Mitigating Teen Harm from Facebook Data and Advertisement Targeting

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

Emerson Berlik
Spring 2022

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

Advisor
Kent Wayland, Assistant Professor, Department of Engineering and Society

Introduction

Facebook and its many services have become household names over the past decade with 40% of Americans stating that they use Instagram, one of Facebook Inc's social media platforms, according to a study by the Pew Research Center in 2021. These social media and chat services have become a primary way for communication and content sharing. Instagram, Facebook's platform with the most teen engagement, gets approximately 22 million teens logging on each day in the US (Wells et al., 2021). In addition, Instagram was used by 72% of all teens in the U.S. as of 2018 according to the Pew Research Center. In the past three years, Facebook's studies have shown that Instagram is mentally harmful to a large percentage of their young user base, specifically teen girls. According to these studies, Instagram makes body image issues worse for one in three girls, which can be attributed to the news feed algorithm and filter bubble these teen girls are placed in. Much of this harm is also a result of Facebook's ad targeting, which preys on known vulnerabilities of teens.

Teenage use of Facebook has declined 13 percent since 2019, with a 45 percent projected drop in the next two years (Heath, 2021). While Instagram has not witnessed a decline like Facebook, Instagram's growth in 2021 has dropped from 0.8% compared to 2016's 22.9% and is predicted to be 0.2% by 2025 (Goetzen, 2021). With teens being a major contributor to Facebook's ad revenue, they are desperate to maintain their engagement with teen users. However, if they continue to use their current operation model, not only will teens continue being victimized but also public backlash against Facebook and lower teen engagement could cause major financial issues for the company. While Facebook has made claims for new products and changes to mitigate their harm towards teens, many of the same downsides can still be seen and are being

criticized by the public. My research question is: what changes in legislature and Facebook's policy and practices are best suited for mitigating teen harm and who should be responsible for these changes? My primary method for approaching this question will be a literature review of papers describing Facebook's current policies and practices, how to change Facebook's policies and practices, and what changes we should make to these policies and practices to mitigate teen harm. I will consider literature and policy with the Surveillance Capitalism framework, which I will discuss in a later section.

Context

Facebook collects thousands of data points on user interactions through interactions on not only Facebook and Instagram but also other sites which use Facebook's technology to collect data and relay it back to Facebook (Ho and Farthing, 2021). Facebook's algorithm uses these data points in order to manipulate and censor data so that users stay engaged with the app. Instagram's algorithm does not simply show users their followings' content, but is designed to display content optimized for the user (Usher-Layser, 2016). This results in a filter bubble, a term coined by Eli Pariser as a "personal, unique universe of information that you live in online" (Gould, 2019). The same data used to decide what shows up on a user's feed, generated through an interpretation of content a user likes, among other factors, is also collected for internal or external research. With teen users, this creates a positive feedback loop where these teen users are perpetually giving up their data through interactions with their constantly changing personalized feeds. Not only is this data used for content for user entertainment, but is also primarily used for deciding which advertisements a user sees. Surveillance advertising is the term used for this type of action, which is defined as using personal data to determine advertisements.

According to the Statista Research Department, 97.9% of all of Facebook's revenue, largely coming from Instagram, was from advertisements as of 2020. Much of this revenue can be attributed to Facebook's advanced targeting algorithm, which allows advertisers to specify their preferred audiences. Teens have certain habits, such as consumerism and impulsiveness, which make them more vulnerable and likely to be subjected to surveillance advertising than adult. This causes advertisers to target teens with certain traits that would cause them to be more likely to purchase their product. One example of how this can be directly harmful to a group is the instance of potentially harmful "flat tummy teas" or dangerous, unresearched exercises which are targeted at insecure teens with impulsive buying tendencies (Ho and Farthing, 2021). These ads can also further cause parent-child conflict among other implications, which lead to negative consequences for teen mental health.

Controversies and scandals associated with teen data privacy have caused the company public backlash and multiple lawsuits. In 2013, teens and their parents filed a class-action lawsuit, accusing Facebook of invading privacy through "Sponsored Stories." (Montgomery, 2015). These sponsored stories were a part of Facebook's early ploy of filter bubbles and targeting advertising. The lawsuit claimed that their practice violated a civil code, which stated that "'appropriating the names, photographs, likenesses and identities' of underage youth for commercial purposes without parental consent" was not allowed (Montgomery, 2015). Facebook had to pay out millions of dollars and claimed it would change its "Data Use Policy" and "Statement of Rights and Responsibilities". Instead of addressing privacy violation, Facebook changed its policy, so that users granted them rights to their personal data. By accepting the terms and conditions, users under the age of consent stated that their guardian also agreed to bypass the civil code. Similarly, in 2021, Facebook stated they would no longer provide most

user personal data to advertisers for users under the age of 18. However, it was found that Facebook was employing artificial intelligence to algorithmically personalize ads which many believe can cause more harm than the prior system (Ho and Farthing, 2021). Both examples emphasize Facebook's intentional ignorance to fixing the actual problem at hand for loopholes to maximize profits and show the need for an actual solution.

Methods/Framework

I will be primarily using literature review to address my research question. I will use different papers to address three sub-questions: What current policies and practices do Facebook and Instagram employ which violate teen and user privacy? Are individuals, policymakers, or Facebook most likely to make the change required to mitigate harm to teens? What changes in legal policy or Facebook's policy are best suited to prevent the continuation of harmful practices towards teens? By answering these questions individually through academic and research papers, I will synthesize of a solution of who should take action and what actions they should take in order to mitigate harm to teen users. In addition, I will analyze existing issues and potential solutions through the lens of the Surveillance Capitalism framework.

Surveillance Capitalism is a branch of the Panopticon theory, which is a surveillance framework that focuses on centralized systems physically or spatially watching over individuals (Galič et al., 2016). The Surveillance Capitalism framework claims that entities that take part in lucrative surveillance are disrupting capitalism by moving it away from supply and demand towards a more manipulative model. Surveillance Capitalism also extends the Information Capitalism theory, which views surveillance as both an economic and political force, by emphasizing the power of surveillance to "predict and modify human behavior as a means to

produce revenue and market control" (Galič et al., 2016, n.p.). Using this framework with a literature review will allow me to use sociotechnical concepts to reinforce the downfalls of Facebook's current model and the importance of a solution.

There are four principal components to this framework, which I will use in my analysis. The first component is perpetual data mining with formal indifference, meaning there is no freely given and informed consent, and functional independence, meaning algorithmic management of data and its usage. The second component is the new form of contracts which are autonomously generated and enforced. In other words, individuals both are giving a great deal of data and being manipulated through data which are regulated through autonomous technology. The third component considers personalized services which tell you "what you want or need to know before you know it yourself" (Galič et al., 2016, n.p.). The fourth and last component is the performance of experimentation on individuals' lives. Given both the continuous and recent nature of my research question and the status of Facebook as a major contributor to the world of big data, using the Surveillance Capitalism framework, and specifically the four components, will provide a beneficial method for assessing the current downsides of Facebook's business model and potential solutions.

Literature Review/Analysis

In order to attain a firmer grasp on the downfalls of the current Facebook business models and inspiration for potential changes which could mitigate teen harm, I am analyzing literature which pertains to Facebook's social and technological interactions with their teen users. The first piece of literature I am considering is a past article by Ralf de Wolf and Stijin Joye, written in 2019, which analyzes Facebook's data privacy using a social constructivist perspective called 'privacy

as control.' Privacy as control refers to safeguards used by an entity to prevent mishandling of private and personal information. Similar to the surveillance capitalism framework, privacy as control focuses on the right to privacy and the potential threat to democracy inflicted by over surveillance.

The authors analyzed the Zuckerberg files, which are a collection of public statements by Facebook's CEO, Mark Zuckerberg. They explain how Zuckerberg provides users a sense of control while placing users, advertisers and Facebook on equal grounds when it comes to privacy. This ultimately takes away from individuals' privacy as control through their empowering of advertisers. When discussing teen privacy, they explain how privacy is strongly associated with control and power because of being able to study individuals through social interactions and their exchanging of information. Ideas of media literacy and online privacy literacy are also introduced. Media literacy and online privacy literacy refer to knowledge of social media usage and application of privacy in social media, respectively. The authors also found that both these literacies have been increasing in the past decade and that individuals with higher media and online privacy literacy "show more privacy regulation behaviors and feel safer using SNS (social networking service)" (de Wolf and Joye, 2019, p. 5506). The surveillance capitalism framework emphasizes how unconsented and uninformed giving of data by a user is a downfall of surveillance. An example of this is the priorly mentioned example of Facebook changing their terms and conditions because of a lawsuit so that teens unknowingly give parental consent to their data by accepting the conditions. It seems evident that increasing online media and privacy literacy, the issue posed by surveillance capitalism can be mitigated. By improving an individual's awareness of a company's privacy and data usage, uninformed and unconsented data collection is less likely. However, while these literacies are gradually increasing, it would be

very difficult to increase these national literacies with legislature in a short period. Posing changes in Facebook's policy or legislature would cause a much more immediate change.

In order to further understand potential legal and policy implications and solutions to my research question, I considered Waldman's article, titled Privacy, Sharing, and Trust: The Facebook Study. This article explains how Facebook's design is ultimately responsible for encouraging users to share personal information by manipulating trust because of a strong relationship that exists between trust and sharing. Facebook is aware of this relationship shown by a committee of Trust Engineers with the specific role of playing with wording and design amongst many other factors, with the goal of getting users to honestly interact with posts. A primary example of how Facebook and Instagram manipulate this trust is by masking native advertisements as user posts with information, such as which friends have interacted with the post or advertisement. This confusion in differentiating advertisements and user posts is by design, with financial gain as an incentive. In the priorly mentioned example of teens being targets of "flat tummy tea" advertisements, by seeing that their friends and network have interacted with this advertisement, they consequently are more trustful in the potentially harmful product.

Viewing Facebook's manipulation of trust through the lens of surveillance capitalism reveals that their profit optimizing practices are examples of active performance of experimentation on human lives. Trust Engineers intentionally use design practices to create user interfaces, which subconsciously trick users into giving up personal data. Most users are not aware of these practices and thus the trust that is created is artificial and harmful.

Waldman poses two potential solutions to mitigate this manipulation of trust, the first being a concept called Privacy by design. Privacy by design is the "notion that we should engineer our online platforms from the ground up with privacy in mind" (Waldman, 2016, p.226). One example of how Facebook could start by employing privacy by design is increasing the transparency of advertisements on their news feeds page. Through implementing privacy by design in this example, the experimentation aspect of the news feed lessens, addressing this aspect of the surveillance capitalism framework. However, because of a need for radical change in culture at Facebook for privacy by design to occur, it is very unlikely that it will occur. We must turn to policy regulators for a more viable and immediate solution. This leads to Waldman's second solution: law enforcement.

The Federal Trade Commission (FTC) was created in 1914 for the purpose of antitrust, however, has now expanded to also stop deceptive practices by industries which threaten privacy rights of consumers (Watson, 2021). There are also multiple cases which give precedent to the FTC being able to regulate manipulative and harmful designs by companies. One example which Waldman mentions is that of Sony BMG Music Entertainment. Sony designed their CDs to discretely install software onto user's computers and intentionally made it hard to remove. In addition, they designed their media players to send user information to their servers for the purpose of using it in targeted advertisements. The FTC decided that Sony had used tactics which "constituted unfair design practices that misled, deceived, and constrained users" (Waldman, 2016, p. 229). The parallels between the Facebook and Sony cases are that both used design techniques to hide potentially harmful and unwanted, but also profitable practices, thus it seems evident that the FTC is responsible of taking action against Facebook's practices.

Similarly, state attorneys general also can be valuable assets in the fight for user and teen privacy, and have the potential to have more of an impact than the FTC (Waldman, 2016). State attorneys general are key figures in creating state privacy legislation and thus have the power to both apply existing laws or newly created laws for social media companies such as Facebook. An example is that of Illinois's state attorneys general. The state attorneys general enforced a right of publicity statute on Groupon, which also used manipulation of trust practices by displaying personal images in advertisements, which "prohibits the use of a person's name or photograph for the sale or advertisement of goods or services without consent." It is clear from the Groupon example state attorneys general have the ability and power to prevent Facebook's manipulative practices. Another example of how state attorneys general have power in company practices was exemplified by California's former attorneys general, Kamala Harris. Harris has created informal agreements with Facebook, amongst other large tech companies, as well as has issued practice guides for state statutory requirements. Companies comply with these agreements since they prevent lawsuits which could damage the company's relationship with the attorneys general and other policymakers in addition to the public.

While none of the components of surveillance capitalism are objectively harmful by nature, their execution and practice often come with harmful consequences as seen in Facebook's news feed, which manipulates trust. Both the Sony and Groupon cases also are examples of this. For the Sony case, the first component, which revolves around consent and freely given information, was violated because of practices of deception by secretly uploading software and sending user information to their servers. The users neither gave consent for this software to be uploaded or their information to be sent. With Groupon, users did not give their consent for their images to be used in personalized advertisements. In both cases, legal enforcement by the FTC and state

attorneys general, respectively, was needed to protect consumer privacy and was also ultimately the solution to the problem at hand. This shows the role and power of both legal bodies in ensuring that none of the components of surveillance capitalism are violated by companies.

Walden's paper gave insight into the importance of the FTC and lawmakers as key players in addressing my research question. Action by these two entities is essential in mitigating harm to teens through Facebook and Instagram's data practices. The question that remains is still what policy changes are needed exactly to prevent Facebook from continuing their harmful practices. To help answer this question, I analyzed an article titled Protecting Children in the Frontier of Surveillance Capitalism which aims to pose a legislative change in the Children's Online Privacy Protection Act (COPPA).

In his article, Watson discusses how data from children is often commoditized for the previously mentioned tendencies of consumerism and impulsiveness. He then discusses the fourth component of Surveillance Capitalism, which involves experimentation on individuals, in the context of society not realizing the effects of essentially experimenting on children through their targeted content until it is too late and the consequences are detrimental (Watson, 2021). Because of children and teens being the most impressionable, it is paramount that protection of these young users is ensured. Watson then discusses the related legal context relating to Surveillance Capitalism behind children. In 1998, the FTC issued the Children's Online Privacy Protection Act (COPPA) with the purpose of protecting children under the age of thirteen's privacy in the new digital era at the time and to allow for parental control over online information collected from their children.

Watson explains a phenomenon that psychologists call “emerging adulthood” which is the social act of differentiating oneself from their peers (Watson, 2021, p. 22). Psychologists have found that while this age of emerging adulthood used to start earliest at the age of eighteen, it is now moving more and more towards adolescent years. This can be attributed to social pressures of comparison amongst others, which lead to this same social act which requires individuals to differentiate themselves. Younger children active online and going through emerging adulthood can also be attributed to the lack of enforcement and the age of COPPA being only 13. The requirement to be thirteen is seen as a simply a guideline due to having no type of enforcement other than sites requiring a checkbox. Children lie about their age online and a study in 2014 found that a fourth of children in the US between 8 and 12 used Facebook (Watson, 2021).

The largest issues that arise from this new era of emerging adulthood deal with two aspects of the surveillance capitalism framework. The first issue stems from the uninformed collection of data from these children and teens, who have practically no knowledge of online safety regarding data. This leads to the second major issue of these companies using this data to maintain engagement with children and teens through personalized feeds, which grants them even more user data through the teen’s interaction with the newly generated posts. This is what is ultimately causing insecurities, which is, in turn, lowering the age of emerging adulthood. In order to address both of these issues, there should be higher enforcement on the minimum age of social media usage, in addition to more restrictions on what this data can be used for. Changing the enforcement around COPPA in addition to COPPA itself can do just that, which Watson dives into.

Watson proposes two potential solutions to address the limitations of COPPA. The first solution is increasing the monetary penalty for violating COPPA. Facebook, along with many other companies, disregards the monetary punishment as a cost of business since their profits using user data greatly exceed it. Consequently, the FTC must redesign COPPA to properly penalize companies for violations in order to dissuade them from continuing the same harmful actions. The second potential solution Watson provides is increasing the age limit set by COPPA. Because of the lack of enforcement and arbitrary nature of the age, increasing the minimum age to use social media to eighteen would cause parents to reconsider what an acceptable age is to allow their children to use social media. In addition, the older a child becomes, the more they can understand consequences and thus is less likely to be victimized by data manipulation practices (Watson, 2021). Both solutions would mitigate the downfalls of surveillance capitalism through decreasing uninformed and unconsented collection of data, as older teens are more aware of the risks, and decreasing experimentation on teen users through personalized feeds, as the punishment would outweigh the benefits.

Conclusion

In analyzing my research question of how to mitigate teen harm by Facebook, three solutions were apparent. The first solution was to increase public media and online privacy literacy. While this solution would address the problems of surveillance capitalism, it is much too difficult and long of a process to increase national literacy of these topics for potentially minimal results. The second solution was to resort to the FTC and state attorneys general to regulate Facebook policy and practices. This solution is very viable given that both have histories of protecting individuals online and data privacy. This third solution provided direction to the second solution and

involved changes to the monetary penalty and age limit of COPPA. It seems clear from the second and third solutions that the best course of action in protecting teens from the harmful practices of Facebook is by turning to the FTC and state attorneys general for help in creating and enforcing policy, in the form of changes to COPPA or new legislature, that creates a penalty great enough to dissuade Facebook from continuing their profitable practices which harm teens. In addition, a change to COPPA should include an increase in the age limit requirement of social media in order to dissuade young and uninformed individuals from using Instagram and other social media platforms which have untransparent data collection and usage. Implementing these changes in legislature would protect teens from not only Facebook and Instagram but also many other platforms and companies that maliciously use data for profitability. For future research, the social and economic implications of changing COPPA should be further analyzed so that the potential repercussions can be properly understood.

References

Anderson, M., & Jiang, J. (2021, May 27). *Teens, Social Media & Technology 2018*. Pew Research Center: Internet, Science & Tech. Retrieved March 21, 2022, from https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/

Bond, S. (2021, July 27). *Instagram debuts new safety settings for teenagers*. NPR. Retrieved March 21, 2022, from https://www.npr.org/2021/07/27/1020753541/instagram-debuts-new-safety-settings-for-teenagers

de Wolf, R., & Joye, S. (2019). Control Responsibility: The Discursive Construction of Privacy, Teens, and Facebook in Flemish Newspapers. *International Journal of Communication*, *13*.

Galič, M., Timan, T., & Koops, B.-J. (2016). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology*, *30*(1), 9–37. https://doi.org/10.1007/s13347-016-0219-1

Goetzen, N. (2021, December 8). *Instagram needs younger users, but new teen safety controls won't help*. Insider Intelligence. Retrieved April 7, 2022, from https://www.emarketer.com/content/instagram-needs-younger-users-new-teen-safety-controls-won-t-help

Heath, A. (2021, October 25). *Facebook's Lost Generation*. The Verge. Retrieved March 2, 2022, from https://www.theverge.com/22743744/facebook-teen-usage-decline-frances-haugen-leaks

Hitlin, P., Rainie, L., & Olmstead, K. (2022, March 8). *Facebook algorithms and Personal Data*. Pew Research Center: Internet, Science & Tech. Retrieved March 21, 2022, from

https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/

Ho, E. Y.-C., & Farthing, R. (n.d.). *How facebook still targets surveillance ads to teens*. Fairplay For Kids. Retrieved March 22, 2022, from https://fairplayforkids.org/wp-content/uploads/2021/11/fbsurveillancereport.pdf

Jargon, J. (2019, June 18). *How 13 became the internet's age of adulthood*. The Wall Street Journal. Retrieved February 24, 2022, from https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201

Lima, C. (2021, October 1). *Lawmakers hammer facebook for hiding how its products may hurt kids*. The Washington Post. Retrieved March 2, 2022, from https://www.washingtonpost.com/technology/2021/09/30/facebook-instagram-congress-hearing-antigone-davis/

Lomas, N. (2021, November 16). *Facebook continuing to Surveil Teens for ads, says report*. TechCrunch. Retrieved March 2, 2022, from https://techcrunch.com/2021/11/16/facebook-accused-of-still-targeting-teens-with-ads/

Olguín, E. (2021, September 23). *To reduce Facebook's harms to teens, target its data-hungry business model*. Privacy International. Retrieved February 27, 2022, from https://privacyinternational.org/news-analysis/4622/reduce-facebooks-harms-teens-target-its-data-hungry-business-model

Protecting kids online: Facebook, Instagram, and Mental Health Harms. U.S. Senate Committee on Commerce, Science, & Transportation. (2021, September 24). Retrieved March 2, 2022, from https://www.commerce.senate.gov/2021/9/protecting-kids-online-facebook-instagram-and-mental-health-harms

Schaeffer, K. (2021, October 7). *7 facts about Americans and Instagram*. Pew Research Center. Retrieved March 21, 2022, from https://www.pewresearch.org/fact-tank/2021/10/07/7-facts-about-americans-and-instagram/

Senators Markey and Cassidy propose bipartisan bill to update children's online privacy rules: U.S. senator Ed Markey of Massachusetts. Home. (2021, June 24). Retrieved February 24, 2022, from https://www.markey.senate.gov/news/press-releases/senators-markey-and-cassidy-propose-bipartisan-bill-to-update-childrens-online-privacy-rules

Senators Markey and Cassidy propose bipartisan bill to update children's online privacy rules: U.S. senator Ed Markey of Massachusetts. Home. (2021, June 24). Retrieved March 21, 2022, from https://www.markey.senate.gov/news/press-releases/senators-markey-and-cassidy-propose-bipartisan-bill-to-update-childrens-online-privacy-rules

Waldman, A. E. (2016). Privacy, Sharing, and Trust: The Facebook Study . *Case Western Reserve Law Review*, *67*(1).

Watson, C. F. (2021). PROTECTING CHILDREN IN THE FRONTIER OF SURVEILLANCE CAPITALISM. *Richmond Journal of Law & Technology*, *27*(2).