Ethics and Engineering
ENGR 482

Snapchat: Fine Lines in Plain Sight

Summer 2019
Group 4

Citation: APA Style

Members:

- Hayfaa Al-Kuwari
- Oscar Martinez
- Sara Al-Mulla

Submission Date: July 9, 2019

"An Aggie does not lie, cheat or steal or tolerate those who do."

Introduction:

With 200 million daily active users and continual rise in popularity, Snapchat has allowed more and more users to mitigate distances and stay connected with friends and family. Snapchat is one of the leading social media platforms used globally and enjoyed by many people it is also one of the most influential apps due to loyal users and celebrity usage. However, in recent times, Snapchat has lost the trust and credibility of many users and non-users. They fear Snapchat despite its beneficial features due to the platform operating under questionable privacy practices and policies. Some people argue that although Snapchat claims to provide a secure social media platform, where anything shared will disappear after 24 hours, and the user's privacy will be maintained; however, this is no longer true, and much information is accessible by third parties and potential hackers. Snapchat also intentionally lends private information to third parties, tracks the user's location, and retains uploaded content that does not disappear from Snapchat's databases for months. It is imperative that snap-chatters delete the application because the new policies changed Snapchat far from its initial purpose, fragile security systems may put private information at risk, and invasive features do not respect the user's privacy, therefore resulting in deceptive practices.

Literature Review:

With the technological development of communication, being on social media and using their features is something unavoidable, most of the people who use social media apps still have some concerns about their privacy and how their data is being used. Even though Snapchat shows the users that their messages, photos and videos disappears within 24 hours, it appeared that they have the right to use our data anytime they need (French, 2015). According to their Terms of

Services it states that “Snapchat has the rights to reproduce, modify and republish your photos and save those photos to Snapchat’s servers, specifically in relation to the ‘Live Story’ feature” (French, 2015).

Social media applications, such as Snapchat, are keen to entertain their users through the built-in features. However, many issues were raised about Snapchat’s built-in features regarding privacy. The authors of “UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION “(Ramirez, Brill, Wright, & McSweeny, 2014) previewed the privacy issues that Snapchat faced since its creation in 2011. They mainly argue about the violations that Snapchat made through creating the built-in features such as, Finding friends nearby and the Snap map without the user’s consent. This solidifies the idea of how these features might be deceptive in some ways and how they cause leakage in the application’s privacy, through listing all types of features and the violations that were being done by the company.

Also, Snapchat is using their privileges as a company to invade people's privacy to make a profit, where in 2017 Snapchat began to give advertisers the ability to employ what is called a “pixel.” This is a tool that allows advertisements to be catered to each individual (Sloane, 2017). This means that Snapchat gives third parties the ability to track our history thus being able to provide ads that are specific to our interests. This article leads us to believe that Snapchat is not concerned about our privacy and everything we search for, or browse through, is being tracked. Even though this could be helpful for the user to see what he/she likes, it is invading our privacy in ways that a user might not consent to.

Furthermore, regardless of the way Snapchat is promoting their application (offering a platform which emphasizes the sharing of temporary content to your friends) people are still concerned about the security of their information. The authors of “Security Analysis of Snapchat”

represented their ideas about the security of snapchat in iOS and Android devices. Their main arguments were about the way the code is created and how it can be used as a double-edged sword for attackers seeking people's information. This can be done by using third parties application called the tweak apps. Also, by using free applications this means we pay our privacy to the application owners so that they can get profit (Leetaru, 2018). Additionally, the article entitled "How to use Snapchat to DoS Attacks any Phone" inspired us to search more around this topic and helped in supporting our arguments about the insecurity of the application, which helped in directing certain questions to Dr. Joseph Boutros an Electrical Engineering faculty at Texas A&M Qatar for this paper.

Discussion and Analysis

- **Policy**

Many users were drawn to the fact that Snapchat revolved around temporarily sharing photos and videos. This brought a new perspective to social media platforms and soon became the favorite app amongst teens and young adults. "Life's more fun when you live in the moment." This simple motto defined early Snapchat as it began to rise in popularity back in 2011. Two years later, Snapchat updated its privacy policy that would almost revert on its original intention. In small, fine text, Snapchat would show users its new changes and make them agree to the new terms and conditions. Many users failed to notice the significant changes and assumed Snapchat still operated under the premise of "temporary sharing." The main feature that came with the new policy stated that "Snapchat has the rights to reproduce, modify and republish your photos and save those photos to Snapchat's servers, specifically in relation to the 'Live Story' feature" (French, 2015). This new statement contrasts with the former privacy policy which stated that "delete is our default" and that "In most cases, once we detect that all recipients have viewed a

message, we automatically delete it from our servers" (French, 2015). The new policy was implemented in a way that allowed Snapchat to retrieve sensitive information that can be used to aid in criminal investigations when obligated by law (Edwards, 2014). This upset many users, rightfully so, since they were no longer able to post videos/photos/send messages without potential legal repercussion. As such, Snapchatters should take the time to consider deleting the app due to the information Snapchat servers retain, and how they could use it against you. During this time, Snapchat has also allowed the sharing of private information to third parties.

Third party information sharing was not an unfamiliar practice when Snapchat implemented it. This has been used by other social media platforms like Facebook and Google way beforehand (Stewart, 2017). Before, Snapchat would show every user the same advertisements, but in 2017 Snapchat began to grant advertisers the ability to employ what is called a "pixel." This is a tool that allows ads to be catered to each individual (Sloane, 2017). This means that third companies can track your history and make you a target to view ads that are specific to your interests. This works by putting a bit of code, pixel, on a website, the companies can then measure when a person saw their ads somewhere else on the web (ibid). Pixels are also used to retarget ads, showing people advertisements they had already seen elsewhere (Edwards, 2014). Snapchat claims that "It lets marketers measure the revenue, performance, growth, and acquisition driven by Snapchat--such as website visits, purchases, and sign-ups--across devices," they followed with "Over the coming months, we'll release additional features beyond measurement -- such as custom audience creation and real-time optimization -- designed to help businesses drive the most meaningful user actions for them" (Sloane, 2017). All of this means that Snapchat users now have less control over their accounts, and they can no longer browse the internet without their every move being tracked. Many people are fearful of allowing Snapchat to dictate the policies in

which users are required to agree to, as such new laws and regulations are being pushed forth by the world's governments. Social media users should back these new reforms to regain many digital rights taken away by these social media platforms.

Snapchat states in its privacy policy, the type of information they collect from users. This includes but is not limited to the content of the installed apps on our devices. We decided to interview Dr. Joseph Boutros, an Electrical and Computer Engineering professor working at Texas A&M University at Qatar. His main expertise is in information theory and digital communication, as such he has knowledge in developing a secure network and applications in general. He informed us that when users give authorization to social media applications, such as Snapchat, they have access to confidential information located on the user's phone. They then allow companies to have access to everything in their mobile phones, which is the opposite of what phone companies like Apple and Samsung claim to protect. They state in their policy that phone details and information is protected (Boutros, J., personal communication, June 25, 2019). These types of policies are unethical according to the National Society of Professional Engineers: Code of Ethics. Canon 1, article C claims that "Engineers shall not reveal facts, data, or information without the prior consent of the client or employer except as authorized or required by law or this Code" ("Code of Ethics", n.d). Therefore, by not allowing Snapchat users to fully consent to that extent of information access, the engineers that implemented this are conducting themselves unethically. Snapchat users should not tolerate this type of behavior and are suggested to delete this application to secure their privacy and rights.

Following the congressional hearings and the backlash Facebook faced after the Cambridge Analytica hack, many social media platforms are regionally being required to update privacy policies and data storing. For example, any company operating on the web, in a country part of the

European Union, is required to adhere to the new law: The General Protection Regulation (Godlewski, 2018). This new law protects social media users by allowing users to access the data that the company stores for them, and also gives the users the right to ask for the deletion of that data (ibid). Companies in this region are now making privacy policies and the terms of service easier to understand. Changing the way, the platforms or companies use data on a country-by-country basis would be difficult, so the new law in Europe has, in turn, positively benefited those globally (Godlewski, 2018).

Many countries still differ greatly in user rights on social media platforms. It is a constant battle between company interests and what they can get away with, against the users and the privacy rights they are entitled to. The victors stem from greater cultural norms or society's economic preferences. For example, in Qatar, Snapchat users are able to turn off targeted advertising and only see the general advertisements, while Snapchat retains no information. Meanwhile, the U.S versions do not have that option, arguably due to the large profits stemming from selling the user's private information. On the other hand, China has completely banned Snapchat throughout the country due to the lack of privacy and governmental emphasis on censorship (Jamie, 2018). More strides need to be taken, but overall some of the new changes and laws are helping users regain some of the privacy that was once unknowingly lost. In the meantime, if a great number of Snapchat users delete the application, this might urge Snapchat to reconsider its unethical policies and update them accordingly.

- **Privacy**

Snapchat has a wide number of users worldwide, and most people are fascinated by its spectacular features and not paying any attention to the details that might have a big impact on their lives. This paper discussed multiple policies that people agree to without conscious, neglecting the drawbacks and consequences that might come along with it. Due to the sudden change in technology and its development, many people believe that the internet has killed the privacy and it doesn't exist anymore. Privacy is having the right over your own information and the way it can be shared and used. (Symanovich, n.d). On the other hand, it is more likely to be exposed by using intelligent features that the application comes up with. Every year Snapchat comes with a new feature that would impress the people with its development. However, it confuses the users of how their information is being used and whether it is safe for them to use the features or not.

Entertaining the users is the main aim that Snapchat focuses on, no matter how these features might harm the person's privacy through using the app. In September 2012, Snapchat came up with the deceptive idea of Finding Friends feature. They were implying that the only information that Snapchat is taking is their mobile phone number to search for their friends easily. However, without taking the user's consent they were collecting all names and numbers of all contacts in their address book. Regarding this feature on New Year's Eve 2013, hackers released a database of the user's contact information and an incomplete version of their phone numbers (Defossez, 2014). Which brightly shows that Snapchat wasn't considering privacy and security as an important manner. Moreover, Snapchat failed to verify that the mobile number belongs to the mobile device that is being used by the individual itself or someone else. With this failure, it helped many people to create their accounts by using phone numbers that doesn't belong to them, which

enabled them to send and receive images and videos from the consumer's phone number, that caused a leakage of privacy.

Furthermore, Snapchat recently launched a location-sharing feature which is Snap Map. This newest feature made a lot of people concerned about whether to trust Snapchat and if their privacy is being violated or not. Snapchat claimed that they don't ask for, track or access any locations from our devices while using the app. However, it has been discovered that Snapchat company has integrated a tracking service in the Android devices and performed as it's a service provider. They used the user's Wi-Fi and Cell-based location information for the tracking service. (Ramirez, Brill, Wright, & McSweeny, 2014). Even though now the people have the opportunity to turn off this feature by turning on the Ghost mode. Many people aren't totally clear of how the app goes and how these features could be risky especially for women; the company isn't making everything clear for the user when using the app, as they mainly show the best of the features without warning the user of its risks. It's true that Snapchat mentioned that when turning on the Snap map feature, it would make their location appear every time they enter the app but only for their friends (Snapchat, n.d.). But it has been shown that many breaches could be caused by the Snap map location feature.

For example, an incident happened in 2018 here in Doha, Qatar, where the videos and photos of women in a private wedding where added in the Snap map without their consent. The girl who took the snaps shared it in her private account but later it appeared that the Snap map feature was enabled and she didn't know about it. So, when sharing such private snaps in famous places. For instance, the Sheraton Hotel a place with a huge number of visitors everyday, it makes it easier for the snaps to go viral and spread really quick by just adding them to the map on purpose

or not. It is important that the company respects people's privacy by notifying the people if their snaps might be added in public ahead of time to maintain their privacy.

Also, from what we observed in the app that even if the user used the Ghost mode, the location still appears in the map for the user only and it is being updated every time the user enters the app. Which can show that the Snapchat company still locate our exact location and it's being stored in their database in an uncertain period of time. Snapchat's default option when creating the app is that people share their usage data with the app unless they figure it out and turn it off. Hence, in this way or the other, privacy is being invaded where our data is being saved and used whenever they need. Due to the unethical problems, Snapchatters should consider deleting their accounts to maintain their privacy and stay safe.

As mentioned at the beginning Snapchat's slogan is "Life's more fun when you live in the moment." this slogan was applied through creating the Snap spectacles which is mainly a glasses that enable the user to take videos/photos while wearing it without holding the phone. It was first released on November 10, 2016. This new technology could be considered as a privacy breaker where it could invade other people's privacy without realizing it. Snapchat offered an easy way to capture photos or videos, without the knowledge of the person who's being captured. In the United Kingdom's law taking pictures of people without their consent is likely to be a breach of privacy law. Where before taking pictures/videos the person has to have permission from the government first ("Photography and Law", Para. 2). These new glasses seem a bit risky due to the possibility that people can use them in an inappropriate way that could embarrass others. For example, the user might abuse others by wearing the spectacles in a public washroom and captures some careless videos that could harm them. Even though these spectacles could be used in a disrespectful way, at the same time it could be used in a useful way. For example, instead of holding the phone and

taking a snap without focusing on the moment these spectacles would help the person to concentrate and picture the moment without wasting time. Regarding this, these spectacles are useful, but at the same time, it could threaten people's privacy through taking snaps without their knowledge as there are people that have no respect for others privacy.

- **Security**

Security is one of the things that many people are concerned about when dealing with an application. Did you know that many data and information on the internet are accessible to the public, unless it is encrypted in a very complex way? Security can be affected by external and internal factors, including the way the code is designed or the trustworthiness of the authorized employees. Hence, security has its downsides and upsides; when you have more security, you are restricting the potential usage of the application. While less security means more risks of cyber-attacks, though it might provide more comfort to the user. This raises a question regarding Snapchat's security, can we trust Snapchat developers with our information? And to what extent is our data secured?

At the end of 2013, around 4.6 million Snapchat accounts, including users' names and phone numbers were uploaded online by a hacker. Prior to this, Gibson Security, a well-known security company, warned Snapchat about a possible breach that could allow hackers to have access to the user's information. However, Snapchat developers did not do anything regarding this matter, and as a result, the hacker took advantage of this and published the data. Gibson security pointed out about the Application Program Interface (API) that Snapchat uses and how it is still vulnerable to any future attacks (Fung, 2014). API is a software that acts like a messenger that provides the requested data asked by you from the server; it is a way of communication within an application or between the operating system and applications (Eising, 2017).

Also, a couple of phishing attacks happened between 2017 and 2018 attempting to obtain a user's sensitive information, and they succeeded in getting 50,000 Snapchat accounts information (Newton, 2018). For example, a real issue happened here in Doha, Qatar. Where a hacker was able to access to a female's Snapchat account, access her messages and private photos that were saved in her Snapchat memory. Then he posted it on his Instagram account. Since he got control of her account, in a nutshell, he was able to secretly get access to her friend's accounts by sending them fake links. It's important to take into consideration the different aspects of human identity and the fundamental cores of human rights, where in some cultures, traditions, and religions such actions are not acceptable nor tolerated to be shared publicly. Although privacy is not a fundamental right, it is important to protect people from harm.

Considering the factor of trust, what if the employees of Snapchat are not trustworthy; can we users trust them with our data? Who is authorized to view this data? When you think about it, security is not only a technical issue but a moral issue too. It is unethical to spy on people and use your privileges to access confidential data. Unfortunately, Snapchat admitted that some employees used special tools that allowed them to get specific data from specified users, which is something against their policy (Ellingson, 2016). Since some of these employees might be engineers, then they are also violating their engineering code of ethics, which requires engineers to make a clear distinction between their personal interests and their professional duties ("Code of Ethics", n.d).

Furthermore, what is more interesting is that there is a surprising number of tweak applications like Phantom, Snapsave, and Snapchat ++ and many others (Dawson, Kim, Lee & Shen, 2016). These applications look like a modified Snapchat where it allows you to secretly screenshot the sender's picture or saves his/her video, as well as giving you the complete freedom to customize your settings. In other words, the sender no longer knows about the screenshot (Perez,

2016). By using these apps, the receiver could view the snaps without the sender noticing that the snap was viewed. To support this, a security researcher, Jamie Sámchez; published an article showing people how Snapchat is considered to be an app full of vulnerabilities. He explained in detail how Snapchat could be used to create Denial of Service attacks (DoS) for iPhone users and make their devices crash and freeze(Sábado, 2014). In a DoS attack, the attackers send a huge number of messages from different machines asking the server at the same time to connect them to one specific account. This account can be chosen at random, or the attackers can deliberately attack a certain user, at which the denial of service occurs(Weisman, n.d) This concerns Snapchat because they clearly prohibit the use of these applications in their privacy policy. However, they are not stopping these applications; and they still exist under different names. Users are unaware of this issue and it's affecting Snapchat reputation. Snapchat also thinks about how people would react and let go of the application if they don't find a solution for it. This is why deleting Snapchat is a way out of all of these issues and complexity.

On the other hand, people say that Snapchat is a new company, and Snapchat developers are working on upgrading their level of security, enhancing their ability to resist cyber-attacks and still gaining trust from users by sticking to their policies (Panzarino, 2014), which can be shown by the dramatic increase of Snapchat active users that reached almost 200 million users early in the first quarter of 2019 (Richter, 2019). This is why many people argue that this is the way social media applications work. They say whether we like it or not, information needs to be stored in the application clouds to be used later for their marketing strategies and storing them is something inevitable (Ashley& Tuten, 2014). Especially, if you are not doing something illegal like drug dealing, promoting sexually explicit content, or crossing the community guidelines, then you are on the safe side. Reason being, that whatever you post or receive would be under government

surveillance. However, those people are forgetting about an important thing. Did they ask themselves, who sets the community guidelines? Community guidelines can be viewed from different perspectives, and what applies to me does not necessarily apply to you. As for security, Snapchat is improving their security level (Panzarino, 2014), but as users why do we put ourselves in a position where our information is dependent on the security of an application, including detailed information about our personal lives and any type of information that could be used against us. Let us take in consideration the breaches that happened earlier and the ones that could happen in the future. It's gradually becoming a trust issue; do we just rely on what they say to the news or should we trust Snapchat based on what we see.

The solutions that we can provide for Snapchat are endless, as Dr. Boutros pointed out that we cannot disable the features that are built in Snapchat, because these features makes it the way it is. Yet, what we can do is limit the number of messages that a user can receive in one minute to two hundred messages, in order to reduce the possibility of having a DoS attack. As a human being, no one can read more than two hundred messages in one minute or view an equal amount of snaps (J. Boutros, personal communication, June 25, 2019). Not to mention, we can give the people the option whether they would want their photos to be screenshotted and whenever someone screenshots or screen records their content, a black screen appears to them similar to what Netflix is doing; somehow like content protection. As demonstrated in Figure (1). Additionally, Snapchat is asking users to do two-factor authentications to provide a more secure platform.

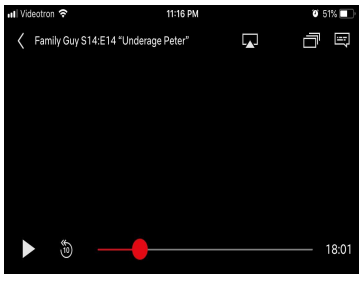

Figure (1)

Conclusion

Snapchat has a great popularity amongst the new applications that have been recently discovered, through sending instant photos and videos with the users. However, Snapchat faced a lot of privacy and security vulnerabilities since its creation in 2011. Privacy and security are important factors that most people are concerned about before using any application. With the huge privacy and security vulnerabilities that the company faced; through hacking, tracking the geo-locations and collecting personal information. Snapchat developers should protect these kinds of attacks by providing a more secure app by using encrypted ways of messaging and coding. People mainly concerns about the privacy policy agreement by Snapchat application, so awareness should be raised among people to sustain their privacy. This can be done by reading the terms and conditions policies, looking at how much information is revealed and the way engineers provide security in such applications. In addition, reading the privacy agreement would show how these policies not only impact negatively on people and society in general but also, on the company itself. When creating an application, we have to take into consideration the different cultures and aspects to create an application that does not necessarily fit all societies, but creates a major satisfaction among people. Moreover, as engineers, we should follow the code of ethics in our work to ensure that the project is ethical and retaining people rights by creating built-in features that contain encrypted codes that would increase user's privacy.

References:

Ashley, C., & Tuten, T. (2015). Creative Strategies in Social Media Marketing: An Exploratory Study of Branded Social Content and Consumer Engagement. *Psychology & Marketing*, *32*(1), 15–27. Retrieved June 26, 2019, from https://doi-org.srv-proxy2.library.tamu.edu/10.1002/mar.20761

Boutros, J. (2019, June 25). Personal Interview.

"Code of Ethics." *Code of Ethics | National Society of Professional Engineers*, www.nspe.org/resources/ethics/code-ethics.

Defossez, D. (2014). The Privacy of Snapchat. Retrieved June 23, 2019, from http://www.cs.tufts.edu/comp/116/archive/fall2014/ddefossez.pdf

Edwards, J. (2014, November 19). *Here Is Everything Snapchat Knows About You.* Retrieved June 26, 2019, from https://www.businessinsider.com/snapchat-user-data-2014-11

Eising, Perry. "What Exactly IS an API? - Perry Eising."*Medium*, Medium, 7 Dec. 2017, Retrieved July 3, 2019 from https://medium.com/@perrysetgo/what-exactly-is-an-api-69f36968a41f

(Ellingson, Annlee). Retrieved June 24, 2019, from https://www.bizjournals.com/losangeles/news/2016/02/29/snapchat-admits-employee-data-breach.html

French, S. (2015, November 2). *Snapchat's New 'Scary' Privacy Policy has Left Users Outraged*. Retrieved June 25, 2019, from https://www.marketwatch.com/story/snapchats-new-scary-privacy-policy-has-left-users-outraged-2015-10-29

Fung, B. (2014, January 01). A Snapchat security breach affects 4.6 million users. Did Snapchat drag its feet on a fix? Retrieved June 26, 2019 from https://www.washingtonpost.com/news/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/?noredirect=on&utm_term=.3d3d14743a37

Godlewski, N. (2018, May 9). *WHAT'S IN THOSE NEW PRIVACY POLICIES FROM COMPANIES LIKE INSTAGRAM, LINKEDIN?*. Retrieved June 27, 2019, from https://www.newsweek.com/privacy-policy-terms-service-new-what-it-means-916103

How to use Snapchat to DoS attack any iPhone. (n.d.). Retrieved June 24, 2019, from https://www.seguridadofensiva.com/2014/02/how-to-use-snapchat-to-dos-attack-your.html

Jamie. (2018, July 5). *Do Instagram and Snapchat work in China?*. Retrieved June 28, 2019, from https://www.techjunkie.com/instagram-snapchat-china/

Lekach, S., & Lekach, S. (2016, November 16). Privacy Panic? Snapchat Spectacles raise eyebrows. Retrieved June 25, 2019 from https://mashable.com/2016/11/16/snapchat-spectacles-privacy-safety/

Leetaru, K. (2018, December 15). What Does It Mean For Social Media Platforms To "Sell" Our Data? Retrieved July 8, 2019, from https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/#7cdfe43b2d6c

M. D., H. K., W. L., & K. S. (n.d.). Security Analysis of Snapchat. Retrieved June 22, 2019 from https://courses.csail.mit.edu/6.857/2016/files/11.pdf

Newton, C. (2018, February 16). A phishing attack scored credentials for more than 50,000 Snapchat users. Retrieved June 25, 2019, from https://www.theverge.com/2018/2/16/17017078/snapchat-phishing-attack-klkviral-dominican-republic

Panzarino, M., & Panzarino, M. (2014, January 02). Snapchat Says It's Improving Its App, Service To Prevent Future User Data Leaks. Retrieved June 22, 2019, from https://techcrunch.com/2014/01/02/snapchat-says-its-improving-its-app-service-to-prevent-future-leaks/

Perez, S. "Extensify Lets You 'Tweak' Your IOS Apps without Jailbreaking." *TechCrunch*, TechCrunch, 1 Mar. 2016, Retrieved June 25, 2019, from https://techcrunch.com/2016/03/01/extensify-lets-you-tweak-your-ios-apps-without-jailbreaking/

Richter, F., & Richter, F. (n.d.). Infographic: Snapchat Returns to (Modest) Growth. Retrieved June 23, 2019, from https://www.statista.com/chart/7951/snapchat-user-growth/

Ramirez, E., Brill, J., Ohlhausen, M. K., Wright, J. D., & McSweeny, T. (n.d.). UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION. Retrieved June 18, 2019, from https://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf

Sloane, G. (2017, November 1). *SNAPCHAT FINALLY LETS ADVERTISERS USE PIXELS TO TRACK AD RESULTS AND EVENTUALLY RETARGET*. Retrieved June 25, 2019, from https://adage.com/article/digital/snapchat-advertisers-pixel-tracking-tool-target-ads/311129

S. S. (n.d.). Privacy vs. security: What's the difference? Retrieved June 22, 2019, from https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html

Stewart, R. (2017, November 1). *More sophisticated targeting is coming to Snapchat as app embraces pixel tracking*. Retrieved June 26, 2019, from https://www.thedrum.com/news/2017/11/01/more-sophisticated-targeting-coming-snapchat-app-embraces-pixel-tracking

Snapchat Support. Retrieved June 25, 2019, from

https://support.snapchat.com/en-US/a/snap-map-faq

Top 5 Snapchat Security Vulnerabilities. (2016, February 23). Retrieved June 27, 2019, from https://resources.infosecinstitute.com/top-5-snapchat-security-vulnerabilities-how-the-app-learned-its-lessons/#gref

"What Are Denial of Service (DoS) Attacks? DoS Attacks Explained." *Official Site*, Retrieved June 28, 2019, from https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html

Walkley, R. M. (2018). Photography and the Law in the UK. Retrieved July 2, 2019, from http://photo.ballandia.co.uk/wp-content/uploads/2018/07/Photography-and-the-Law-in-the-UK.pdf