Gerardo Nunez
SOC 250
10/25/18
Presentation Reflection

Being a citizen means being a legitimate participating member of society. With the rise of technology and the growing number of ways the internet is used to communicate and interact socially, citizenship in digital culture is has become an important topic. Citizenship in digital culture has many expectations like being a citizen in the real world does, such as societal competence, navigating the public sphere, and privacy. This week our group was set to present on Citizenship in Digital Culture. Based on a survey that paired our online interests with similar topics to present the weeks' topic, our group focused on privacy and cloud storage that are integrated into our daily digitized lives through the apps and services we use. The internet offers many services that range from streaming to storage. These services often require user information that is perceived to be protected under various privacy policies from online hosts. The research my group conducted revealed the realities of online privacy and the uses of cloud storage and its susceptibility to malicious online behavior often found on several online platforms such as social media and streaming services. With a rapidly advancing society, transition to a digital society is a new and tricky process that needs to be treated like a tangible society. Citizenship in digital culture is being an active member of the online community. The internet has become its own society with its own subcultures that are structured differently than others but, the general principle of an online society and digital citizenship backs should support the rights of the users rather than use loopholes and exploit the user's privacy and information.

Chapter eight of the textbook highlights privacy as being public. Many internet researchers have shown how the boundaries between the public and the private are eroded in digital society (156). While the book goes on to speak on how political and personal affairs are now becoming intertwined due to the internet and social media, Jessica focused her research on user privacy on various levels of the web. Jessica's research on privacy established its definition, per Business Dictionary, as *"the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed."* The Oxford Dictionary defined publicity as *"the giving out of information about a product, person, or company for advertising or promotional purposes."* These two definitions seem to not apply on the internet. Privacy on the internet is the opposite of what it is defined as. The reality of privacy on the internet is hidden in privacy policies and agreements that people sign off on. These policies allow websites and companies to collect personal data with the intent of selling your information for their profit. This poses the question: does online privacy exist in a digital society? The internet was developed in the 1960s but did not become the internet we know today until 1990. Based on the research and readings, the internet was invented to be used in the military with privacy in mind. Following the attacks on 9/11, The Patriot Act was passed which allowed for more and new surveillance authority to be granted to law enforcement and intelligence agencies. This marks the start of the invasion of property on the internet from the government and other online intelligence. Several other technological advancements, like the invention of the smartphone, have made personal privacy easier to exploit. Several data breaches have occurred across several platforms of social media and many go unnoticed by the user. Furthermore, these same social media platforms utilize terms and conditions to access personal information and allow them to share it with third-parties. Companies do not protect privacy as much as they say they do. What they make private on the platform, the backend information gets sold to advertisers or other researchers. This is possible through the user agreement when they sign off on the terms and conditions. Companies purposely write their terms and conditions in corporate jargon and make it difficult to read in depth with the intention that you will agree to their discrete activities. Companies can track your information in various ways such as cookies and fingerprinting. Whenever you are on the internet you leave a digital footprint. Everything you do online leaves behind information about you that others can pick up and follow to create a profile and gather information about you. This information is sold to third-parties and used in several ways to create an online environment tailored to your likes and interests. With more online platforms being user based, information is stored in many fashions including cloud based storage that is also susceptible to privacy issues.

Cloud storage is a cloud computing model where data is stored on remote servers accessed from the internet, known as the "cloud." It is maintained, operated and managed by a cloud storage service provider that must handle many users on their storage platform. Andrew's research was focused on the cloud based storage systems and their uses in today's digital society. The "cloud" allows users to use external storage without using the storage on their computers or another physical hard drive. What is stored on the personal cloud storage is based on the user. When using platforms that use platform based storage, personal and user information is stored on the "cloud." As found in Andrew's research, many services like email, finance & accounting, and HR services, are among the top business currently in the cloud. With the advancing technology and the immersion of the general population with the internet, storage will become an issue and cloud based storage services offer a solution. There are several benefits of cloud storage that appeal to businesses and individuals such as the cost, maintenance, and ease of use. Although the benefits of cloud based storage are appealing, problems have occurred that have questioned the security of cloud based systems. The Snowden scandal proved that private information stored online can be made public. The cloud offers online storage that is accessible to a collection of users or a single individual but is still at the discretion of the users and the online community that can hack into these storage services. As more services and platforms move to cloud based storage, companies are sneaking privacy policies into the terms and conditions so they are not held completely liable for your information and grants them the ability to use your information as they please. As a citizen of the digital culture, the user's rights to privacy need to tightened as using the "cloud" leaves individuals exposed to the threats of online hackers and third party entities.

As mentioned previously, privacy becomes a big issue when the services and platforms people use on a daily basis intentionally misguide the user in the terms and conditions with lose privacy policies. This is found across all platforms that contain a terms and conditions agreement. My research was focused on the everyday applications where privacy is being falsely presented. First, we are in an age of advancement where technology is become an integral part of everyday life. Taking tangible objects or material and converting them to a digital copy is known as digitization and is steadily becoming a norm in our society. My research found an example of people shifting from cable television to subscription based streaming services, referred to as "cord cutters." With the rise of streaming in both television and music, these subscription services require users to set up accounts with personal information. These services are using user information to build a personal experience on the platform. These platforms get to know the user and there likes and interests and caters the content to their taste. This use of information is private and personal that is available to a computer. These files of information are susceptible to online dangers that surround the internet. These services that are used daily and collect data on the user are thought to be public but are actually readily available to corporations who are willing to sell and pay for our information.

Looking to the future of the digital culture, privacy will continue to be an issue with the platforms and services that are widely used. The growing trend of corporations using user data as a consumer good for third-party buyers leads to theorize the future of privacy will follow suit. The same companies that are requiring accounts to be made are creating overly complex terms and conditions that trick the users into signing loose privacy terms. Based on research and cultural trends, companies will continue to write these overly complex terms and conditions as long as there no pressure from the users of these platforms or stricter privacy regulations are placed by the government or some other governing entity.

. Through technology and the numerous ways, the internet has been used to communicate and interact socially, citizenship in digital culture is has become a key point on the internet. The internet has become its own society with its own subcultures that are structured differently than others but privacy becomes a growing concern in every part of the web. Our group focused on privacy and cloud storage that are integrated into our daily digitized lives through the apps and services we use on a constant basis. As a citizen of the digital culture, it is important to be aware of privacy agreements that an individual use. It is a right as a citizen to understand what is really going on when the private is public on the internet.

Works Cited

Lindgren, Simon. *Digital Media and Society*. SAGE Publications Ltd, 2017.