Attitudes Towards the Valuation of Data Privacy on Social Media

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Daniel Le

Spring 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signed: Daniel Le Date 05/11/2021

Daniel Le

Approved: _____ Date _____

S. Travis Elliott, Department of Engineering and Society

Introduction

Issue

In contrast to their limited functionalities in years past, social media platforms have exponentially expanded into cultural powerhouses. Beyond providing a means of communication between people, they now also represent news outlets, marketplaces, information archives, and education centers. Combined with ever-increasing availability of internet connections and portable devices, social media has woven its way deeper and deeper into everyday life. Despite most of these platforms being free to use, the companies that provide them are among the most valuable entities in the world. If there is no profit to be made from using the services, then that revenue must come from elsewhere. In fact, the overwhelming majority of money made comes from targeted advertising in which users are selectively chosen to be shown ads based on their online behavior. In order for the most effective targeting, companies must retrieve extensive insight on user accounts, including and not limited to search histories, link clicks, time spent scrolling, and GPS pinging. How much of this is warranted, let alone permissible? How is it that social media companies have become so profitable off the details of our lives? This paper shall evaluate how current trends in society's perception of the internet have contributed to big data and its controversial roles.

STS Framework

In order to interpret the factors that play into public attitudes towards data privacy, the Social Construction of Technology (SCOT) framework can be employed. An important distinction that SCOT makes is that human behaviors shape the progress of technology, not the other way around. The technology in question cannot be analyzed by itself; its performance is

dependent on the people that utilize it. SCOT provides formal criteria to which social media and privacy rights can be evaluated, rather than blindly trying to extract relevant points of contention from a vast source of information.

There are five main tenets of SCOT: interpretive flexibility, social groups, design flexibility, conflict, and closure. The former simply asserts that every example of technology is viewed differently by different people. There can be multiple competing opinions regarding the issue, and each has a valid justification for their belief. These differences are due in part to the concept of relevant social groups. Stakeholders of a technology approach the technology from many perspectives, and their expectations are dependent on their individual backgrounds and use cases. Consequently, the development of technological principles is difficult to succeed in appeasing each and every social group. The problems and conflicts concept gives rise to design flexibility, which understands that despite there may be one prevalent implementation or interpretation of a technology, that is by no means the only viable option.

As social groups gradually compromise on a solution, interpretive and design flexibility give way to closure, which is when society perceives the technological problem as being sufficiently solved. It may not be entirely resolved, but the opinion would be that there is no need to search for other ideas. Conversely, the technology at hand could be redefined to apply to a different problem. Whether the option is satisfied or shifted, closure is only a temporary state. SCOT allows for new social groups to introduce new perspectives that may call into question the viability of a design at any point.

Background

Before interpreting attitudes toward data privacy on social media, it is important to contextualize how prevalent social media's reach is into society. As of early 2021, nearly sixty percent of the world's population actively use the Internet. Out of that group, 92.6% are reported to use mobile devices as a primary means of accessing it (Statista, 2021). Other surveys reflect that 83% of all internet users are involved with some form of social media, with 99% of them logging on via their mobile (Dean, 2021).

As a result of their deep presence, the industry has become hugely profitable. Facebook alone is the eight most valuable company in the world, valued at $757 billion. Furthermore, an astounding 97.9% of its annual revenue is in thanks to selling ad space on its sites. Advertisers compete to promote their products or ideas on users' timelines, and engagement on these posts collect insights that can be used to fuel subsequent ads (McFarlane 2020). At the root, the users are the ones driving the process, yet the average account receives little to no recognition or compensation for their information.

While many terms and conditions agreements permit the social media company to access user statistics, the desire to perpetually increase profit margins have resulted in them overstepping their promised limits. The infamous Cambridge Analytica scandal involved Facebook secretly disclosing detailed insights on nearly 87 million of its users to external entities. CA was able to manipulate the information such that users could be categorized to receive biased political messages. These messages were designed to be as subliminally convincing as possible in order to influence upcoming elections (Isaak & Hanna 2018). This discovery was a shocking revelation that not only was user data not as protected as many had

imagined, but also that there were ethical risks to having one's information feed manipulated without knowing.

Social Construction of Technology (Analysis)

According to SCOT, it could be inferred that the issues of privacy are not *caused* by social media. Rather, social media is just a catalyst that exposes the flaws among the userbase. Why is it that social media platforms have as much free access to user data as they do? Considering three major relevant social groups: users, developers, and advertisers, there is expectedly a high degree of interpretive flexibility when it comes to valuing data privacy. In order for the status quo to reach the point that it has, one group's agenda must have come out on top, with other groups adjusting their expectations to compensate.

As mentioned before, users represent the base of the social media empire, for their usage is what drives the entire moneymaking process. Privacy literacy is a concept that refers to one's understanding of their digital presence and how to control it. There is a positive correlation between those that are more privacy-literate and the amount of effort dedicated to securing their account data. Approximately 72% of Americans surveyed expressed some level of concern about their data (Symantec 2019), but concern does not directly lead to higher literacy. In a five-question quiz about proper privacy practices, only 3% of participants were able to answer all questions correctly, and just 70% could manage at least one correct at all (Bartsch & Dienlin 2016). What may increase literacy however, is education about privacy rights as well as active management of app settings. School-aged children who were taught about how their information could be used against them for persuasion "had higher feelings of privacy intrusion…and eventually higher engagement in privacy-protective behaviour," (Desimpelaeer & Van 2020).

Having knowledge of where one's information goes may encourage users to take more initiative in limiting app permissions on their devices and avoiding posting identifying information.

In addition to an education discrepancy, there appear to be generational divides in attitudes towards data privacy. In a comparison of responses from five generations: Greatest Generation (-1928), Silent Generation (1928-1945), Baby Boomers (1946-1964), Generation X (1965-1980), and Millennials (1980-), there was a general trend of higher trust of governments and corporations as time goes on. All groups surveyed hold a consensus that wrongful breaches of information are disapproved of, but suspicion that these breaches are likely to happen generally decrease with each subsequent generation. Regan et al. (2013) surmises that this may be due in part to increasing interactions with technology with time. Newer generations are able to become accustomed with the Internet earlier in their lives, and be more comfortable with adopting it as a commonplace tool. In an era of instant information, quick gratification is highly valued, and users may be more easily inclined to relinquish the rights to their data in return for the latest media.

While it may be in users' interest to protect their data, the companies that provide the social media service have a different goal – to grow their business. Increasing both the quantity and effectiveness of in-app advertisements should expectedly increase a platform's value in the market. In order to offer more relevant products and services, advertisers require more insight to users' interests and behaviors. When advertisers are able to be make more money, the social media that provides them these outlets share in the success as well. Thus, the companies are incentivized to gain as much access to user data as possible. In this regard, out of the three major social groups at play, two share a convergent goal that conflicts with the individual's desire for privacy.

Haida and Rahin (2015) identify five criteria that companies must evaluate in order to maximize their advertising effectiveness: product awareness, value, informativeness, entertainment, and irritation. The first term is vital to brand equity, as one cannot generate sales unless consumers know they exist. The market for ad space on Facebook has continued to grow, with the average cost per thousand impressions (CPM) rising from about nine dollars USD in early 2020 to over fifteen dollars in May 2021 (Revealbot, 2021). Value and informativeness deal with the quality of the advertisement. With a small window of opportunity, i.e., one post on a timeline, advertisers must communicate their product as providing some kind of inherent benefit in order to create interest. Not only must ads be descriptive, they must be engaging. Social media places enhanced emphasis on positive first impressions. Customers are highly likely to be drawn in with aesthetics and engaging interactions. The digital medium provides almost unlimited potential for creativity when it comes to aesthetics and entertainment, thus advertisers must leverage consumer interests to stand out from the rest. Somewhat ironically, ads that optimize these previous four criteria are not guaranteed success unless they can minimize the fifth one: irritation. The internet is a realm in which trends move quickly, and the line between popular and annoying can be exceptionally thin. Consumers may not be affected by ads the way advertisers intend, and a negative perception of a brand can rapidly sink its prospects. One method to minimize the corporate vs. user dynamic is viral advertising. Rather than appealing directly to users, advertisers make use of the "social" part of social media. They attempt to manufacture new trends by emulating other users. News feed posts, shared articles, and direct group messages about a product have proven to be effective measures because the average social media user is more likely to positively engage with other (perceived) users, rather than a business (Chu, 2013). This kind of insight into consumer tendencies would not be possible

without collection of personal data. Engagement statistics must be gathered to determine potential markets, communication analysis is necessary to understand public perception, and contact information is required to reach a specific consumer base. Expectedly, social media companies in this case are the middleman between users and advertisers, and they play an important role in how much data may be disclosed. While laws exist to protect the consumer, companies have been shown to capitalize on the trend of decreased privacy literacy to write intentionally vague user agreements that allow this data to be divulged. Of a subset of mobile applications reviewed, 68% were deemed to have an "unacceptable" lack of transparency in their terms and conditions, yet were still available for download and use (O'Laughlin 2019).

Is the current balance of power between individual users and social media companies in a stable state? The closure tenet of SCOT implies that as each problem concerning the proliferation of user data is gradually resolved, the need for improvement declines accordingly. Currently there appears to be conflicting goals in regards to data collection. Social media users generally desire withholding and protecting as much of it as possible, reflected in aforementioned surveys, while businesses require more of that same resource to grow. Breaches, hacks, and leaks occur on a "daily" basis. From 2004 to 2017, there have been at least 30,000 significant data crises in which billions on billions of accounts' details were dispersed without consent (Liu et al. 2018). The frequency and severity of these events reflect that there is still public unease regarding privacy, and thus there is still not a stable balance in the relationship between people and business.

Discussion

In accordance with SCOT, the invention and development of social media should not be blamed for the abuse of personal data as a commodity. Rather, the issue is simply a reflection of trends in consumer values. Closure can only occur once at least one side concedes or alters its objective. The simple path toward closure is for the users to relax their stance regarding privacy rights. If subsequent generations continue to express less and less concern about their private information being disclosed, pushes for increased protections would no longer occur. Social media companies would have the power to gather what they wish, and so long as they provide satisfactory services to their customers, the issue would be resolved. While possible, this path is concerning as it places businesses in a position of power with little checks against them. Users could be seen as lacking emphasis on principles such as autonomy and individuality, instead valuing entertainment and convenience above all.

Another path which is less straightforward is to improve data protection methods to a point which users can be assured their information is properly handled while companies still have access to a profitable resource. Design flexibility suggests that modifying current practices to better accommodate the side of users may bring the business model for social media nearer to closure. Data anonymization is one potential solution. Certain methodologies involve Hadoop Files Systems to quickly encrypt large volumes of data. Personally identifiable tokens are removed, but other valuable data are preserved for use in analysis and projections (Sedayao et al. 2014). While being less useful for advertisers to target customers, this option may be a satisfactory compromise that can please average users with minimal impact to ad effectiveness. There would have to be an additional social group with the authority to strictly enforce these rules and ensure that data is responsibly handled.

Conclusion

Issues regarding data privacy and the power of targeted advertising were not brought about by social media. Rather, the increasing popularity of these platforms had brought to light already-present trends in society that proliferate friction between personal rights and access to quality services. The internet and its related inventions are becoming increasingly advanced and accessible. In order to thrive in a market that prioritizes innovation and responsiveness, companies have deemed it necessary to utilize consumer information to make their products more relatable. However, public opinions of trust in proper information handling have relaxed over the years, and combined with a lack of increase in education, has created a prime environment for such a resource to be abused. In order for the interests of involved parties to be satisfied, changes to the current system are imperative.

References

Bartsch, M., & Dienlin, T. (2016). Control your facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147-154. doi:10.1016/j.chb.2015.11.022

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior, 110*, 106382. doi:10.1016/j.chb.2020.106382

Haida A. and Rahim H.L. (2015). Social Media Advertising Value: A Study on Consumer's Perception. International Academic Research Journal of Business and Technology 1(1): 1-8

J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," in *Computer*, vol. 51, no. 8, pp. 56-59, August 2018, doi: 10.1109/MC.2018.3191268.

J. Sedayao, R. Bhardwaj and N. Gorade, "Making Big Data, Privacy, and Anonymization Work Together in the Enterprise: Experiences and Issues," *2014 IEEE International Congress on Big Data*, Anchorage, AK, USA, 2014, pp. 601-607, doi: 10.1109/BigData.Congress.2014.92.

Liu, L., Han, M., Wang, Y., & Zhou, Y. (2018). Understanding data breach: A visualization aspect. *Wireless Algorithms, Systems, and Applications*, 883-892. doi:10.1007/978-3-319-94268-1_81

McFarlane, G. (2020, August 28). How Facebook, Twitter, social media make money from you. Retrieved March 13, 2021, from https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx

O'Loughlin, K., Neary, M., Adkins, E. C., & Schueller, S. M. (2019). Reviewing the data security and privacy policies of mobile apps for depression. *Internet Interventions, 15,* 110-115. doi:10.1016/j.invent.2018.12.001

Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation: The European Journal of Social Science Research, 26*(1-2), 81-99. doi:10.1080/13511610.2013.747650

Revealbot. (n.d.). *Facebook, Instagram & Google Ads optimization platform*. revealbot.com. https://revealbot.com/facebook-advertising-costs.

Ruckenstein, M., & Granroth, J. (2019). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy, 13*(1), 12-24. doi:10.1080/17530350.2019.1574866

Shu-Chuan Chu (2011) Viral Advertising in Social Media, Journal of Interactive Advertising, 12:1, 30-43, DOI: 10.1080/15252019.2011.10722189

Symantec. (2019, March 29). 72 percent of Americans are concerned about their Privacy, Symantec report says. Retrieved March 13, 2021, from https://www.securitymagazine.com/articles/90054-nearly-three-out-of-four-americans-are-concerned-about-their-privacy-symantec-report-says

Wan-Shiou Yang, Jia-Ben Dia, Hung-Chi Cheng and Hsing-Tzu Lin, "Mining Social Networks for Targeted Advertising," *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Kauai, HI, USA, 2006, pp. 137a-137a, doi: 10.1109/HICSS.2006.272.