The Internet is no longer an equal playground. During its inception, everyone that was able to log on was equivalent to one another, sharing media and information amongst themselves. However, as time went on, corporations realized the power that the world wide web had over people, and the value of the data that could be collected from its users. Big data collection quickly became the gold rush of the 21st century. Patterns of when people were online, where they were located, which age-range of groups were more likely to be looking for specific information, and plenty more were all beginning to be mined through various platforms. Smart devices began invading people's lives; Google Home, Alexa, Siri, and plenty more Internet connected devices collect data on their users. Internet explorers are put down due to oppressive algorithms, and hateful individuals using the tools at their disposal to cause harm. The Internet continues to create opportunities for conglomerates to profit, and a lower quality of life online for its users.

The Internet was first conceived for the primary purpose of sharing research throughout the military. By the 90's, it was setup in such a way to be operated by "the non-expert", allowing for less tech-savvy individuals to get online, and control of the web's infrastructure was handed over to the private sector (Simpson, 2004). In the following decades, that infrastructure massively expanded, and began hosting new commercial development space. The major companies that allow us to connect with friends, email colleagues, and share media all may seem to give us these products for free, but that in turn changes the corporate formula: the users are now the products. Platform models shifted from paying for access to email, searches, and instant messaging to a free-to-use archetype, where users' data was being collected and sold off. Facebook became a huge target for ethical issues with data sharing. The site was reported to share demographic data, names of users and their friends, and even private messages between users with other conglomerates. It was estimated that American companies spent nearly $20 billion in data collection in 2018 (CBS News, 2018). Concerns over data collection have been rising as the corporatization of the Internet goes on. With the data being offered up by consumers freely in exchange for these conveniences being shared and sold, there is a very real threat of the data being leaked and stolen. In 2017, nearly 2 billion consumer records were exposed, which includes personal data on almost half the population of the United States (Kennerly, 2018). These breaches can end up with people having their identity stolen, credit cards opened in their name, accounts being used fraudulently, and in some cases, blackmail, and similar strategic personal attacks. Corporations including Yahoo, Uber, eBay, and Equifax have all had user data lost in various ways, despite having multibillion dollar infrastructures. This brings the question of how much in resources are they devoting to the safety of their users. How long until hackers infiltrate Google or Apple servers to expose private information being shared in homes? Has it already happened without notification to the public? These companies collect data on physical movements, personal and family interests and activities, private messages, and general social communications (Andrew & Baker, 2019). Putting all this information together, an accurate picture can be created of an individual. There is doubt to be had about how much security is in place to protect the information we have shared online, and the information we have not given as willingly.

As the Internet becomes accessible to a greater population, we have seen an increase in devices connected to the Internet, or Internet of Things devices (IoT). Google Nests, Amazon Ring doorbells, Apple Watches, and millions of other devices are constantly transmitting user data back to their respective servers. Sensors in these devices collect data, often without the user thinking about it, which is then sold off to advertisers. Snapchat appears to be a fun form of entertainment using a device's

camera to take filtered photos and add effects to videos, but many do not realize that data is being collected on users' facial features, with a very real revenue opportunity for the company (Hild, 2017). This model of trading data for services has become forced on manufacturers because users have become so accustomed to getting these services for free and allowing these devices their smart capabilities to be connected to "the cloud" (Allan, 2018). Plenty of this information appears innocuous enough to share in exchange for services, but as businesses continue to push what information they collect - such as who users are spending the night with and blueprints of their homes - consumers are becoming more wary. In 2016 a survey was conducted on Americans' confidence with various groups' collection of data. It revealed there was plenty of skepticism with social media sites, and mixed concern with companies and retailers (Kennerly, 2018). IoT systems face numerous threats outside of their corporations failing us: "communications can be intercepted or data compromised by unauthorized parties to collect [personally identifiable information], authentication can be brute-forced, credentials can be extracted from device firmware, credentials can be extracted from mobile apps, credentials can be intercepted at login, and new firmware can be uploaded with malware" (Bastos, Shackleton, & El-Moussa, 2018). Users are not all going to be aware of the potential security threats when using IoT devices, and it is imperative that the corporations step up security measures to ensure data is not falling into the wrong hands.

There is no doubt about the value of user data to both advertising and hacker groups, but user data is also targeted by individuals looking to cause harm to other, specifically targeted individuals. Doxing has come about as a tangent to hacking in internet communities where personal information is exposed without a person's consent, including their address, telephone numbers, employment information, and more about their private lives on and offline. A small portion of those who have been doxed reported being physically attacked in person, with some even turning into fatalities. Users have stopped using various internet platforms entirely in some cases due to fear of continued harassment. "I don't have any social media accounts using my legal name. I don't connect with people that I know in real life. I don't really use social media except for the promotion of my work now" (Eckert & Metzger-Riftki, 2020). Greater attention was brought to the public about the harms of doxing in the past decade, specifically during "The Fappening", when numerous nude images of celebrities were released against their will, and #Gamergate, when female gaming journalists had their information leaked online. Both caused major concerns and produced an unfortunate amount of harassment towards these women both online and offline. This is not just a few isolated occurrences either; in 2016, over 3,000 Americans were surveyed, and 30% were found to have experienced an invasion of their privacy online (Eckert & Metzger-Riftki, 2020). Whether these individuals were attacked due to their stance on abortion, their gender identification, or their views on a new videogame, it is obvious that there has been a failure by corporations to ensure their users' online data stays safe and secure.

Conglomerates in charge of so much of our online wastelands obviously are lacking in either control or care for their users' safety regarding their data, and many have also been growing with a lack of empathy for minorities. Users that do not fit into the same demographic of those in charge of website and app algorithms are not necessarily able to use these platforms as easily as users who are more related to those designers. Safiya Noble writes about the oppressive algorithms that apps and websites are built upon. Algorithmically driven data failures, specifically to women and people of color, show how racism and sexism are structured into huge websites. In the past, searching for "black girls" on Google would yield pornographic results at the top of the page, despite being an innocent phrase. During

Obama's presidency, Googling "Michelle Obama" would turn up a related search term of "ape" (Noble, 2018). While these have now been updated, the issue still remains that systemic racism and sexism are built into our everyday search algorithms and affect what content users are given. This cannot be tolerated with how synonymous Google is with the Internet itself. It is imperative we hold them to a high standard for their search results, keeping algorithms fair for all. These have not been the only marginalized groups online though; Anti-LGBTQ+ campaigns have gained traction recently, organizing on large platforms to share disinformation after posts made from a number of republican politicians. In a study from the Center for Countering Digital Hate in collaboration with the Human Rights Campaign, it was found that Meta ran 59 ads in the month following the passage of the 'Don't Say Gay or Trans' law promoting the narrative of LGBTQ+ communities grooming minors, which also contributed to a 406% increase in 'grooming' related content on Twitter and Meta's platforms. "Twitter failed to act on 99% of the 100 most-viewed hateful tweets", and Meta's platforms reportedly only removed one of the 59 advertisements. Almost 1 in 5 of all hate crimes are now motivated by anti-LGBTQ+ bias, creating the deadliest past two years for the LGBTQ+ community (CCDH & HRC, 2022). These companies are not only showing great disregard for the safety of data, but also for individuals' safety and well-being. With how much information and traffic comes through Meta, Google, Twitter, and the like, they need to do better with removal of hate speech on their platforms and ensuring equality in terms of how their platforms are run.

Ever since children were able to figure out how to bypass age restrictions on sites, there has been valid concern for the privacy of minors online. While many platforms may be protected legally themselves by restricting content to those above a certain age, realistically there are still plenty of people that log on to these sites and apps claiming to be younger than those restrictions allow. Concerns of how image-driven social media are affecting users' self-confidence and self-image were shown in a study done by Katherine Hild (2017). Images displayed online are very often filtered and touched-up electronically, creating a façade of what younger audiences may want for themselves in terms of body image. Hild also discusses an "elimination game" passed around on Instagram, which boils down to a mean-spirited beauty contest. Cyberbullying has been a growing concern for middle and high school students as the popularity of social media has exploded. The CCDH & HRC found that more than 60 percent of LGBTQ+ youth feel their mental health has deteriorated, which can be attributed to the hateful messaging online (CCDH & HRC, 2022). In general, social media usage is associated with negative psychological outcomes, even though most young adults use it regularly. Internal research at Instagram found that nearly a third of teen girls reported having a more negative body image of themselves when using Instagram, with one in five teens saying the platform makes them feel worse about themselves overall (Wells, Horwitz, & Seetharaman, 2021). Despite this, the platform continues to expand to younger audiences with little disregard for their users' mental health. Facebook as well continues to consistently downplay their app's negative effects on teens and adults' mental health, hiding internal research from the public and evading answering questions on the topic. Younger generations, as well as their parents, need to seriously consider how much time, and where they spend it, online.

Clearly the Internet has suffered from the corporatization it has experienced in the past decades. People are being used like products for their personal data, minority groups are being marginalized, and users' safety has taken a backseat to profits. We have seen how hate groups are able to organize and preach their hate speech unbothered on large platforms, and there is great concern this problem will only increase in the future. Better protections need to be put into place for children,

minorities, and the general public by the government, with penalties going to corporations that remain ignorant. Schools need to be teaching students about best safety practices when it comes to their data online, and to not tolerate cyberbullying and hate speech. Law enforcement needs to be kept up on best practices for assisting those who have had their private information leaked online and getting victims the resources they need. The corporations that deal in data need to hire more employees to monitor what gets posted online, ensure hate speech is minimalized, and constantly improve algorithms so they are working fairly for all. The dangers that come with our hyper commercialized world wide web hardly seem worth it, and changes need to be made to ensure surfers' safety.

References

Allan, A. (2017, November). *The coming privacy crisis on the Internet of Things | TEDxExeterSalon.* Retrieved from YouTube: https://youtu.be/yG4JL0ZRmi4

Andrew, J., & Baker, M. (2019). The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*, 565-578.

Bastos, D., Shackleton, M., & El-Moussa, F. (2018). *Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments.* IET.

CBS News. (2018, December). *Facebook faces lawsuit for Cambridge Analytica privacy breach.* Retrieved from YouTube: https://youtu.be/JADsm2YmApQ

Hild, K. A. (2017). *Leave me alone: Protecting children's privacy in the digital age.* Washington DC: Georgetown University.

Kennerly, E. (2018). *Privacy and the internet.* CQ Researcher.

Metzger-Riftkin, J., & Eckert, S. (2020). *Doxxing, Privacy and Gendered Harassment.* The International Encyclopedia of Gender, Media, and Communication.

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism.* New York: NYU Press.

Simpson, S. (2004). Explaining the Commercialization of the Internet. *Information, Communication & Society*, 50-68.

The Center for Countering Digital Hate. (2022). *Digital Hate: Social Media's Role in Amplifying Dangerous Lies About LGBTQ+ People.* The Human Rights Campaign.

Wells, G., Horwitz, J., & Seetharaman, D. (2021). Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show. *The Wall Street Journal*.