells how the customer interacts with brands, including website visits and customer service calls. There is Behavioral Data, which is how the customer responds to products, services, or marketing efforts. And then there is Attitudinal Data, which relates to the satisfaction, dissatisfaction, and generalized sentiment towards a brand (Davis, 2023). These four elements combined capture the entirety of an individual's online presence, and a considerable number of companies have acquired this knowledge. The golden standard is Personal Identifiable Information (PII), which is any form of information that can be used to directly or indirectly uncover one's identity (CSO, 2022). PII is used to target the specific user, and in its most nefarious use, can be used to commit crime like fraud and identity theft.

How data is collected matters, as it is collected through various methods, with the most ethical one being directly from the users themselves. Have you ever witnessed a YouTube advertisement that prompts a quick survey before continuing to the video you chose? What about being stopped mid-scroll on TikTok and asked how you felt about the video you saw seconds before? This is a strategy for gathering data, and you have full authority over it. However, the same cannot be said for others.

One particular type of collection is referred to as location-based advertising. This is a tactic that tracks the IP addresses of devices like smartphones, laptops, and apple watches. It is used to fix the overwhelming quantity of advertisements by using technologies like GPS to accurately pinpoint the location of customers, thereby enhancing the relevance of advertisements they will receive (Bauer, 2016, pp. 161-163). Geofeed is a tool commonly employed in location-based advertisements that allows for the delivery of information that is selectively filtered based on an individual's geographic location (IPinfo, 2021). By leveraging geofeeds and location-tracking tech, companies can make their advertising campaigns more effective and efficient by delivering contextually relevant messages to consumers' physical locations.

Another is the use of cookies, which monitor a user's browsing activity on particular websites. They can be described as personalized bookmarks because of their ability to save a user's credentials, record web sessions, and match preferences. Several websites advise their users about the usage of cookies and request permission; nevertheless, if the user declines, there is a chance they will be denied access to the website in its entirety. This fosters a misleading illusion of choice, pressuring users to ultimately accept those cookies anyway.

Furthermore, the challenge of maintaining control over personal data intensifies when companies opt to sell the information entrusted to them. While users and companies agree to

share data for specific services, the situation shifts when companies decide to monetize it by selling to third parties. One example of this is the Cambridge Analytica scandal. In 2018, millions of Facebook users used a personality quiz app called “This is Your Digital Life” that harvested tons of personal data about them. Users gave consent to this app to collect their information, but they did not give consent to Cambridge Analytica, the consulting firm that it was sold off to (2018, Langone). Users are frequently uninformed of what personal information will be shared with external entities, when it would happen, and where it ends up. And most of the time, that is intentional.

So the big question is, who benefits from this?

Benefits

The main reason that companies track their customer data is to improve personalization of their services. By tracking the clicks, website visits, and searches, it enables companies to customize their products, services, and marketing to suit individual users. This, in turn, optimizes their experience (Freedman, 2023). So do not be surprised if you see an ad for dog leashes after yours breaks- it is likely not a coincidence.

With knowledge that includes a customer’s behavior and preferences, companies can develop advertising campaigns that relate to individual users. One example being skin-care products. An individual with a dryer skin type is more likely to buy products advertised to hydrate their skin instead of products designed to dry it further. This maximizes the impact of a company’s marketing efforts, effectively reaching the right audience with the right message at the right time. By analyzing customer data, companies can also pinpoint areas for improvement, innovate according to customer preferences, and adapt to market trends (Graeff and Harmon,

302-303). This system also helps to lower the possibility of irrelevant ads, leading to a more enjoyable user experience.

Corporations profit greatly from this system, mainly in terms of money. However, a large portion of revenue also comes from selling it to third parties. Selling customer data can be a significant source of revenue for companies because it is valuable to other companies that rely on such data for targeted advertising, market insights, and to gain a competitive advantage. By exchanging data, companies create a win-win ecosystem, using gathered information to boost finances and strengthen their competitive position. Though beneficial to companies, the sale of customer data raises ethical concerns surrounding user privacy and consent.

Ethical Dilemmas in Data Commerce

Corporations selling their customer data to third parties is a widespread practice. It is viewed as a lucrative revenue system because of the large amount of personal data that is being collected daily. This data is a goldmine to companies who want to stay on top of trends and formulate strategies to increase revenue.

One way data can be sold is through database marketing companies like Acxiom and Experian (2019, Pasternack). These companies act as a “middleman” between ones who collect data and those who want to purchase them. They can be thought of as Amazon, but our personal data is the merchandise. Another way to sell data is from partnerships. A pharmacy may need help marketing their products and ask healthcare providers for anonymized patient data, medication usages, and medical histories. The same can be said between insurance companies and car manufacturers, where insurance companies need information that can curate driver risk profiles. Companies who have a direct relationship with consumers or access to valuable data may leverage alliances to monetize this information. That is when partnerships are formed. Many

industries already have this kind of symbiotic relationship with telecommunications companies (2022, Recio). With e-commerce and online advertising, selling the data to companies who also claim to need it can be a significant source of income for both sides. But by doing this, they walk a fine line between maximizing profits and respecting customer privacy rights.

Alarming statistics highlight the extensive data collection, emphasizing the widespread nature of this practice. For example, Walmart's transactional database contains 40 petabytes of data, exclusively collected in a few weeks (Marr, 2017, p. 8). This massive number is only data gathered in a short amount of time, so imagine the amount that is gathered in a few years. By retaining such vast amounts of data, companies become prime targets for hackers and malicious actors, thereby unleashing a multitude of security risks, like opening Pandora's box. Identity theft, financial fraud, and ransom attacks are only a few of the types of attacks customers would be vulnerable to. And it becomes even more difficult to keep consumers safe when their data is sold to third parties, increasing the number of potential targets for malicious actors. The original company has little to no control over how the data is secured once it is in the hands of third parties, as these entities may not uphold the same security standards.

When consumers click "I agree" on the Terms and Conditions, they are believed to be legally bound by the agreement, even if they have not thoroughly read or understood them. Companies take advantage of this by filling the document with broad, complex jargon, incomprehensible to the common individual. They might make that document hundreds of words long, when only a few bullet points would suffice. They may even gift the user an "auto-scroll" feature, prompting the individual to skip past the convoluted details in order to gain access to the website quicker. It is presented in a way to make it easier for the user, when in reality, serves as convenient loopholes for companies to infringe upon user's rights, particularly the ownership of

their own personal identifiable information. And once in possession of that information, the company gains free reign to analyze and distribute that data in any way they see fit.

It begs the question: Is our information still personal?

While users willingly share their data with platforms and services, the degree of control they have over it is minimal to none. The data that is being collected is often obscured. Where it ends up after being sold is nearly impossible to track. Companies might claim ownership of the data they collect, using user agreements that give them extensive rights to utilize and profit from it. However, this viewpoint fails to recognize the inherent worth of that data, which frequently contains personal and private information about the individual's existence. This action, on its own, can be seen as a violation of personal privacy. Individual profiles gathered from preferences, behaviors, and personal details can be used in ways that users may not be comfortable with or may not have explicitly consented to, but must abide by because of the initial agreement.

Privacy norms are also diminishing as individuals become more acclimated to constant surveillance. With each store visit and online click, there is a slight sensation of being "watched". This phenomenon is tolerated by a significant portion of our society, possibly in exchange for the convenience and efficiency from what being complacent provides. As the regular individual lowers their standards for personal privacy, companies exploit it for their own gain. After years of this, acceptance becomes deeply rooted, causing the line between public and private domains to blur. This, in turn, results in the increasing lack of autonomy within the average individual. The essence of the matter lies in the delicate trade-off between the economical benefits derived from the collection and sale of customer data and the ethical consequences associated with the violation of privacy.

Changes to Protect Privacy Rights

There are few changes that could be made that would effectively benefit both corporations and their customers. Companies are in constant competition with themselves, seeking more and efficient ways to boost their income. It is difficult to determine solutions that would keep that competitiveness without infringing on their user's rights, but implementing at least one of these recommendations could be the start of a more ethical and sustainable approach to data commerce.

Transparency and Informed Consent:

When making the collection of user data more ethical, the first step is to prioritize transparency and informed consent. Using broad explanations and complex terminology within User Agreements is considered manipulation, simply because it intentionally hides the company's true motives. It is imperative that companies are thorough and direct with their users because they deserve to know what is being taken and why. That information should also be easily found whenever needed. Any changes to those agreements should be sent to the user directly, highlighting what exactly has been changed. Not only that, but they should be able to follow their data if it ends up with new recipients. By providing complete transparency, users can fully comprehend the terms they agree to, allowing them to make informed decisions about it.

Limited Availability:

Users should be able to control who has access to their information and who does not. This is a right that is expected, but sadly not enforced. Once a user grants permission for a company to have access to their data, that does not mean other companies have full, unrestricted access to the same. It is the original company's responsibility to prioritize the privacy of each

individual. Simple measures like utilizing strong encryption, having regular security checks, and even asking that user before sharing their sensitive information are just a few examples. If the data is protected, so is the integrity of the company. Mutual respect plays a vital role in establishing a strong foundation between companies and their customers, which can be built by limiting the availability of their customer's data.

Option to Opt-Out:

Users should be granted the right to withdraw their data from a company once they have shared it. As it stands, users have minimal options to reverse their decision once they have already disclosed that information, especially if that information has already been sold to a third party company. Not only will giving the customer an option to take back their data respects their autonomy, it also enhances the trust between the user and company. Coupling this with complete transparency about any changes of data usage, transportation, and providing prior notice to the user are essential. So, in the event that the user decides to alter their decision later down the line, they can do so. Furthermore, it is imperative that this option offers user-friendly interfaces, ensuring that the execution of tasks is both swift and straightforward.

Reward Programs:

Providing an incentive enhances users' willingness to share their personal information. Examples such as discounts, raffle prizes, or points are among the methods that can pique user interest and lead them to permit certain practices. This, on its own, exhibits greater ethical soundness as it provides advantages to all parties involved. Companies benefit from easy access to customer data, while customers benefit with tangible prizes in exchange for their information.

Closing Thoughts

A large chunk of human life is spent over the internet. The digital realm is vast and nearly impossible to get away from. With every click, scroll, and google search, a trail of invaluable digital footprints are left behind to encompass the entirety of our technological lives. Overtime, each individual profile becomes more comprehensive, painting a detailed portrait of each user's digital persona. Corporations use algorithms and analytical techniques to monetize this information, and by doing so, pushes past the ethical boundaries that cross into a user's privacy and autonomy. And society permits it. Is the long-term implications of data commerce worth the continuous erosion of privacy norms? While the average individual continues to stay complacent with the misuse of their personal information, corporations get richer and privacy rights become forgotten. If there is to be change, it has to start with the community because that is where these issues arise the most. The government often exhibits a passive approach in addressing these privacy concerns until the voices of the community become loud enough to demand action. Meaningful change occurs when individuals unite to raise awareness, leading to legislative actions that safeguard privacy and ensure corporate accountability. Transparency, informed consent, limited availability of data, the option to opt-out, and reward programs are a good start to prove that they care about their users' rights. By fostering a culture of mutual respect and accountability, we can strive to create a digital landscape where individuals have greater control over their personal information and where the benefits of technological innovation are balanced with the preservation of fundamental rights.

References

Bauer, C., Strauss, C. (2016, January 16) *Location-based advertising on mobile devices.* Manag Rev Q 66, 159–194. https://doi.org/10.1007/s11301-015-0118-z

CBS Interactive. (2014, November 19). *Uber crunches user data to determine where the most "one-night stands" come from.* CBS News. https://www.cbsnews.com/sanfrancisco/news/uber-crunches-user-data-to-determine-where-the-most-one-night-stands-come-from/

Davis, L. (2023, October 5). *What is customer analytics? (2024) guide*. Forbes. https://www.forbes.com/advisor/business/customer-analytics/

Freedman, M. (2023, October 20). *How Businesses are Collecting Data (And What They're Doing With It)*. Business News Daily. https://www.businessnewsdaily.com/10625-businesses-collecting-data.html

Fruhlinger, J. (2022, January 10). *What is PII? Examples, laws, and standards*. CSO Online. https://www.csoonline.com/article/571817/what-is-pii-examples-laws-and-standards.html

Graeff, T.R. and Harmon, S. (2002), "Collecting and using personal data: consumers' awareness and concerns", Journal of Consumer Marketing, Vol. 19 No. 4, pp. 302-318. https://doi.org/10.1108/07363760210433627

Hochheiser, M. (2015). The Truth Behind Data Collection and Analysis. *UIC John Marshall Journal of Information Technology & Privacy Law*, 32(1), 32–55. https://repository.law.uic.edu/jitpl/

IPinfo. (2021, September 17). Geofeed: What is it and how to set up a right one?. IPinfo blog. https://ipinfo.io/blog/what-is-geofeed-how-to-it-setup/

Langone, A. (2018, April 4). *What to know about Facebook's Cambridge Analytica problem*. Time. https://time.com/5205314/facebook-cambridge-analytica-breach/

Marr, B. (2017). *Big Data in practice: How 45 successful companies used big data analytics to deliver extraordinary results*. J. Wiley.

Pasternack, A. (2019, February 3). *Here are the data brokers quietly buying and selling your personal information*. Fast Company. https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information

Recio, P. U. (2022, July 27). *Council post: How companies are building data partnerships with Telcos*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/07/26/how-companies-are-building-data-partnerships-with-telcos/?sh=2c5d7c777f8c