Sebastian Olmos

Professor Nithyanand

Intro to Networks and their Applications

9/1/2022

Internet & Social Media Data Privacy

As a user of the internet, I am constantly being bombarded with ads that are tailored towards my recent searches or the current location that I am in. I see these advertisements show up on my Instagram feed about shoes that I searched for a week ago on Nike.com from my laptop. These instances happen quite often and have gotten to the point where I am almost preparing myself to see advertisements from stores that have the exact or similar products to the ones I looked at previously and fighting the urge not to buy it. Although I was frightened at first with how much knowledge and how specific the advertisements have gotten, it sparked my interest as to how interconnected these different platforms are and how they built a profile unbeknownst to me and were able to implicitly incorporate it into my internet browsing. Where I see my internet use as aimless scrolling and clicking, I've learned that each decision I make is considered and is used as a metric for these social media and advertisement companies. They track just about everything, time spent viewing, time of scrolling, likes, saves, interests, searches, etc. I'll take a deeper dive and see just how private we really are and how much the internet knows about us.

I am going to be looking at not only what companies do with our data but also how they gather it and the reason why this market has become so lucrative. Data is a hot commodity but only to certain companies who thrive off high volumes of personalized customer engagement, we will see which companies are players in this data frenzy., I will also investigate bigger social media data privacy violations that have occurred with well-known platforms such as Facebook, and Twitter and what the government as well as some companies have implemented to try and be as transparent with the users as possible about their data.

Online retailers as well as other companies who aim to make their customer experience as personable as possible, use a feature called HTTP cookies. What the objective of these cookies is to identify who is browsing their site and use previous information to tailor their experience to items that match what they predict the customer would want. According to an article by Kaspersky, cookies are used for:

1. Session Management
2. Personalization
3. Tracking

While the intended idea was to benefit the user, cookies have taken a malicious turn because of their vulnerability to being hijacked. Different types of cookies pose different threats, 3rd party cookies are especially dangerous because they allow advertising companies to track users scrolling through any website with their advertisements on it regardless of what content that site contains.

Beyond just cookies that can help with target advertising, social media apps track our data using three main techniques, accessing phone and email contacts, tracking user behavior and browser history, and lastly location tracking. Using those three techniques, social media companies paint a better portrait

of who we are not only to provide more suggestions on our feed that keep us engaged but also sell our data to advertising firms or companies who utilize target advertisements to sell their products.

You may be wondering, what benefit tracking and selling our information has on social media platforms? To answer that question: it provides a large amount of revenue for the social media company and far more user traffic of interested people in the vendor's product. If we take Instagram for example, there isn't really any large profit they earn from just simply having users. Instagram does not have a yearly subscription plan, a cost per profile, or a time limit that makes users pay for the time spent on the app. Instead, they implement advertisements within the feed that ad companies pay for which contain links to their storefront. Instagram has also added a marketplace where companies can advertise their products, and it has even taken the place of the "profile activity" button. According to Investopedia, "It (Facebook) collected $69.7 billion in advertising fees, and a hefty portion of this income came directly from Instagram." This large amount of revenue provides great reason as to why Instagram has only further focused their platform on vendors and ads.

Target Marketing is the form of marketing that the social media companies are using. The idea is that instead of bombarding random user's social media feeds with ads, only specific groups of people see these ads based on three subcategories of market segmentation. The first subcategory is demographic segmentation. Social media companies learn about your gender, age, income level, Race, etc. from profile creation as well as what types of accounts you follow or interact with. The second segmentation is Geographic, a majority iPhone users have seen the modal appear when they first open an app or search on google, "(This app) would like to use your current location" having the user location is great for hyperlocal activity especially for smaller businesses who only serve in their specific community. Lastly the psychographic segmentation is basically the way our data splits us up economically. From the article, "What is Target Marketing?" by Susan Ward, she explains that we are split into six social grades with social statuses that range from Upper class which is for occupations such as higher managerial or administrative professionals to the subsistence class which is for people who are unemployed or seasonally employed. With these three segments, any company can utilize the data that the social media companies possess and find their audience for fees per ad click ranging from one to two dollars depending on the platform.

Data scientists and software engineers who work for the social media companies are the ones who are using our consumer behavior and predictive analytics on the backend to find audiences for these advertisements and generate more revenue for the company. Where the data is stored depends on the social media company. Facebook and Twitter are web2 social media companies and all their data is stored on physical servers also known as server farms. The reason for these servers is so that the data can be accessed regardless of if the user is online or not. Although it is evident that the companies are accessing and using our data, there is not much information regarding the specific tools the software engineers and data scientists use once they have this data. Being as vague as possible makes sense for big tech companies because they would not want the public knowing truly how much their data scientists are able to see about the users, as that would hurt the brand and leak company secrets. It is certain that they focus on the topics of big data mining, machine learning, and database management software in creating new models and advancing their ability to predict user behavior.

Facebook has been the frontrunner for social media platforms that have been in different legal troubles and lawsuits. One instance occurred from 2010 to 2011 where they were caught doing illegal user tracking outside of their platform. Several websites incorporated the Facebook "like" button on their page and using cookies, Facebook was able to obtain user data and track the person on that site and gather more data that they would not have had just on the Facebook App. This only further proves that

Facebook's reach is far greater than what the user is doing while they are browsing their Facebook account and feed. Another prime example of Facebook's tracking and privacy violations occurred within the last year and as of now only Illinois residents have received settlement for it. Facebook used biometric scans and facial recognition data from tagged photos to grow their user advertisement profile. The data led to bigger issues because once the AI gathers enough photos of the user, they utilize auto-tag features and can recognize a user even if the account was not manually tagged by the one posting the photo.

Not only has Facebook seen backlash for their wrongdoings, Twitter has also violated privacy laws by claiming to only use user's phone number and email for security purposes, when in reality it was also being used in advertisement tracking without letting them know. The activity that occurred was between 2013 and 2019. Because of this misleading, Twitter payed $150 million in settlement fees and must now notify users within the US who joined prior to September 2019 that they comply with the new measures put into place and provide the user with options on how they want to protect their data in the future.

The government responses have been relatively sporadic, occurring state by state but as we are learning more about how social media companies are violating security measures more states are following suit and integrating further safety protocols for users to maintain their privacy. One law that has taken into effect is the California Consumer Privacy Act (CCPA). The CCPA forces businesses to share the information they have about their customers/users and allows users to request deletion of their personal data from the servers of the businesses. While this is a big milestone for internet privacy, there are many ways that companies can work around these laws. In the article, "Four possible loopholes in the California Consumer Protection Act (CCPA)", author Johnny Ryan states, "We are troubled by the Act's exception for personal information to be used or shared when necessary to perform a 'business purpose'… A business purpose can include: "… *providing advertising or marketing services, providing analytical services, or providing similar services on behalf of the business or service provider.""* Ryan and the team at Brave Software, Inc. shed light to the loopholes that the social media companies still have after the CCPA.

Another recent feature in the fight for data transparency that Apple has implemented is the "Ask App Not to Track" button that appears in a modal after an app is installed. The reason for this is to show Apple users that they are providing an option so that third party applications and cookies won't monitor what you are doing when using the app. On the flip side, applications can still track behavioral data and find out who the user is based on their IP address as well as phone number. The wording for the button also follows in the same pattern. The reason for adding the word "Ask" at the beginning and not "Do not Track" is because Apple has no way of being able to enforce that all methods of tracking are not being used. The button is yet another method of seeming like a solution but instead just a way to have people think they are being cautious and private. The button is analogous to the pedestrian walkway button across intersections, it is said that some of the buttons across metropolitan cities are not connected to the stop lights but instead just there for the pedestrian's mental reassurance that the light will change sooner now. In essence, we do not truly know if these apps are monitoring and taking our data. The only sure way of knowing is being a developer for one of the apps or websites and being able to take a deep dive into the meat of the code.

After my research on internet and social media data privacy, I first am going to strongly consider investing in a reliable VPN, second have given a lot more thought as to how I have been vulnerable in my web browsing and social media use. I have been a user of social media apps practically since I was in middle school so to think that these companies know more about me than say my parents, that just absolutely fascinates and frightens me. As I mentioned in a previous paragraph, the data that is out there already cannot be deleted as there are servers that withhold the information, going further I will really

give more thought about my actions on social media and be sure to not register my phone and email to just any site.

Credit

- https://www.kaspersky.com/resource-center/definitions/cookies
    - Provided an understanding of types of cookies as well as how they worked and what makes them useful for companies but sometimes harmful for users.
- https://www.loyola.edu/academics/emerging-media/blog/2017/3-ways-that-social-media-knows-you-better-than-your-friends-and-family-do
    - Gave me 3 unique overarching examples of how social media knows us more than we realize.
- https://www.thebalancesmb.com/target-marketing-2948355
    - Gives overview of what target marketing is and how it is used.
- https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=13c99cfb2d6c
    - Explained what data selling is and how social media CEO's have skewed a narrative that they really aren't selling our data and that it is a completely legal practice.
- https://leadsbridge.com/blog/ads-cost/#21-facebook-ads-cost-in-2022
    - Graphs and information of how much Facebook/Instagram has made through ads.
- https://www.cnbc.com/2022/05/25/facebook-paying-users-over-data-privacy-lawsuits-google-could-be-next.html
    - Facebook facial recognition lawsuit in Illinois.
- https://topclassactions.com/lawsuit-settlements/open-lawsuit-settlements/facebook-external-site-user-tracking-90-class-action-settlement/
    - Facebook "like" button cookie tracking across the web.
- https://topclassactions.com/lawsuit-settlements/open-lawsuit-settlements/facebook-external-site-user-tracking-90-class-action-settlement/
    - Twitter claiming use of phone numbers and emails is for account security but instead using it for advertising.
- https://oag.ca.gov/privacy/ccpa
    - Explains what the CCPA is and the reason for why it was made.
- https://brave.com/brave-ccpa-mar-2019/
    - The CCPA has many loopholes that businesses can take advantage of.