Introduction

In March 2018, a story was published and it was revealed that a firm that had helped the campaigns of Ted Cruz and Donald Trump for president in 2016 had harvested the data of 50 million Facebook profiles. This data was used by the firm based out of the UK to create psychological profiles of Americans so Americans could be better targeted with political propaganda. This caused a large public backlash and caused a great stir about digital privacy in the public discourse (Meredith, 2018). Obviously using services like Facebook and Google come at a cost, the data collected from people using these companies' services is used to better target these people with advertisements. And in the case of Cambridge Analytica, it wasn't just used to better serve ads, but was used to target people shown to be susceptible using psychological profiles. Events like these have caused people to have large amounts of doubt and anxiety about the usage of this data as a Pew Research Center survey showed (Auxier, 2019). 62% of the people surveyed believed it is not possible to get through a day without some company harvesting data from them. 79% of those polled said were concerned about the usage of data collected by companies. These results show that people are becoming increasingly aware of data being collected on them (Auxier, 2019).

Still, these online platforms want to continue to monetize user data so they can target these users with ads and/or sell it to third parties as well. It has become increasingly obvious that there is a tradeoff, people can use these digital services where data collected about them or suffer the consequences of not being able to use them but have a greater sense of privacy. But for some of these companies, data has to be collected because selling this data or using it to target users more

accurately with ads is central to their business models.

There are two groups of people when it comes to data privacy, a person either cares or doesn't care. People may not care because they don't know enough about it to be concerned or they simply don't care if their data is being collected by companies as they use the Internet. An IBM survey done in August 2019 reveals that 89% of the 1000 people surveyed believed tech companies need to be more transparent and 75% say they have become less likely to trust tech companies to handle their data in the last year (Hart, 2019). However, this contrasted by the by that fact that 45% of those surveyed said they have had not updated their privacy settings, and only 16% stopped doing business with a company because of purported misuse of data(Hart, 2019). These results shows a large portion of the public is not willing to put in the work to understand how companies they interact with daily are using the data they are gathering. This paper examines the evolution of the internet as a system encouraging a large percentage of users to be ignorant of, or uncaring about, how their lives are tracked online. A second component of the paper considers an emerging movement to bring awareness and agency over data sharing back to users of digital technologies. It is a story about scripting and counter-scripting the relationship of people and their data.

Literature Review

Many of the free online services we use today are free because the service can be used to advertise and also be used to collect data on the users. Google has an very dominant market share in the realm of search engines, over 92% of all searches done are done using Google. This large gap seems to not be shrinking much over time(Oberlo, 2019). Considering this ability to reach so many people, it is not a surprise that in 2018 over 70% of Google revenue, which amounts to a

staggering $117 billion(Clement, 2020). So obviously serving ads is a huge industry, but in order to better serve these ads, Google uses their multiple different services they provide free of charge, like YouTube and Google Search.

So the collection of data is a major part of many of the companies like Google and Facebook, which both acts as major backbones for the internet. Their services are popular because they are easy to use and require no explicit payment to use. Most people that use these services never read any of the privacy policy that defines how their data linked to their account can be used, as shown in a Harris Interactive survey done in 2013 of 2000 people in the US, where over 51% said they had not looked at the most recent privacy policy of any of their social media accounts (Cobb, 2013). But a poll conducted by Pew Research in 2015 showed that 74% of those surveyed thought it was really important who can access their personal data (Madden & Rainie, 2015). It's very odd what this data shows, because it seems like most of the public really cares about their privacy, but they don't take any actual actions. This is commonly known in the digital privacy research field as the privacy paradox (Barth & De Jong, 2017). A paper published in the International Journal of Communication titled "'What Can I Really Do?'" analyzed how the privacy paradox works and showed that young people tend to care about privacy, but think that once their information is shared onto a social media platform, they no longer have control over it (Hargittai & Marwick, 2016). So even younger people, who could be seen as more able to understand data privacy do not feel like they have any real control over who has access to their data and how it is used.

In order to better understand the entities at play and to analyze how we got to the current system we are in, and what can be done going into the future, I will be using social construction of technology (Bijker, 2008). This pairs groups of people affected by a given technological problem, in this instance digital privacy, with solutions to the problems they face. The stakeholders when it comes to this debate are the consumers that use digital platforms like Facebook or Google in their everyday lives. Another set of stakeholders are the companies themselves that want to be able to harvest the data from the users of their products in order to sell or better target people with ads. And the final set of stakeholders is the government. The internet evolved over the past two decades like any other technology that is brand new and used my broad swathes of society. Services like Google and Facebook are popular because they both fulfill a need people are looking for. Google allows people to browse the web quickly and accurately, it acts as a giant pipeline of information for anyone that has access to it. And Facebook acts as a way people can substantially connect with each other instantly over any distance. And since the their beginnings, both of these companies have prioritized not making people pay, and leveraging people's data collected through using their to attain monetary gain.

Data Privacy: A Brief History

Data privacy has been a growing issue since the beginning of the internet. Companies have wanted increasing access to data that allows them to better target consumers browsing the web with ads. Early pioneering companies in the late 1990s like AOL and Yahoo were able to garner advertising fees from people using their online portals. Advertising profit led a lot of companies to try and serve many ads so that they could turn a profit, which led to the speculative bubble that burst in 2001 (Encyclopedia Britannica, 2020). But starting in the 2000s,

companies were able to start using browsing habits and other pertinent data to better serve these ads, so that ads could be served to a relevant audience regardless of what website they are visiting. Consumers have noticed more obvious results of data being collected on them as shown by a Pew Research poll conducted in 2012, 68% surveyed said they were not okay with targeted advertising since it involved being tracked (Purcell, Brenner, & Rainie, 2012). And this has become more than just serving ads, in the case of the aforementioned Cambridge Analytica scandal, Facebook gave access to millions of people's very personal data to a third party, where, according to Facebook COO Sheryl Sandberg, they " 'still don't know what data Cambridge Analytica have'". They didn't know what the firm was doing with the data and even when they suspected something chose not to audit the company and to trust that they deleted all the data they harvested with out actually checking themselves(Edwards, 2018). So companies, especially Facebook, have shown a disregard for their users' data privacy. It only makes sense with a increasingly anxious public sentiment on the topic that people are more and more wary of what is being done with their data. Another notable company that has rose in prominence is Google, though it is not viewed as negatively as Facebook. The only reason providing a very robust search engine for free is profitable is because they serve ads to people. And Google knows much more about people the more services they use. By using their services like Youtube, Gmail, and Google Maps, they can know your name, gender, birthdate, where you lived, and what interests you have. According to Google, it uses this data to improve its services (Haselton, 2017). These companies have found that the best way to subtly monetize their products. Facebook has filled a want to connect with other and Google with their massive search engine, has satiated a need for more information and quicker access to said information. They, along with many companies, have decided to use ads and selling their user's data as ways to actually make money of their services. It is a popular

business model because it works. But why do people not really seem to care much about all of this data about them floating out there in the ether, currently it is hard for an individual to tell who can look at their personal data collected by entities and how it is being used by said entities. This system has grown to value having free access to the resources of the internet over having more control over one's personal data. This is the current system society has embraced, but as evidence from studies cited below shows, there are many people who don't like how this system values their data privacy.

People Controlling Access To Their Personal Data

As stated before, a poll conducted by Pew Research in 2015 showed that 74% of those surveyed thought it was really important who can access their personal data (Madden & Rainie, 2015). Obviously just like real life privacy, people tend to also care about the privacy of their online presences. But it also seems like a lot of people don't do anything to better their privacy when they browse the web. As stated before, this is known as the privacy paradox. Multiple studies have shown that this phenomenon is real, such as a study conducted in 2012 where a field experiment was conducted. In this experiment, participants were given the opportunity to buy CDs from two different stores. One store asked for their personal info, their income and their date of birth, and this store in one phase had lower prices. More people went to the store with cheaper prices. And interestingly enough people still went to both stores equally even when they had the same prices (Beresford, Kübler, & Preibusch, 2012). These results show that people really don't seem to care much about privacy at all, even when there is no financial incentive not to. It seems that is harder for people to understand how much they value their personal data. This makes sense since personal information isn't really a tangible thing. It's hard to imagine the possible

repercussions of a bunch of personal info floating out there in society.

Data Privacy Defeatism

A study published by the International Journal of Communication used focus groups of university students in order to better understand the privacy paradox. One participant, a 22 year old, was quoted as saying "'On Facebook I think it's been drilled into me that you just have to assume anything you post is public. You can set your privacy settings at the strictest you want, but you just have to assume that anything you put out there can be made public to the world.'" Many other participants in this study shared this similar view. The authors concluded that comments showed that some people had a sense of apathy or a sense of cynicism. And also a very interesting line from the study is when the authors state that "Privacy is not an individual process, but rather a collective effort that requires cooperation of those with whom we connect with on social media, as well as the technological affordances of the social media sites themselves" (Hargittai & Marwick, 2016). While there are a number of people who genuinely don't care about their privacy and/or are ignorant about how much their data is floating about, it seems like even if they did care, they would feel similar to those who feel like they lack any control over their data.

Can People Have Ownership Over Their Data?

` So people want to have control over their data, but it seems like the innovations that could better enable the public to do so need to be much more built up. One way this system that

unequally favors the companies that collect data has been restructured was done by the California Consumer Privacy which was signed into law in October, 2019 and became effective on Januray 1, 2020 (Wikipedia Contributors, 2020). This laws enable residents of California to be able to: have knowledge of what personal data is being collected about them, know if their data is being sold or given to entities(and which entities those are), allow citizens to disallow their data from being sold, deny access to their data, ask a company to erase any personal data of theirs they have, and finally they can't be discriminated by the company for using their lawful rights (Wikipedia Contributors, 2020). This modifies how consumers interact with companies they take advantage of while using the internet, consumers are now much more empowered and can now go to these companies like Facebook and Google and tell them what they can do with their data. Very tangible examples of this broad reaching law is that a company's home page must have a link to portal where they can opt out of the company selling their data, and companies covered under the law must also update their privacy policy in order to reflect the rights to privacy Californians have (Wikipedia Contributors, 2020). This law being enacted in California does seem to speak to a larger political will to protect the people who are ignorant about data privacy or those who feel like keeping their data private is a hopeless endeavor, which seems to be a large majority of Americans. People no longer have to have VPNs and use a TOR browser to have more control over their data.

Education

One other crucial factor that needs to be considered when talking about data privacy is the need to better educate the public. People have to be taught how data is collected on them and what they can do to better protect their data and also know how they can opt out of services. This needs to be done from elementary school and on. It should be as ubiquitous as teaching Microsoft Word and Excel is in grade school computer labs. With respect to these concerns, a very interesting product has been developed called Fakesbook, which is a social networking platform dedicated to teaching kids about privacy and security when using social media and the wider internet. This fake social media platform was tested over many years with hundreds of students and found that 86% that used it said it helped them better understand online security and privacy. The most interesting thing about the platform is that it showed a graph that gave them a visualization of how their profile data spread across the site, which was dependent on who their friends were and what their privacy setting were (Zinkus, Curry, & Others, 2019). Innovations like this are needed to better connect with students and really hammer home how to deal with privacy as an active thing people must do, not something you are barely aware or that is in your periphery.

Conclusion

So it seems like there are two solid ways of dealing with the massive systemic problems with data privacy. Members of the public and the government who believe in strengthening data privacy rights for everyone need to enact legislation that allows consumers to more easily manage what data a company collects and sells about them. It can’t be one way street, consumers need to have rights, just like rights in any other arena of society. And then comes education, which is ultimately very important because these business that benefit from how the system currently works

will fight or try to subvert the law, so people need to be on the offensive when it comes to understanding how companies might try and violate their privacy.

Sources

Oberlo, Search Engine Market Share in 2019. (n.d.). Retrieved from https://www.oberlo.com/statistics/search-engine-market-share

DuckDuckGo Privacy. (n.d.). Retrieved from https://duckduckgo.com/privacy

Clement, J. (2020, February 5). Google revenue breakdown by source 2018. Retrieved February 14, 2020, from https://www.statista.com/statistics/266471/distribution-of-googles-revenues-by-source/

Shankland, S. (2019, July 26). Brave's browser can pay you to see ads. Now you can convert those payments into cash. Retrieved February 14, 2020, from https://www.cnet.com/news/brave-now-lets-you-cash-out-ad-revenue-browser-pays-you/

Meredith, S. (2018, April 10). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. Retrieved from https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Edwards, J. (2018, April 6). Sheryl Sandberg: Facebook knew about Cambridge Analytica 2 1/2 years ago but didn't follow up. Retrieved from https://www.businessinsider.com/sheryl-sandberg-facebook-knew-about-cambridge-analytica-2018-4

Holmes, A. (2020, January 2). A new law gives you the power to tell websites not to sell your personal data. Here's how to exercise your rights. Retrieved from https://www.businessinsider.com/new-law-ccpa-privacy-tell-websites-not-sell-personal-data-2020-1#the-law-also-requires-that-businesses-tell-users-what-information-is-being-collected-about-them-ranging-from-their-name-and-contact-information-to-their-browsing-history-3

Athey, S., Catalini, C., & Tucker, C. (2017, June). The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. Retrieved from https://www.nber.org/papers/w23488.pdf

How Stuff Works, How do advertisers show me custom ads? (2012, September 25). Retrieved from https://computer.howstuffworks.com/advertiser-custom-ads.htm

Consumer Champion Organization. (2020, February 22). Would You Sell Your Online Data For Profit? (Survey Results). Retrieved from https://consumer-champion.org/resources/would-you-sell-your-online-data-for-profit/

Auxier, B., Raine, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, December 31). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Hart, K. (2019, February 25). Consumers kinda, sorta care about their data. Retrieved April 17, 2020, from https://www.axios.com/consumers-kinda-sorta-care-about-their-data-3292eae9-2176-4a12-b8b5-8f2de4311907.html

Barth, S., & De Jong, M. (2017, November). *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*. ScienceDirect.com | Science, health and medical journals, full text articles and books. https://www.sciencedirect.com/science/article/pii/S0736585317302022

Beresford, A., Kübler, D., & Preibusch, S. (2012, April 30). *Unwillingness to pay for privacy: A field experiment*. ScienceDirect.com | Science, health and medical journals, full text articles and books. https://www.sciencedirect.com/science/article/abs/pii/S0165176512002182

Bijker, W. E. (2008, June 5). *Technology, social construction of*. Wiley Online Library. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781405186407.wbiect025

Cobb, S. (2013, November 13). *Do consumers pass the buck on online safety? New survey reveals mixed messages*. WeLiveSecurity. https://www.welivesecurity.com/2013/11/13/do-consumers-pass-the-buck-on-online-safety-new-survey-reveals-mixed-messages/

Encyclopedia Britannica. (2020, February 26). *Foundation of the internet*. https://www.britannica.com/technology/Internet/Foundation-of-the-Internet

Hargittai, E., & Marwick, A. (2016, January 24). *"What can I really do?" explaining the privacy paradox with online apathy*. International Journal of Communication. https://ijoc.org/index.php/ijoc/article/view/4655/1738

Haselton, T. (2017, December 6). *How to find out what Google knows about you and limit the data it collects*. CNBC. https://www.cnbc.com./2017/11/20/what-does-google-know-about-me.html

Madden, M., & Rainie, L. (2015, May 20). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Purcell, K., Brenner, J., & Rainie, L. (2012, March 9). *Search engine use 2012*. Pew Research Center. https://www.pewresearch.org/internet/2012/03/09/search-engine-use-2012/

Wikipedia Contributors. (2020, April 15). *California Consumer Privacy Act*. Wikipedia, the free encyclopedia. Retrieved April 18, 2020, from https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

Zinkus, M., Curry, O., Wood, Z., Moore, M., & Peterson, Z. (2019, February 22). *Fakesbook | Proceedings of the 50th ACM technical symposium on computer science education*. ACM Digital Library. https://dl.acm.org/doi/abs/10.1145/3287324.3287486