Jessica Laemle
Presentation Paper Reflection

Prior to researching and presenting privacy and security in our digital world, I didn't have much knowledge regarding these topics. I was aware that privacy and security are much debated issues in today's society and I had heard that companies have access to our information, but I had no idea of the extent to which our personal information is taken from us and being used by large companies to generate profit. I also wasn't aware of the many vulnerabilities of new technology and how it is very easy for others to break into what we believe to be secure databases. After learning more about how easy it is for our personal information to be taken without our permission by companies who intend to use it for profit or without our knowledge by hackers who use it for identity theft or other schemes, I have found myself being more cautious and skeptical when I am using the internet and digital platforms.

There were many key concepts that I was able to identify based on the research our group completed and the lesson that we developed to share our research with the class. The first key concept is that there are many ways that companies/platforms can track you, and as a result, it is next to impossible to keep yourself completely anonymous. Some of the ways that companies track users are known, but others remain hidden. Some surveillance techniques include: lead generation (information retrieved from surveys, applications, forms filled out online) (Hebert 2016); loyalty cards (which are used to track what a customer buys and build a profile about them) (Villanova N.d.); cookies (files that give your device a number and allow it to be recognized when it comes back to the site) (Ucros N.d.); heatmapping (tracking the movements of your mouse/finger) (Ucros N.d.); and, Wi-Fi (free Wi-Fi networks will track where your device goes and can see what you do while on the Wi-Fi) (Ucros N.d.). While these are just a few ways that companies can track your information, there are many other more obvious ways

that companies can also capture your data. With so many possible entry points to accessing information, consumers face a constant struggle (and one we have not been very successful at tackling) to try and keep our data safe, especially when we may not even know that our information is being taken from us.

Jumping off of the idea that it is nearly impossible to keep our data and information to ourselves, another key concept that came out of our research is that wherever we go online, and whatever we do, we leave a "digital footprint" (Internet Society N.d.), which has many implications--some good and some bad. Every click, like, tweet, post, Google search, etc. contributes to a growing file of information that is stored about us, allowing the internet to know us better than we know ourselves. Even the personal information that we share on social media is part of what is accessed and used to create our digital footprint (Internet Society N.d.). While the traces of information that we leave behind can help personalize our digital experience and make it more convenient and focused on us, such as populating our feeds with targeted ads which match our interests and allowing us to store personal information on the web (Internet Society N.d.), the negatives outweigh the positives. Our information and past actions can be sold for profit, from which we don't benefit. In addition, this widespread collecting of our information makes us more vulnerable to hackers and others whose intentions aren't good when handling our data. The type of information that can be obtained about us digitally is overwhelming, including things such as: phone numbers, name, birthdate and address (Haselton 2017). Other things that can be obtained are current and past locations we have visited, private emails, political party affiliation and your search history (Zomorodi 2017). Another concerning piece of information that can be collected is credit card/banking information. Collecting all of this data and using it to target us with advertisements or articles that we might be interested in creates our own little box,

or echo-chamber (similarly called a filter bubble by Eli Pariser), that feeds us only the information that relates to what we already follow, thereby failing to expose us to other products and information that may be beneficial for us to know (Lindgren 2017:56). The information gathered about us can also extend to have an impact on our offline world. For example, the government can use your digital footprint against you. A cyclist named Chris Bucchere was responsible for hitting and killing an older individual. In order to build the case against him, information from Chris' fitness tracker was gathered (Weinstein 2015). In this example, the use of information was helpful and used in a positive way to solve a crime, but it is important to look deeper and understand the amount of privacy that was violated to gain access to Chris' fitness tracker data.

How has this rise in privacy violations and increase in information gathering become possible? As time has progressed, we have seen a proliferation in the number of digital consumers, who can be classified as those who get their information and products and basically do all of their transactions online. They are people who use the internet constantly (Lindgren 2017:148). This shift to doing everything online and constantly being "plugged in" combined with technology becoming more advanced and sophisticated, has allowed for the clever minds behind some of the biggest digital platforms (and those that are not as big) to figure out how to take our constant use of the digital world, gather the content we are producing online and capitalize on it. As we become increasingly molded into digital consumers, we have less of an issue accepting the fact that we are unable to completely control the ways in which companies and others have access to our personal information. In addition, as we become more representative of digital consumers, we are engaging more and more in what Fuchs and Scholz call digital labour (Lindgren 2017:171). The concept of digital labour talks about how, as we

voluntarily use the many platforms, services and websites that our digital world has to offer, we are creating valuable profiles that are taken advantage of by those who control these platforms. The information and data we produce online is created on "free" platforms. However, these platforms aren't really free because just about every piece of our data is sold by for profit companies. These companies are paid by marketers who want our data so that they can create targeted advertising campaigns and ultimately influence our buying patterns and decisions. Smythe defines this as audience commodity (Lindgren 2017:172). The companies behind digital platforms and services aren't concerned with keeping the consumer safe and protecting their data as much as they are focused on their corporate growth potential and they see users merely as a way to make money. Therefore, we need to keep in mind that when we choose to engage with the digital world and participate in digital consumerism, we are trading privacy and protection of our personal information for convenience and ease of use. But is it worth it? That depends on which users you ask, but a majority of users would likely say yes.

As the digital world becomes more widely used, consumer behavior enables companies to stay in business because of our "free" use. Facebook, Instagram, Twitter and Snapchat, just to name a few, are all continually growing in popularity. With billions of users, these platforms count on the creation of new content and information from users to keep them in business. Furthermore, other companies such as streaming services (Spotify and Netflix) and additions to Apple (such as iCloud), have taken the gathering of data a step further by charging consumers to use their services. Spotify and Netflix have been seeing a rise in the number of subscribers due to cord-cutting (Snider 2018). Cord-cutting is when a user will get rid of their cable subscription or satellite radio subscription and instead invest in a streaming service (Snider 2018) Part of the reason that users engage in this behavior is because of the price (Snider 2018). While still

expensive, these streaming services are not nearly as pricey as cable and satellite radio subscriptions. However, while the visible costs of these streaming services are less expensive, ultimately, they could end up costing you more. Not out of pocket, but because the personal information that is retrieved about you can be worth thousands of dollars to a company you may never have heard of before. One of the ways that streaming services can access and use customer information is because users store their credit card/billing information and preferences in order to continually renew their subscription month after month. In addition, these services will watch and keep track of what you are interested in and will then use the information gathered about you to give you recommendations for what to listen to or what to watch. For example, on Spotify you can see recommended playlists and on Netflix you will be given a section containing movies or TV shows you might like. These user preferences can also be sold to other companies in order for them to form a larger and more detailed profile about a user. Consumers won't always know what is done with the data they leave behind when using online streaming services. Users who leave credit card information on the web to expedite future transactions, can be susceptible to having their information hacked and used by others maliciously (Webroot N.d.).

Another digital platform that is growing in popularity is iCloud. While iCloud is free initially, most people have lots of information to store and if you want all your information to be conveniently saved, you will need to purchase more storage. But what are you really purchasing? Are you purchasing space where your information and private files will be safely stored and protected? Or are you paying for your vast amounts of personal information to be available to other sites, platforms and potential hackers? The cloud is one example of a term that has changed its meaning over time as technology has continued to evolve and become more sophisticated. Prior to the rise of the internet and the digital world, the cloud was simply referred to as the

fluffy thing in the sky. In our current digital world, however, the cloud is the place where users and businesses can store information such as notes, photos, work, contacts and so on. In addition, the cloud gives us the ability to access these files from anywhere (Coles N.d.). The meaning of this seemingly common word has drastically changed over time.

If you were to ask most users about the cloud, they would probably have a general understanding of what it is and what it does. However, few would look beyond its functions and convenience. If we take a critical lens to look at the cloud, we can see the hidden meaning behind the word: this way of storing our information is "fluffy" (or lacking a secure and serious approach to keeping our uploaded information private). While the cloud's meaning, if analyzed deeply, has a negative connotation, there are some benefits of this service including: ease of use and access to information; a fairly cheap way to store data and information; a system that allows different members of an organization, group or family to all have access to uploaded files in a way that is portable; and, the cloud can handle a lot of demand and store a large amount of content (Coles N.d.).

While the cloud has different functions, it is similar to other platforms in that there can be more potential concerns than there are benefits. In addition, the benefits can become concerns if they are taken advantage of and used with bad intentions. The main concern associated with the cloud is the potential for invasion of privacy and for hackers to steal and use private information (Angeles 2013). In our research, one important example that our group came across to highlight the dangers associated with the cloud, was the case of Edward Snowden. Snowden worked for the NSA, and while there, he tried to raise security and privacy concerns to those higher up and was ignored. Snowden then publicly leaked the information that the NSA had on individuals,

including some of which was gathered from the cloud (Szoldra 2016). This case gives a very powerful real-life example of the impact of the fragmented privacy we face in our digital world.

Another important aspect that came up in our research is that all of the platforms/services that have emerged come with their own 'terms and conditions' agreements. These terms and conditions need to be accepted by the user before they start to engage with these platforms. In relation to these 'terms and conditions' agreements, a key idea that our research pointed out was that, not surprisingly, most 'terms and conditions' agreements are extremely long, and are purposely designed to be hard to read because of the use of small lettering, capital letters and condensed wording and sophisticated digital jargon that no average user (and even some professionals) can't understand (Lomas and Dillet 2015). In addition, words or phrases that might raise a red flag for consumers are included among the usual legal jargon and no effort is made to highlight or point out a potential concern in the terms. So, while users do agree to these terms, we are often deceived into agreeing to certain things. Companies purposefully make these agreements hard to read so that we quickly scroll through and then click 'accept' by default. What is crucial to remember about 'terms and conditions' agreements is that we are agreeing to these companies having the ability to take and have access to all of our personal information. We are agreeing that they can use our data how they see fit (Lomas and Dillet 2015). Unfortunately, these big companies don't necessarily have a moral vision for how to use our personal data, which leaves us in a vulnerable position. As consumers, we click accept because we wrongfully assume that just having terms and conditions in effect means a company will protect us and our information. However, these agreements don't mean that we are protected, and having these agreements doesn't automatically mean they are followed. Furthermore, companies can frequently change their terms and conditions without formally notifying users. As digital

consumers, we trust these large companies by default and are not automatically skeptical of their motives. This is often another reason why we don't read the terms and conditions agreements put in front of us. As a society, we collectively assume that these large companies will be dedicated to protecting our information and that they will not violate what they say. These misconceptions on the part of the user have been the source of much debate and tension between companies and users. If we look at other fields in society (such as medicine), the side effects of a medication must be communicated and made available to a consumer. This is not the case with terms and conditions agreements. A question to think about for the future is whether or not for-profit companies should be required to disclose and describe specific points within their terms and conditions agreements, which could compromise user data. This could help users make more informed decisions when they click 'accept' because they will have a chance to understand the potentially harmful terms they may be agreeing to. As we continue to witness more frequent leaks and abuse of consumer information, this requirement could be beneficial for our digital society.

What would be the implications of companies being required to notify consumers about the specifics of their terms and conditions agreements? There are so many online users in our society that if a handful were deterred from signing onto a platform because of the terms and conditions, it would not pose a significant risk to big companies. There would still be billions of other users to gather data off and to make money from. However, for an individual user, not agreeing to the terms and conditions means you will be missing out since most other people you are connected with will still be using the platform/service. For example, not agreeing to Facebook's terms and conditions could potentially mean that a consumer loses access to many people they would otherwise be able to connect with. Therefore, it is more of a compromise to

the user experience if you do not agree to the terms and conditions. As a result, most people will choose to agree because of the convenience and necessity of staying current within their friend or family groups. The reliance on digital platforms and services to keep us informed and in touch with others makes users more likely to compromise their concerns and be vulnerable to giving up their private information. However, the users who do agree to the terms and conditions are becoming more aware of the potential misuse of their information; and, with companies under fire for their lack of responsibility, we may start to see some impact.

The fact that the large and powerful companies which are responsible for major data breaches are not punished for the invasion of privacy they perpetuate, brings up another key idea that we encountered in our research. This is the fact that there is a big divide in our society and certain groups have control over others. Something we see with a lot of large companies is that the right to remain silent is utilized to its full potential. The government is getting much of our personal information from these companies, so forcing them to expose what they gather and limiting how they are allowed to get information would not be beneficial to the government (Wolff 2018). We also see that companies can often say what they want without facing repercussions. And, like we saw with Edward Snowden, individuals who try and expose the inappropriate relationship between companies and the government will be punished in order to protect the group that is more powerful. In addition, many of these large companies have personal connections with individuals that work for the government, further incentivizing the government not to be strict when dealing with these companies (Wolff 2018). We have to wonder what the potential impact of this dynamic will be down the line, and it is likely that it won't be good for the average consumer.

Theorizing about the impact of the lack of privacy associated with our increasingly digital culture, it is hard to identify any good outcomes. The increase in the ability of for-profit companies to gather our personal information undermines the potential benefits of participating in our digital culture. Every time a new platform or aspect of digital culture is introduced, more privacy threats arise. In the past, users have been relatively unaware of the access that others have to the personal information that is available online and how it is being used. In the wake of recent and more frequently occurring data breaches (for example the Snapchat data breach in 2013 that affected 5 million users (Elsevier 2014) and Cambridge Analytica) and news stories exposing how companies and others get our information, users should be more aware, concerned and skeptical of the ways they engage in social media and online services. Many users see this lack of privacy and security as a concern but feel that the convenience of our digital society is worth more than keeping their personal information private (Miao N.d.). Others who want to increase the level of protection on their information will look for tips and ways to stop companies from gathering their data. These users believe that if they can find ways to block their personal information, then they will be able to protect themselves while continuing to use the digital platforms which are very important in their day-to-day lives (Rainie 2018). However, the corporations and hackers seem to always be one step ahead in developing ways to access data and find holes in the current system. Users who are aware that their information is being exploited may want to stop using digital platforms all together, but this would require them giving up full use of the internet and digital media, which makes it basically impossible to function in our modern world. Our society has become so reliant on the digital world that being able to survive without at least a minimal use of digital platforms and services would be difficult for most users to imagine.

With our society's rapidly increasing reliance on the digital world, almost all of our transactions and interactions can be conducted online. We gather news, make purchases, connect with family members and friends (local and long distance), store passwords and banking information, etc. We are trusting the complex and sophisticated digital world with almost all of our most valuable information. While we think we are finding ways to protect our privacy and we are doing what the companies tell us to do in order to be protected, these methods are not sufficient. As our world continues to become more wrapped up in digital culture and technology continues to advance, new ways of tracking and gaining access to users' private information will surface. There are no signs that our digital culture will slow down. In fact, the future of digital culture seems to be heading towards increased reliance on digital platforms. If tracking, privacy of information and surveillance of users is already such a big issue, we can expect the future impact to be even more dangerous if stricter measures are not put in place. The companies performing surveillance and violating our privacy will only become stronger in the methods they use to gather our data and generate profiles about us.

As we move towards the future of privacy, security and tracking in our digital culture, we need to be aware that companies won't be willing to change their surveillance habits because of the benefits they receive in the current climate. Recently, we have seen some of these companies be confronted for their actions (like when Target had to go public about a breach (Elsevier 2014) in their credit card system). This is a good starting point, but this isn't nearly enough to change the current culture. Often, when companies get in trouble for spreading user information, they will put out a statement, testify if necessary, and move on. If changes to their 'terms and conditions' agreements are required, companies will write them in such a way that they can still gather the desired information. We need to develop strict guidelines and consequences for these

companies when they cross the line in how they gather and use personal information and our society needs to hold them accountable for their actions. Changing privacy policies and implementing consequences requires corporate compliance, social responsibility and individual effort and will not likely be a smooth transition. However, this is a necessary change because if not, we will foster an increasingly dangerous digital culture where others know more about us than we know about ourselves.

Works Cited:

Angeles, Sara. 2013. "8 Reasons to Fear Cloud Computing." Waltham, MA: Business News Daily. Retrieved October 1, 2018 (https://www.businessnewsdaily.com/5215-dangers-cloud-computing.html).

Coles, Cameron. N.d. "11 Advantages of Cloud Computing and How Your Business Can Benefit from Them: How Companies Using the Cloud Grow 19.3% Faster Than Their Competitors." Skyhigh Networks. Retrieved October 8, 2018 (https://www.skyhighnetworks.com/cloud-security-blog/11-advantages-of-cloud-computing-and-how-your-business-can-benefit-from-them/).

Elsevier. 2014. "Target and Snapchat Suffer Major Data Breaches." *Computer Fraud and Security* 2014(1): 1, 3. Doi: https://doi.org/10.1016/S1361-3723(14)70001-6.

Haselton, Todd. 2017. "How to Find out What Google Knows About You and Limit the Data it Collects." CNBC. Retrieved October 2, 2018 (https://www.cnbc.com/2017/11/20/what-does-google-know-about-me.html).

Hebert, Amy. 2016. "How did That Company get My Info?" Federal Trade Commission. Retrieved October 8, 2018 (https://www.consumer.ftc.gov/blog/2016/09/how-did-company-get-my-info).

Internet Society. N.d. "Your Digital Footprint Matters." Reston, VA: Internet Society. Retrieved October 4, 2018 (https://www.internetsociety.org/tutorials/your-digital-footprint-matters/).

Lindgren, Simon. 2017. *Digital Media & Society.* London: Sage publications Ltd.

Lomas, Natasha and Romain Dillet. 2015. “Terms and Conditions Are the Biggest Lie of Our Industry.” TechCrunch. Retrieved September 29, 2018 (https://techcrunch.com/2015/08/21/agree-to-disagree/).

Miao, Christine. N.d. “Why You Don’t Care About Internet Privacy (And Why You Need To).” Medium. Retrieved October 9, 2018 (https://medium.com/@christinemiao/you-dont-care-about-internet-privacy-you-should-7b16ef2fcc71).

Rainie, Lee. 2018. “Americans’ Complicated Feelings About Social Media in an Era of Privacy Concerns.” Washington, DC: Pew Research Center. Retrieved September 10, 2018 (http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/).

Snider, Mark. 2018. “Cord-cutting Isn’t Just Happening, it Could be Escalating.” *USA Today,* June 22. Retrieved September 30, 2018. (https://www.usatoday.com/story/tech/talkingtech/2018/06/22/cord-cutting-isnt-just-increasing-could-escalating/720812002/).

Szoldra, Paul. 2016. “This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks.” Business Insider. Retrieved September 28, 2018 (https://www.businessinsider.com/snowden-leaks-timeline-2016-9).

Ucros, Melody. N.d. “10 Sneaky Ways Companies are Collecting Data to Understand Customers: Find out How and Why They are Doing it” Medium. Retrieved October 1, 2018 (https://medium.com/@melodyucros/10-sneaky-ways-companies-are-collecting-data-to-understand-customers-be0b9089d54a).

Villanova University. N.d. “6 Unusual Ways Companies Can Collect Your Data: Find Out How Companies are Gaining Access to Your Personal Data.” Villanova University. Retrieved October 10, 2018 (https://www.villanovau.com/resources/bi/6-ways-companies-can-collect-your-data/).

Webroot. N.d. “The Dangers of Hacking and What a Hacker Can do to Your Computer.” Broomfield, CO: Webroot. Retrieved September 29, 2018 (https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-hackers).

Weinstein, Mark. 2016. “What Your Fitbit Doesn't Want You to Know.” The Huffington Post. Retrieved September 10, 2018 (https://www.huffingtonpost.com/mark-weinstein/what-your-fitbit-doesnt-w_b_8851664.html).

Wolff, Josephine. 2018. “Why it’s so Hard to Punish Companies for Data Breaches.” *The New York Times,* October 16. Retrieved October 16, 2018. (https://www.nytimes.com/2018/10/16/opinion/facebook-data-breach-regulation.html).

Zomorodi, Manoush. 2017. “Do You Know How Much Private Information You Give Away Every Day?” *TIME,* March 29. Retrieved September 11, 2018. (http://time.com/4673602/terms-service-privacy-security/).