5-2022

TERMS OF SERVICE AGREEMENT CONTRACTS: AN OVERVIEW OF PERSONAL RISK MANAGEMENT AND RECOMMENDATIONS FOR ENHANCING USER AWARENESS

Brenda Collazo Taylor
California State University - San Bernardino

TERMS OF SERVICE AGREEMENT CONTRACTS: AN OVERVIEW OF PERSONAL RISK MANAGEMENT AND RECOMMENDATIONS FOR ENHANCING USER AWARENESS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology

---

by

Brenda C. Taylor

May 2022

TERMS OF SERVICE AGREEMENT CONTRACTS: AN OVERVIEW OF PERSONAL RISK MANAGEMENT AND RECOMMENDATIONS FOR ENHANCING USER AWARENESS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Brenda C. Taylor

May 2022

Approved by:

Dr.Conrad Shayo, Committee Member, Chair

Dr. Conrad Shayo, Committee Member, Reader

Dr. Jay Varzandeh, Committee Member, Chair IDS Department

ABSTRACT

This cumulative project will explore the personal risks involved when a user agrees to an online service's Terms of Service (TOS) Agreement contract, especially when a user checks the "I Agree" box on an online service's TOS. The key questions were: (1) What are the personal risks involved when a user clicks on the "I Agree" box on an online service TOS Agreement? (2) How are these risks co-related? and (3) How can end users mitigate risks after they have agreed to the TOS? To answer the questions, various TOS agreements were reviewed, and a poll was conducted asking a small sample of students and IT professionals if they read the TOS terms of their online social networks. Additionally, to answer how a user can mitigate risks after they have agreed to terms, a test was made over a five-month period pertaining to web browser tracking. Research suggests that there is a lack of transparency pertaining to data protection, user tracking, data ownership and data sharing on the online services' behalf. The conclusion is that people can mitigate those risks by doing the following: (a) reading the TOS Agreement prior to giving their consent and agreeing to the TOS, (b) limit the data that is shared, (c) opt-out of data tracking if possible. Areas for further research include a comparative study on tracking prevention among various web browsers, and a behavioral study to examine why users choose to ignore the TOS agreements.

ACKNOWLEDGEMENTS

Thank you to Dr. Shayo and Dr. Son for your constant guidance and support. Thank you for encouraging me to pursue my graduate degree, and for the abundance of knowledge that you supply every student that enters this program. Thank you Dr. Tapie Rohm for igniting my passion for this field when I began my undergraduate degree, I think of you fondly and I constantly reflect on your words of inspiration. You motivated your students to never give up and persist, regardless of what life lays on this journey that we are on, God Bless you and thank you.

DEDICATION

My deepest gratitude is to my best friend, husband, and peer. Thank you for your support, your love, and for this beautiful life that we have built together. I am incredibly proud of you and for all that you have achieved here at CSUSB. You possess determination and strength that is unwavering and admirable. I also dedicate this to my parents for their support and devotion; thank you for all of your hard work that does not go unnoticed. Lastly, I want to dedicate this to my daughters who make life beautiful beyond measure, you are my greatest achievement and my pillars of ceaseless inspiration.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE:

INTRODUCTION

People agree to legal contracts every day. One of the most common legal contracts that people agree to, and sign virtually are the Terms of Service (TOS) Agreements associated with online services. During the lockdowns of 2020, people's work and social lives transitioned to the virtual world more so than before. People began to use additional online services for work such as Zoom and Google, as well as an increase in online services for socialization such as Snapchat, Instagram, and Pinterest. When a person uses one of these online services, they agree to the TOS to be granted the privilege to use the service. TOS agreements are standard, and businesses compose the TOS to educate the customer about the rules in place prior to their use of a product or service. The TOS also contains the legal protection that the service and company have.

TOS agreements vary depending on the business and the types of services they provide. TOS Agreements explain what the company deems acceptable and unacceptable, it outlines content ownership, arbitration rights, as well as information on how a user's data and information is collected, stored, shared, or sold. It is important for a user to understand the TOS when they select the "*I Agree*" checkbox whilst interacting with an online service. At times, people may feel pressured to agree to these terms due to the necessity to use a specific product or online service. This project will explore the personal risks that a user

may incur when s/he agrees to the TOS Agreement. Some users may tend to overlook the personal risks involved when they make the swift decision to select the “I Agree” box.

To understand the personal risks involved when a user agrees to the TOS Agreement, it is imperative to read, analyze, and ask questions regarding these service agreement contracts and how they will affect the user in the future. This culminating experience project focuses on educating users of the personal risks involved when they agree to an online service’s TOS agreement contract. In this project the term TOS will be used to stand for Terms of Use (TOU), or User Contract as online services use either term when they present the TOS or TOU or User Contract agreements. To create a plan on the best tools and processes that a user can implement to protect themselves from TOS Agreement risks, we must answer the following three questions:

1. What are the personal risks involved when a user clicks on the “I Agree” box on an online service TOS Agreements?
2. How are these risks co-related?
3. How can end users mitigate risks after they have agreed to a TOS?

This project will explain the user’s risks associated with agreeing to Term of Service Agreements, such as granting consent for online services to collect your personal data. Furthermore, a correlation between the individual risks will be

analyzed to understand how a user's personal data is used and shared by the online service. Lastly, this project will detail what tools and actions a user may take to mitigate these risks.

Organization of the Project

This project will be organized as follows: Chapter 2 will provide background information on what a TOS is and how to properly read the document(s). Chapter 3 will provide analysis of personal risks involved in TOS agreements. Chapter 4 will provide risk management solutions and user awareness findings which include poll results conducted in a small sample of student peers and IT professionals, and test results obtained from a test that I conducted to mitigate my tracking on Microsoft Edge. Lastly, Chapter 5 will provide a discussion and will provide areas that require further research.

CHAPTER TWO:

UNDERSTANDING TERMS OF SERVICE AGREEMENTS

A Term of Service (TOS) agreement, or a Term of Use (TOU) agreement is an agreement that a user agrees to, and abides by, to use a website or an online service. This agreement includes terms related to third-party websites, content ownership, copyright notices, payments, and additional information (upcousel.com, 2020). It is essential to understand that the TOS is important for both businesses and individual users, as it is a legally binding agreement between the two parties. The first important detail to understand is that signing an online contract is no different than signing a physical copy, therefore a user should perform their due diligence in safeguarding their rights and read the TOS. TOS agreements tend to be hidden, written in small print, and service providers tend to post the contract on the website via a hyperlink at the bottom of the screen below the large “I Agree” button. Additionally, due to the length of these documents, it is far easier for a user to ignore reading the contract and click on the “I Agree” box or button without due diligence.

A Business Insider article shed light that over 91 percent of consumers accept legal terms and conditions without reading them, for younger people ages 18-34 the rate increased to 97 percent agreeing to the conditions without reading the TOS Agreement or Terms of Use (Cakebread, 2017). These numbers could be considered alarming, and it is imperative to understand why users may

choose to agree to terms they have not read because these legal contracts are legally binding. Courts routinely impose these contracts onto the user, and they are responsible for reading these terms. Although the user is responsible for reading the terms, the opposite party (online service) does not have the duty to draft contracts and terms that are readable and understandable to the average user. According to Becher and Benoliel (2019), “in fact, when the contract is unreadable, the duty imposed on consumers to read the illegible contract becomes unfair” (ibid., p. 2262). Furthermore, this has raised fairness concerns, and scholars have suggested that these contracts are indeed written in a manner that dissuades a user from reading them (Becher and Benoliel, 2019).

The TOS is only accessible by clicking on hyperlinks which leads the user to another page(s), and yet again there are more hyperlinks for the additional terms such as the Cookie Policy, Privacy Policy and so on. Companies have legal teams on retainer and use them to write TOS Agreements, Privacy Policies, Acceptable User Policy, and Cookie Policies. In turn, for the general public the contracts and policies may seem daunting to read as they are full of legal terms and jargon that the general public fails to understand (Becher and Benoliel, 2019). The TOS can range between 20-60 pages and is updated at least once a year. For example, Amazon.com TOS is 18 pages, Walmart is 35, and AT&T’s TOS is roughly 60 pages. A user would need a college-level degree to understand the TOS Agreement and would take 244 hours a year for a typical American internet user to read the privacy policies of all the websites he or she

visits (Schaub, 2017, p. 4). In addition, it should be noted that this number must be augmented to include all the applications that a user installs on their mobile devices, as well as the new cloud services that a typical consumer now uses such as Microsoft One Drive and Google Cloud.

Readability of Terms of Service Agreements

Becher and Benoliel, (2019), applied well-establish linguistic readability tests to the five hundred most popular websites in the United State that use “sign-in-wrap” agreements, i.e., the contract that a user must sign when signing up for websites such as Facebook, Amazon, Uber, and Airbnb. The source of data was the Alexa Top Sites web service which ranks the list of the most popular website in the United States. A Summary of this data, collected in September 2018 is shown in Table 1.

Table 1. Becher and Benoliel Study (September 2018 Web Traffic)

	Mean	Median	Standard Deviation
Unique Visitors	10,169,272	7,860,347	11,246,053
Pageviews	203,202,295	55,643,205	1,446,362,157

The examination was conducted via two different readability tests that are often used together in empirical readability studies: (1) the Flesch Reading Ease (FRE) test, and (2) the Flesch-Kincaid (F-K) test. The recommended FRE score for consumer-related information should be 60 or higher, whereas a FRE score lower than 60 means that the text is not understandable by consumers. The median FRE score in Becher and Benoliel sample is 34.20 and the mean FRE score is 34.86. Almost all the sign-in wrap agreements in this study's sample (498 out of 500, or 99.6%) received an FRE score that is lower than the recommended score of 60. Likewise, the recommended F-K score for consumer-oriented materials is 8.0 (meaning eight-grade reading level), the median F-K score in this study's sample is 14.9, and the mean F-K score is 14.67. It should be noted that in keeping with this recommendation more agencies are recommending that material be written at or below an eight-grade reading level, for example, many state insurance regulators require insurance contracts to be written at or below an eight-grade reading level, the U.S. Department of Education recommends that health-related information be written at or below an eight-grade reading level, and the Food and Drug Administration and the National Institutes of Health recommend designing consent forms at or below an eight-grade reading level (p.2275). Under the F-K test, 99.6% of the contracts in Becher and Benoliel's study sample are unlikely to be understood by consumers. TOS terms are not only difficult to understand, but they are inescapable as many TOS agreements are necessary for applications and online services.

Furthermore, failing to understand and read what a user has agreed and consented leads to more concerns that will be explored. Due to this user misjudgment in agreeing to terms they do not read or simply do not understand; the underbelly of the TOS Agreements is riddled with terms that violate user's privacy and rights.

Continued Growth in Applications and Online Services

In 2021 there was a boom in every application. For example, financial apps grew by 31 percent, with newer apps seeing the most increase (Nelli, 2022). Nelli (2022) describes the negative outcomes when a consumer does not read the terms of conditions. For example, 80 percent of consumers do not know that fintech apps use third-party providers for collecting and storing their financial data, the consumer does not have a relationship with these data aggregators, and most do not know that they exist (p.6). In addition, even fewer consumers know that these data aggregators can sell their data for a variety of purposes. A single data aggregator stores banking data from 25 percent of U.S (United States) banks combined. Seventy-three (73%) of users do not know that these apps have access to their banking account username and password, yet remarkably the same percentage of users are confident that their data is secure. Undoubtedly there is a disconnect between what a consumer thinks they know, and what they actually know about who can access their data and how it is collected, stored, and shared.

The TOS agreements are written by highly skilled legal teams, which results in a TOS that most people do not fully understand or comprehend. Most people would say that they, “I don’t think anyone reads them,” and that “Why would I read them?” (Pulvermacher, 2021). The general public suffers when they sign a legal clause that they simply cannot comprehend, because included in the TOS are forced arbitration clauses that are legally binding. Koenig & Rustad (2014) examined the TOS of 329 of the world’s largest social media providers. This examination determined that 29% of the 329 social media providers require users to submit to predispute mandatory arbitrations as a condition of using their service. The TOS examination also suggest that forced consumer arbitration clauses are mostly a “U.S. (United States) phenomenon,” as 42% of the 188 U.S.-based social media providers contain forced arbitration clauses, whereas 13% of the 141 providers headquartered in foreign nations included these forced arbitration clauses in their TOS. “Mandatory arbitration, under the one-sided terms specified by most social networking TOS, efficiently and effectively eliminates liability” (p. 373). Given the potential impact that forced clauses in TOS agreements have on a user, taking the time to study what is in the terms may be beneficial to the user as there are additional personal risks associated with TOS agreements. Chapter 3 will discuss the personal risks that a user incurs when they agree to a TOS next.

CHAPTER THREE:

ANALYSIS OF PERSONAL RISKS INVOLVED IN TERMS OF SERVICE AGREEMENTS

Chapter 2 discussed the definition of what a TOS is, how accessible TOS contracts are to the user, and other caveats that are hidden within these contracts. This chapter further demonstrates how to identify the personal risks associated with these contracts, which may potentially lead a user into a vulnerable position. This chapter will also present these risks in a simplistic manner, so that a user may have a guide which may help them identify these personal risks and what they can do to mitigate the risks. Below, a TOS Risk Taxonomy Analysis Table (See Table 2) is presented identifying four major areas of concern regarding TOS agreements: (A) Arbitration Clauses, (B) Privacy Concerns, (C) User Data Ownership, and (D) Third-Party Affiliates (Becher and Benoliel, 2019, p. 2266).

How to Effectively Read the Terms of Service Agreement

Terms of Service Risk Taxonomy and Bloom's Taxonomy

In the previous chapter this work discussed literature and research that supported readability concerns associated with a TOS. Even though these

contracts are difficult to comprehend, there are tools that can assist the user to make a better decision when deliberating the terms. The user can use the TOS Risk Taxonomy Analysis Table below (See Table 2) in addition to Bloom's Taxonomy (See Figure 1), so that they may reflect on the TOS agreement and make informed decisions on whether they should click on "I Agree" box and consent to the terms presented by an online service or application. Table 2 will help a user to: recall their knowledge pertaining to contractual information, analyze the personal risk patterns in the contracts, and evaluate the outcomes. Bloom's Taxonomy may be used after the user has read the TOS, users can reflect on the six levels of reasoning and reflect on their understanding of the TOS. Furthermore, the user can self-assess to determine if they can identify any personal risks in the TOS. These two resources can help a user to review what they have read in the TOS and decide whether to agree or not agree to the TOS based on logic.

Table 2. TOS Risk Taxonomy Analysis (Taylor, 2022).

TOS Agreement Risk Taxonomy Analysis	
A. **Arbitration Clauses**	
User Concern	Key Points: 1. Forced Arbitration Clauses
B. **Privacy Concerns**	

User Concern	Key Points: 1. User Privacy Violations 2. Child Privacy 3. User Tracking
C. **User Data Ownership**	
User Concern	Key Points: 1. Who is the data owner? 2. How long is this data stored?
D. **Third-Party Affiliates**	
User Concern	Key Points: 1. User Data Collection 2. User Data Sharing Violations 3. User Data Confidentiality and Integrity

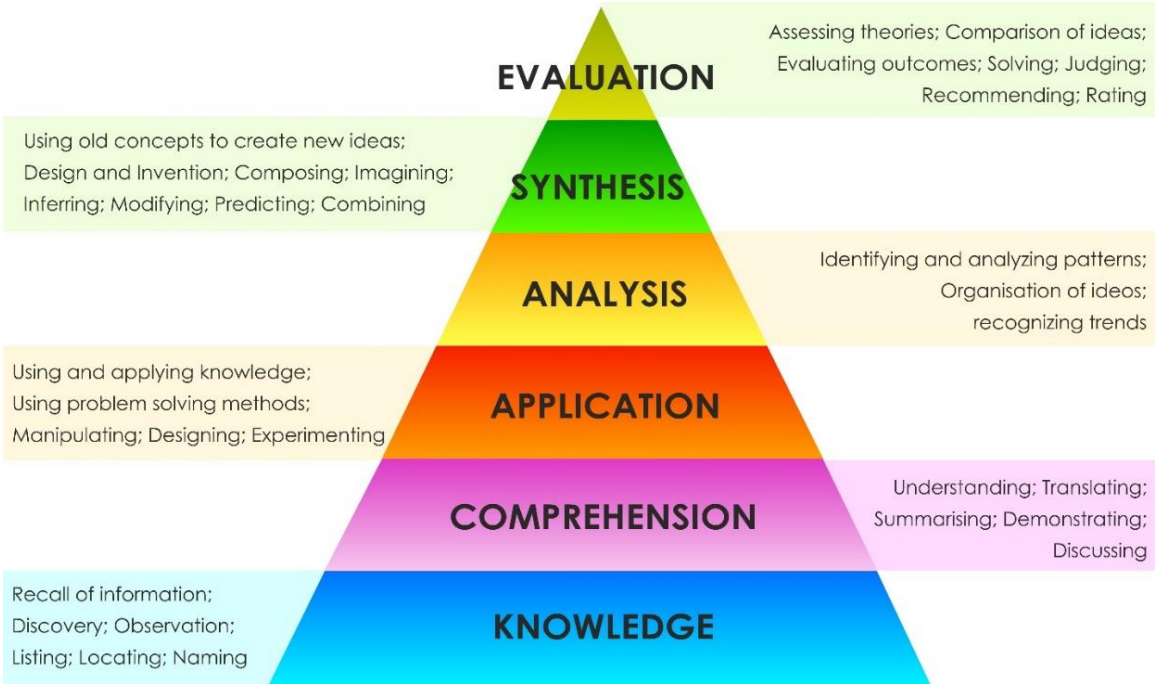

Figure 1. Bloom's Taxonomy (1956).

To assist the user in making cognitive and educated decisions when determining whether they should agree to the TOS, Bloom's Taxonomy can be used during the decision-making process. For example, (1) Knowledge: recalling the TOS facts, the length of the contract, observation on the legal terms, (2) Comprehension: the understanding and apprehension of the TOS, comprehension of the legal terms used, understanding the terms outlined, summarizing the TOS characteristics, (3) Application: correct use of the facts, rules or ideas, and applying the acquired knowledge by reading the TOS and identify connections in the terms, (4) Analysis: breaking down information provided in the TOS into constituent elements or parts such that the relative hierarchy of ideas is made clear and/or the relations between ideas expressed are made explicit, (5) Synthesis: combining the facts, ideas, or information to make meaning about the TOS, (6) Evaluation: judging or forming an opinion about the TOS material, and making a judgement about the information that was presented in the TOS. The TOS Risk Taxonomy Analysis Table along with Bloom's Taxonomy can assist users when reading the TOS agreement, because they will be able to evaluate the terms and determine if the pros of agreeing to the terms outweigh the personal cons affiliated with the TOS. With a foundation regarding what a TOS is and how a user can apply this project's TOS Risk Taxonomy Analysis Table along with Bloom's Taxonomy, the user can review a TOS and Privacy Policy and identify personal risks. This project will now discuss

violations in TOS agreements based on the four categories: arbitration clauses, privacy concerns, user data ownership, and third-party affiliates (Table 2).

Four Areas of Personal Risks in Terms of Service Agreements

Forced Arbitration Clauses

The first personal risk that is identified in a TOS is the incorporated mandatory arbitration clauses. An arbitration clause is when a user agrees to settle out of court, through arbitration cases, any dispute that arises with your counterpart (Shonk, 2022). Through forced arbitration clauses, the TOS are depriving users of their rights to civil recourse against providers who violate their privacy. Social networking sites (SNS) require a user to agree to the TOS Agreements and Privacy Policy before they can use that SNS and require the user to agree to predispute mandatory arbitration as a condition of joining their SNS. For example, consumers that enter clickwrap or browsewrap TOS agreements waive their right to a jury trial, discovery, and appeal, without reasonable notice that they are waiving these important rights (Buckingham et el.) As stated previously, forced arbitration clauses are principally a U.S. phenomenon, therefore we should examine why this is the case.

Koenig and Rustad (2014) performed a systematic examination of 329 of the world's largest social media providers. Their study demonstrated that 42% of the 188 U.S.-based social media providers contained forced arbitration clauses.

Forty percent (40%) of the social networking websites (SNS) specify the American Arbitration Associate (AAA) as the provider and 19% specify Judicial Arbitration and Mediation Services, Inc (JAMS). AAA and JAMS are the two largest arbitration companies in the United States (Koenig &Rustad, 2014). Koenig and Rustad compared the fifty-nine social media Terms of Use (TOU) against the due process fairness tests adopted by the AAA and JAMS. The findings demonstrate the arbitration clauses of providers that specify the AAA and JAMS fail the majority of the provisions of these two arbitral providers' consumer due process fairness tests. These forced clauses also have provisions such as hard damage caps that place an absolute dollar limit on recovery that is significantly below the cost of filing an arbitral claim with either the AAA or JAMS. This means that if a consumer is willing to file a claim there may be caps on the dollar amount for which the SNS is mandated to pay out, and this dollar amount can even be significantly less than the cost of filing a claim.

The social media service Snapchat has made headlines due to their forced arbitration clauses as well as the notable cyberattack on January 1, 2014, which resulted in 4.6 million Snapchat usernames and redacted phone numbers on a website. As a result, the Federal Trade Commission (FTC) entered a settlement with Snapchat because of security negligence and false misrepresentations on their Terms of Service. Since users agreed to Snapchat's TOS, there was no remedy to compensate the user for the fraudulent mis-representations and their negligent security as Snapchat's Terms of Service state

that if the social media site “is found liable to you for any damage or loss which arises out of or is in any way connected with your use of the Services or any content, Snapchat’s liability shall in no even exceed $1.00” (Snapchat TOS, 2021). Forced arbitration clauses such as these are written to protect the company and in essence allow them to be in a liability-free zone which leaves the consumers powerless if their data is stolen by malicious actors. Snapchat’s TOS agreement also states, “You and Snap agree that disputes between us will be resolve by mandatory binding arbitration, and you and Snap waive any right to participate in a class-action lawsuit or class-wide arbitration,” this means that the users as a group with the same or similar grievance are unable to join and file a lawsuit (Snapchat TOS, 2021). Unfortunately, once a user clicks on the “I Agree” box they are relinquishing far too many rights. Forced arbitration clauses are a risk that corelates with the next risk that was outlined in our TOS Risk Taxonomy Analysis in Table 2, under the sub-heading Privacy Concerns.

Privacy Concerns

Online services and social media companies have made false claims in the past regarding user privacy, and there have been more headlines in recent years that have been brought to the forefront. As users who daily interact with online services social networking sites, a great deal of information is shared such as our names, date of birth, telephone number, address, email address, photos, and videos. Users assume that online services will protect their data when they

agreed to the Privacy Policy contract, because when we read the word “Privacy” we assume that this policy pertains to how our data is protected and secured by the online service. But term “Privacy Policy” has taken a new meaning in the marketplace, as “privacy policies simply inform consumers that unless they “opt out” of sharing certain information, the company will communicate their personal information to other commercial entities” (Good et al., 2007).

The federal government—specifically the Federal Trade Commission (FTC), an independent agency charged with protecting American consumers—has played a crucial role in regulating the collection and use of consumer data online (Hans, 2012). In 2019, US lawmakers and regulatory agencies began to direct at tech firms the kind of criticism that has been advancing in the European Union for years (Paul, 2019, p16). As the average American became more aware of the privacy issues and the magnitude of data collection, calls for legislation intensified, said Hayley Tsukayama, a legislative activist at the not-for-profit Electronic Frontier Foundation (Paul, 2019, p.18). The increased pressures from legislation on tech firms are due to the General Data Protection Regulation (GDPR) that went into effect in May 2018, legislation such as this is a step forward for protecting user privacy and data concerns.

For example, privacy concerns that users of Snapchat experienced, were when Snapchat made false claims in their TOS that photos and videos shared by their users disappear after they have been viewed (FTC, 2014). After the New Year’s Eve cyberattack, the Federal Trade Commission fined Snapchat in 2014,

for not only negligent security but for additional false information such as falsely claiming that messages are truly disappearing in the TOS. The users were under the impression that once they posted a photo or video, the content would disappear from their story within 10 seconds of being viewed (Snapchat, 2013). This was false and it has now been included in the TOS to reflect that Snapchat does in fact save all your data including photos and videos. In addition to those false claims, the company misrepresented its data collection practices. The company transmitted geolocation information from users of its Android application, despite stating in its Privacy Policy that it did not track or access such information. Alongside Snapchat, Facebook has also been fined by the FTC for violating consumer privacy (FTC, 2019).

On July 24, 2019, the FTC imposed a $5 Billion penalty on Facebook, “Despite repeated promises to its billions of users worldwide that they could control how their personal information is shared, Facebook undermined consumers’ choices,” said FTC Chairman Joe Simons (FTC, 2019). The FTC investigation findings were presented at an in-person press conference at FTC headquarters, by FTC Chairman Joe Simmons, FTC Commissioners Noah Joshua Phillips and Christine S. Wilson, and Gustav W. Eyler, Director of the Department of Justice Civil Division’s Consumer Protection Branch. Facebook monetized user information through targeted advertising. This resulted in $55.8 billion in revenues in 2018. To encourage users to share information on its platform, Facebook promises users they can control the privacy of their

information through Facebook's privacy settings. Facebook users who installed an app ("App User") agreed to Facebook sharing with the third-party developer of the installed app both information about the App User and the App User's Facebook Friends ("Affected Friends"). The default settings on Facebook were set so that Facebook would share with the third-party developer of an App User's app not only the App User's data, but also data of the App User's Facebook Friends, even though the Affected Friends had not themselves installed the app (FTC, 2019). During a yearlong investigation by the FTC, it was determined that once the third-party developer received the data, they would target advertisements to the App Users and Affected Friends. While under investigation, Facebook included a disclaimer to the Privacy Settings warning users that the information they shared with their Facebook Friends would also be shared with the apps those Friends used. Four months after the 2012 Order was finalized, Facebook removed this disclaimer whilst still sharing the user data with the third-party developers (FTC, 2019). Facebook allowed millions of third-party developers to access and collect massive amounts of consumer data and failed to track the data in an organized and systematic manner. This investigation was eye opening for Facebook users, because users trusted the social networking site (SNS) to be transparent on how it was collecting, sharing, and protecting their data.

This event gave users an insight into the vast amounts of data that online services and social networking sites gather from the user and how it is shared to

third-party affiliations. Privacy Policies began to state what data was being collected from the user, but as stated before these policies are hidden within each other and only accessible if the user selects the underlined hyperlink in the TOS that simply states, "Privacy Policy." If the user does not click on this link, they will not be able to view the contract. There is still a need to improve the accessibility of these terms as Personal Identifiable Information (PII) is collected in vast amounts. As discussed previously, when a user agrees to the TOS, they are inherently forced into arbitration clauses which leave them vulnerable in the event of a cyberattack. As a result of these forced arbitration clauses and loopholes in the TOS, the users may not be compensated if their personal information is stolen by an attacker. Depending on the TOS agreement, the user's personal information may potentially be accessed by malicious attackers due to negligent security measures. These risks are correlated as forced arbitration clauses protect the company and not the users, therefore in the event of a cyberattack the users' data is vulnerable, and no user is able to take lawsuit action against the company.

The last privacy risk that will be discussed is Child Privacy concerns. TOS agreements and Privacy Policies are also signed by minors, as more minors are given smartphones at an early age. These children can download applications and create accounts in applications without their parents' consent. Snapchat's TOS is written as follows: "No one under 13 is allowed to create and account or use the Services. If you are under 18, you may only use the Service with the prior

consent of your parent or legal guardian. Please be sure your parent or legal guardian has reviewed and discussed these Terms with you before you start using the Services." This short and brief statement is aimed for minors to "please" have the parents or guardian "discuss these terms with them," yet there is no way for Snapchat to know for certain that a parent or legal guardian was made aware of these terms. This type of verbiage is inserted in the TOS Agreements to protect the company, as they assume that minors will have their parents explain what this legal contract means. This is placing a lot of faith in minors and frankly it is incomprehensible to trust that a child is or is not agreeing to contractual agreements will full parental consent.

In September 2019, the Federal Trade Commission and the New York Attorney General fined Google and YouTube $170 million for alleged violations of the Children's Online Privacy Protection Act (COPPA) Rule by illegally collecting personal information from children without their parent's consent (FTC, 2019). Google LLC and YouTube LLC will pay $136 million to the FTC and $34 million to New York, which marks the largest amount the FTC has obtained regarding a COPPA case since the rule enactment in 1998. YouTube earned millions of dollars by using the identifiers, commonly known as cookies, to deliver targeted ads to viewers of these channels, according to the complaint (FTC, 2019). The COPPA Rule requires that child-directed websites and online services such as Google and YouTube, provide notice of their information practices and obtain parental consent prior to collecting the personal information from children under

13 years of age which include identifiers (cookies) which track a user's Internet browsing habits for target advertising. Targeting ads to children without their parental knowledge and consent has been an ongoing issue. By imposing harsh penalties on child privacy laws violations, and with additional legislation governing big tech, children can be further protected in the internet world.

User Data Ownership

The next risks that will be discussed are significant, as stated in the previous section that children are now using online services and social networking sites more frequently. As users of online services, we have a false understanding that the data that we provide to the online services via the website or application is "legally ours" such as: our name, telephone number, username, email address, date of birth, photos, videos, and messages. Yet as stated in the TOS', the data that is uploaded by a user is collected, stored, and shared by the service. Therefore, a user should understand what data is collected and who owns and has the legal rights to their data.

For example, Snapchat's TOS Section 3 "Rights You Grant Us" states: "For all content you submit to the Services, you grant Snap and our affiliates a worldwide, royalty-free, sublicensable, and transferable license to host, store, cache, use, display, reproduce, modify, adapt, edit, publish, analyze, transmit, and distribute that content". This means that the user grants Snapchat the right to make their content available to, and pass these rights along to, service providers

with whom Snapchat has contractual relationships related to provision of the Service. By agreeing to these terms, the user grants Snapchat extensive licensing rights to the content that they posted. Unbeknownst to the user, by agreeing to the terms they have granted the online service or social networking site licensing rights to store and distribute their content. As users of services, we are under the impression that data that we “post” on our profiles is fully and completely “legally ours,” this is a huge misconception and false. For example, Snapchats TOS state:

> “You also grant Snap, our affiliates, other users of the Services, and our business partners an unrestricted, worldwide, royalty-free, irrevocable, and perpetual right and license to use the name, likeness, and voice, of anyone featured in your Public Content for commercial and non commercial purposes. This means, among other things, that you will not be entitled to any compensation if your content, videos, photos, sound recordings, musical compositions, name, likeness, or voice are used by us, our affiliates, users of the Services, or our business partners” (Snapchat, 2022).

Aside from granting online services and social networking sites rights to our content and data, an area for concern is that these companies can store this data for as long as they deem necessary. Pinterest is a visual “discovery engine for finding ideas like recipes, home and style inspiration, and more” (Pinterest,

2018). Users can create visual boards for various interests, as well as upload photos, videos, and blogs. Pinterest has a simple and brief statement on how long the user data is stored:

> "Following termination or deactivation of your account, or if you remove any User Content from Pinterest, we may keep your User Content for a reasonable period of time for backup, archival, or audit purposes. Pinterest and its users may retain and continue to use, store, display, reproduce, re-pin, modify, create derivative works, perform, and distribute any of your User Content that other users have stored or shared on Pinterest" (Pinterest, 2018).

Simply put, the user grants permission to Pinterest to use the content to "provide and improve Pinterest," even if you delete the content from your account and delete the account. The general user would be confused by the terms because this social platform does not clearly state how many weeks, months, or years they store the user's content. The lack of transparency in these types of terms will leave a user asking themselves the question, "How long exactly will my data be stored?" and there is no true answer to this question.

Additionally, the TOS by Snapchat state: "We store your basic account information — like your name, phone number, and email address — and list of friends until you ask us to delete them… Keep in mind that, while our systems are designed to carry out our deletion practices automatically, we cannot promise

that deletion will occur within a specific timeframe" (Terms of Use, Snapchat, 2021). Once again, there is no specified period on how many weeks, months or years Snapchat will store user data. This loophole written into the contracts does not guarantee users that their data will be deleted once they delete their account and stop using the service. If online services and social networking sites are not transparent with their users, there is a lack of trust by the user. The risks involved with Privacy Concerns corelate with Data Ownership, because once there is a lack of trust by a customer, that customer may search for an alternative online service and social networking site that is more transparent and honest.

Third-Party Affiliates

The last risks that will be discussed in this chapter are the risks pertaining to third-party affiliates. As mentioned earlier, online services and social networking sites share a lot of user data and personal information with third-party affiliates such as third-party data aggregators. Online services and social networking sites that users utilize also have contractual relationships with third parties. This means that user data is shared with these third parties for the purpose of the online service or social networking site to provide their "Service" to the consumer. As most users do not read the TOS Agreements, they are unaware that their data is shared with other companies, and possibly sold by these third parties to additional companies. It is a cycle of selling user data continuously, without the user's knowledge. A common theme in TOS

Agreements for various providers is that the user data is sold to third parties for the purpose of “personalizing advertising” to the consumer.

During the FTC investigation of Facebook, third-party developers that received user and Affected Friend information could use that information to enhance the in-app experience or target advertising to App Users and their Affected Friends. In the wrong hands, user and Affected Friend data could be used for identity theft, phishing, fraud, and other harmful purposes (FTC, 2019). Before strict regulations began to be implemented onto online services, agencies, and social networking sites, there may or may not have been a disclaimer available to the consumer regarding the relationship between the main party and third-party affiliates. It was up to the online service of social networking site to disclose this information to the users. Disclosing the third-party relationships between the service provider and the third parties should be included in all TOS Agreements; because as a user, if we do not know that these third parties exist then how are we to know whether our data is safe and in secure hands. Furthermore, when an online service or social networking site share user data with a third-party, they should know who gets access to log data on how this data is used. Also, service providers should be notified promptly if a cybersecurity incident or other adverse event occurs. Vida (2019), notes that a series of interconnected actions should be taken to ensure data is secure when being shared with third-party systems, including access control policies, deploying multifactor authentication, separating authentication from access

control and other best practices. Strict security policies must be included in the TOS Agreements to assure that data confidentiality and integrity is maintained by these third-party data aggregators. The following chapter will provide ways that a user can mitigate the risks described in this chapter.

CHAPTER FOUR:

RISK MANAGEMENT AND USER AWARENESS

FINDINGS RESULTS

In this chapter it shall be demonstrated how users can mitigate risks associated with TOS Agreements, as there are steps and efforts that a user may take to protect their information, data, privacy, and anonymity. To assist the user during the reflection period prior to clicking on the “I Accept” button, all personal risks should be taken into consideration to make a coherent judgement. For this project, I constructed the table below for users to utilize when considering the consequences before agreeing to a TOS Agreement. Table 3 presents personal questions pertaining to the four areas of concern: A) Arbitration Clauses, B) Privacy Concerns, C) User Data Ownership, and D) Third-Party Affiliates. Table 3 will allow the user to actively reflect on the terms they have read and consider the personal risks that have been described in this project. The user can ask themselves the questions presented in Table 3, as these are questions that we may not ask ourselves when considering TOS personal risks.

Table 3. Terms or Service Assessment Prior to Agreeing (Taylor, 2022).

TOS Assessment Prior to Agreeing

User Area of Concern		Are You Willing to Take the Risk?
A. Arbitration Clauses		Y or N
User Concern	Questions to Consider: 1. Forced Arbitration Clauses a. Am I willing to waive my arbitration rights? b. Am I willing to waive my right to participate in a class action suit? c. Am I willing to travel to the State where the headquarters are located to present my case?	
B. Privacy Concerns		Y or N
User Concern	Questions to Consider: 1. User Privacy Violations a. How do I feel if an online service monitors my private messages? b. How do I feel about online services saving all my photos in a database? 2. Child Privacy Violations a. How do I feel about my child signing TOS Agreements? 3. User Tracking a. How do I feel about an online service tracking my history on their website and private browsing? b. Is it ethical to be “tracked” by an online service?	
C. User Data Ownership		Y or N
User Concern	Questions to Consider: 1. Who is the data owner? a. Do I want to allow an online service to use my photos and video content to promote their service? b. Do I want to waive royalty rights over my content?	

	2. How long is my data stored by the online service? a. Am I comfortable knowing that my data will be stored indefinitely by the online service?	
D. Third-Party Affiliates		Y or N
User Concern	Questions to Consider: 1. User Data Collection a. Why is my data shared to a third-party that I do not know exists? b. Will the third-party take proper actions to safeguard my data? 2. User Data Sharing Violations a. If the third-party company sells my data to another party, why am I not notified? 3. User Data Confidentiality and Integrity a. If third party servers gets hacked, what position am I in regarding my personal data?	

Table 3 is meant to be used by a consumer and/or user prior to clicking on the “I Agree” box, and the questions presented in Table 3 allows a user to reflect on the ethical concerns involved in these risks. After reading numerous TOS agreements from online services and SNS sites, and researching academic journals written on TOS agreements and user privacy, the identification of the major areas of concerns pertaining to personal risks in TOS’ became clear. Once the four areas of personal risks were identified, the next step was to consider the ethical concerns that a user would have pertaining to their privacy and data. This led to the development of Table 3, as this project needed to include additional

tools for users to utilize during the reading of a TOS. For example, when a user creates an account on Pinterest.com they may use Table 3 and consider the four areas of risks such as: A) Arbitration Concerns- waiving the right to a trial by jury or to participate in a class action, B) Privacy Concerns- Pinterest will use your IP address, which is used to approximate your location, even if you don't choose to share your precise location, C) User Data Ownership- Pinterest does not provide a time frame on how long they store the user data, D) Third-party affiliates- user data is shared with third-party companies to process information and delivery of ads (Pinterest, TOS and PP, 2018). The user can recall Table 3 and based on those questions determine if: they are willing to waive a class action suit, have all their data stored for as long as Pinterest chooses to store it, have their data shared with agencies and companies that Pinterest conducts business with, and have their precise location identified. Users can utilize Table 3 and ask themselves questions that they otherwise may not have asked if these questions were not presented in advance prior to agreeing to the TOS. In addition to providing Tables 1 and Table 3 as tools for users to utilize, this work will also present two findings: 1) Poll results pertaining to how many users read the TOS, and 2) Results on my efforts to control my privacy by disabling Tracking in Microsoft Edge.

Poll Results Pertaining to How Many Users Read Terms of Service

One of the most important ways to mitigate risk is to first read the TOS Agreement. As research suggests, over 91 percent of consumers accept legal terms and conditions without reading them first, and for younger people ages 18-34 the rate increased to 97 percent. For this project, a poll was taken amongst Information Technology professionals and fellow Graduate students. The graduate students polled include business and information technology majors; and the information technology professionals were made up of desktop support staff, system administrators and application analysts.

Table 4. Poll Results.

	IT Professionals 11 Polled	Graduate Students 12 Polled
Do you have an online social network (OSN) account?	8 - Yes 2 - No	11 - Yes 1 - No
For those that do have an OSN, did you read the TOS and Privacy Policy Agreements prior to clicking on “I Agree”?	2 - Yes 6 - No	1 - Yes 10 - No

Based on the Poll I was able to discover some interesting findings. For graduate information technology professionals: 72.7% (8 out of 11) have an OSN, and based on those that do have an OSN, 25% (2 out of 6) read the TOS. For the non-IT graduate students: 91.6% (11 out of 12) have an OSN, but only .09% (1 out of 11) read the OSN. The polls suggest that information technology professionals are slightly more likely to read the TOS Agreement. When I asked three IT professionals why they did not read the TOS I received common responses throughout. One IT specialist stated, “the TOS was too long to read, and I honestly could not be bothered to read it when I opened my LinkedIn account.” The second IT professional said that she did not read the TOS for Facebook because she opened the account when she was in high school, and at that time she did not care or have an interest in reading the TOS. This user said that because she now works in IT, she is more aware of methods that are used to store information and user data, and it has made her more aware of the TOS and PP agreements because she wants to know exactly what is collected and to whom it is shared. She stated that she now reads the TOS for the online services and applications when the service emails her an updated TOS or PP to her personal email address. The third user that I questioned stated that he created his social media accounts when he was a teenager and at that age, “kids do not care to read whatever the TOS was.” The trend when asking users why they did not read the TOS was evident, users were less likely to read the TOS when they were teenagers, and at that age they were less inclined to know the

consequences of agreeing to terms they did not read. It is recommended that online services develop a method to receive parental consent prior to teenagers opening these types of accounts.

The second way that a user can mitigate risks such as Privacy Concerns is to enable tracking prevention and “Do Not Track” requests in their Internet web browser such as Google Chrome or Microsoft Edge. For this project I performed a test with the internet web browser Microsoft Edge, this will be explained in the next section.

Disable Tracking and “Do Not Track” on Microsoft Edge

These features allow the user to take control of how they are being tracked online. Tracking features are advertised to the public as a way for websites to personalize the user experience as “rich, fast and personal as possible” (Microsoft). This means that user data such as cookies and browsing history is collected by web browsers. A “personalized” experience may sound harmless to some users, but others view this as an invasion of privacy where every website that is visited is collected and sent back to Microsoft Edge to collect, store and share.

The internet web browser that was used for this test was Microsoft Edge. Over a five-month period I enabled settings on the browser to test and limit Tracking capabilities. In addition to enabling blocking trackers, I also enabled “Do Not Track” requests feature. Under Tracking prevention, I enabled “Strict”

Tracking prevention on Microsoft Edge. Step 1: Click on the three-dot button on the upper left of the browser and Select Settings.

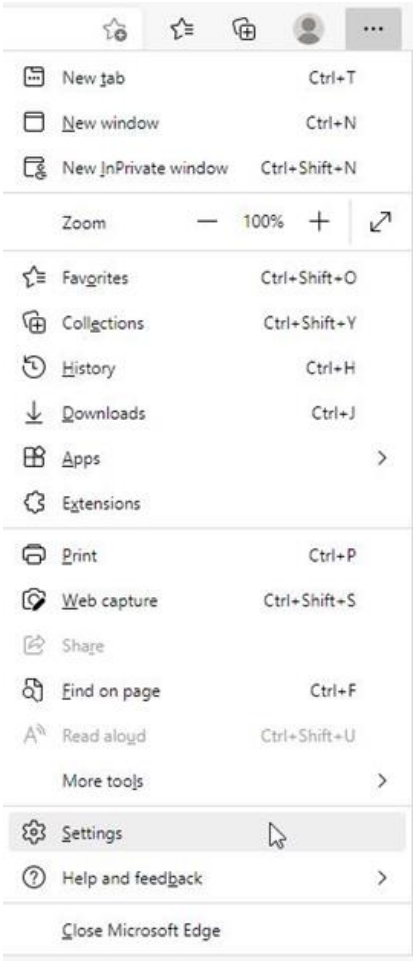

Figure 2. How to Access Settings in Microsoft Edge.

Step 2: Click on Privacy, search, and services.

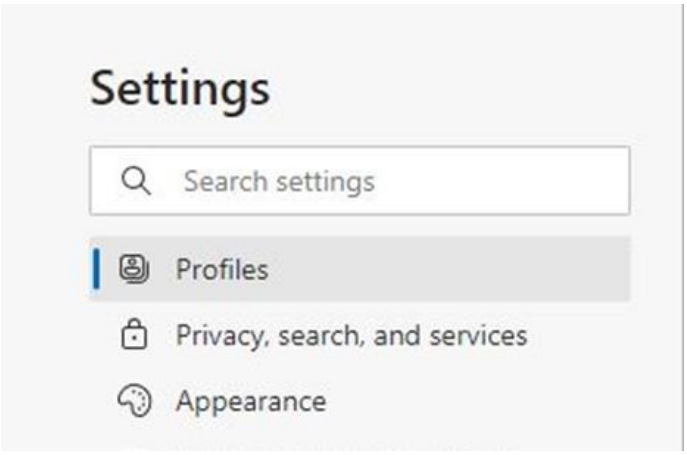

Figure 3. How to Access Privacy, Search, and Services.

Step 3: For Tracking prevention, Select “Strict”. By selecting “Strict,” Microsoft states that this: “Blocks a majority of trackers from all sites, Content and ads will likely have minimal personalization, Parts of sites might not work, and Blocks known harmful trackers.”

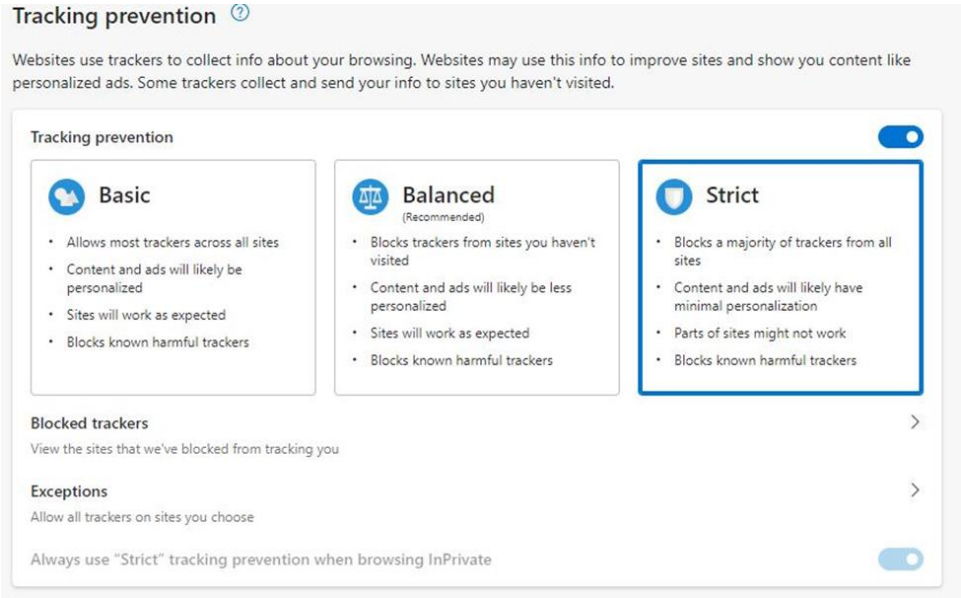

Figure 4. Enabling Strict Tracking Prevention.

Step 4: For the Privacy option I Enabled “Send “Do Not Track” requests”.

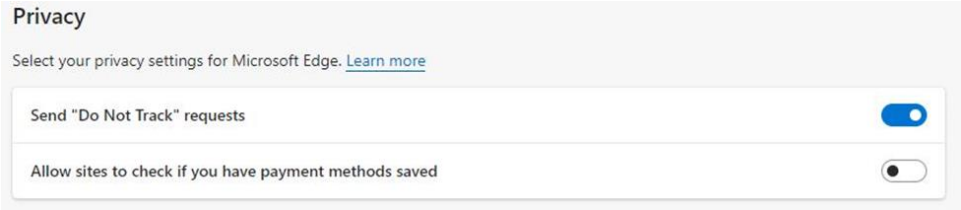

Figure 5. Enabling Send “Do Not Track” Requests.

Over a five-month period these settings were enabled to test how many blocked trackers were blocked by Microsoft Edge. Tracking prevention blocked

51,513 blocked trackers from a total of 270 trackers. The top ten trackers were: Taboola, Facebook, Criteo, AT&T, comScore, Bazaarvoice, RubiconProject, PubMatic, media.net, and Outbrain.

Figure 6. Blocked Tracking Results.

Taboola had the most trackers (25) seen on 27 sites.

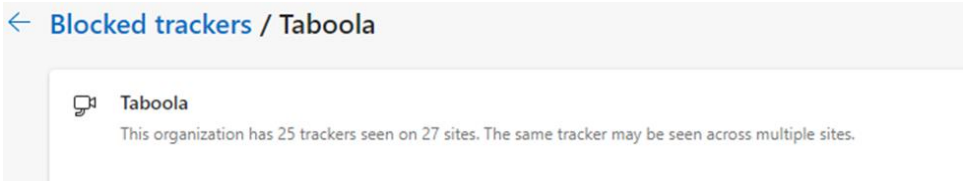

Figure 7. Taboola Tracking Results.

Out of the 270 trackers, Facebook had the most tracking on sites (171 sites) with 15 trackers.

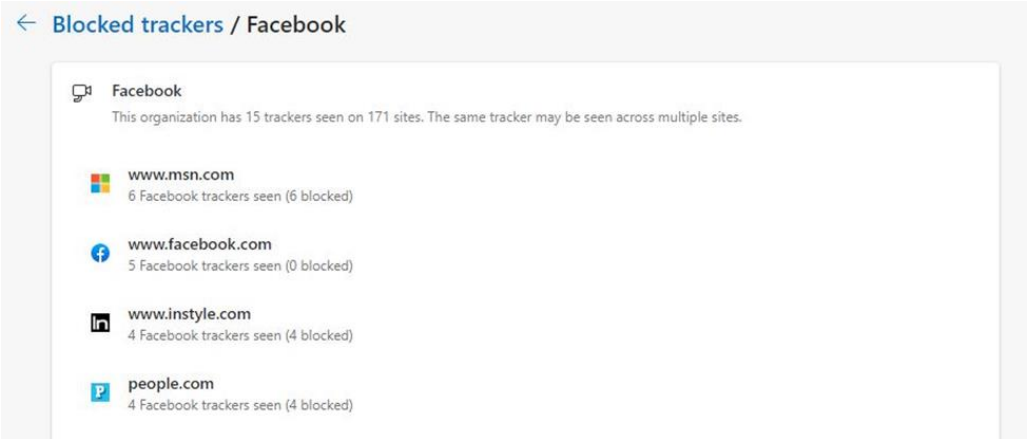

Figure 8. Facebook Tracking Results.

These test results were able to provide an understanding of the vast number of trackers used by internet web browsers, which are tracking user online activity. This tracking prevention attempt blocked 51,513 blocked trackers from a total of 270 trackers, and I was able to take some control of my Privacy when using Microsoft Edge. By enabling “Do Not Track” and blocking trackers, users are able to take another step towards taking control of their data and privacy.

Additional Personal Risk Management

Another method that can be used to understand how users can protect their Privacy online, is to visit https://tosdr.org “TOS Didn’t Read,” or ToS;DR for short (ToS;DR, 2012). The website aims to educate users on the TOS agreements for websites and online services. The website states, ““I have read and agree to the Terms” is the biggest lie on the web. We aim to fix that.” ToS;DR is a young project that aims to empower users and educate the public on their online rights and privacy. ToS;DR grades websites and online services-based topics such as: data collection, privacy concerns, third-party sharing, tracking, and user content licensing. For example, Facebook received a “Grade E” for the following: Facebook stores your data whether you have an account or not, Your identity is used in ads that are shown to other users, The service can read your private messages, This service can view your browser history, and Deleted content is not really deleted. YouTube also received a “Grade E” for the following: This service can view your browser history, deleted videos are not really deleted, Third-party cookies are used for advertising, you are to defend, indemnify, and hold the service harmless in case of a claim related to your use of the service, and This service can use your content for all their existing and future services. The Grade E that these services received are based on having a TOS agreement that raises “very serious concerns,” this grade is based on a Grade A to E scale. Websites such as ToS;DR aim to help people, and their work is appreciated by many who strive to protect their rights and privacy.

Another useful tool which allows a user online privacy and anonymity, is a virtual private network (VPN). A VPN creates a private network from a public internet connection, as well as masking the internet protocol (IP) address so that a user's online actions can become untraceable. Additionally, a VPN encrypts data that a user sends and receives on multiple devices such as phones, computers, and tablets, and it sends this data through a secure tunnel. VPN's are affordable and help maintain user privacy, security and anonymity. Another convenient tool is a Virtual Machines (VM), these are beneficial as they allow a user to build a secure browsing environment with virtualization. VM's are a software-based, or "virtual" version of a computer which runs on a physical machine such as the user's PC. A virtual machine runs its own operating systems that behaves like a completely separate computer in an application window. A virtual environment adds a layer of security, allows a user to build a secure browsing environment, and helps prevent hacking. Open source virtual machines are free and save the user additional expenses.

Another determinant for safeguarding user data is by limiting the content and personal identifiable information that is provided on an online service. To enjoy and use online services, the public can still enjoy the service whilst limiting the data that is shared. For parents, safeguarding their children's privacy should be a top priority. Parents can help safeguard their child's privacy by limiting smart phone and computer access, restricting the websites that can be accessed, reading the TOS and Privacy Policy of such sites, and restricting the upload of

photos and videos on social networking websites. Parents must protect their children from the internet by taking steps to mitigate access to websites that respect the users' rights and privacy.

Summary

It should be noted that not all online services require that a user agree to a TOS contract to use that service, but as more companies adopt this business process the users should be aware of the risks involved. Users must contest forced contracts by adding pressure to local, state, and federal legislators to enact laws safeguarding user rights, privacy, and third-party sharing. Users are misled with contracts such as a Privacy Policy because they assume that these contracts are meant to protect their data and personal information. Unbeknownst to the user, their data is shared with third-party affiliates such as data aggregators and not only is data not protected, but it is sold and shared continuously. Changing legislation so that users are aware of which third-parties have their data and how the data is secured is imperative. Users must remember that by refusing to use an online service and/or product we make an impact on making progressive change. As consumers and users of products and services, we at times forget that we hold power by making choices about which companies we will trust and which services we use. There is power in education and

activism; by adding pressure to legislators and by refusing to use services that violate our rights and privacy, we can make an impression.

CHAPTER FIVE:

DISCUSSION AND FURTHER RESEARCH

TOS agreements are inescapable, therefore safeguarding the user privacy and data should be a high priority for online services provided to the general public. Creating an environment where the user can take control of their privacy and data and how this data is shared, can create a positive relationship between the user and the online service. Additionally, by creating TOS terms and policies that do not confuse a user but make users feel safe and confident, a trusting relationship between the user and the online service can grow. Users can use the findings and recommendations provided in this project to learn more about what happens when they click on the “I Agree” box. Understanding what such contractual agreements are is important and casual users must make informed decisions.

This Project Posed the Following Questions:

Q1. What are the personal risks involved when a user clicks on the “I Agree” box on an online service Terms of Service Agreement?

Q2. How are these risks co-related?

Q3. How can end users mitigate risks after they have agreed to a TOS?

Result Question 1:

The four areas of concern in a TOS were: (A) Arbitration Clauses, (B) Privacy Concerns, (C) User Data Ownership, and (D) Third-Party Affiliates. This project has presented to the user the four areas of personal risks that may harm the user if proper steps are not taken to protect their privacy and data. Parents should also consider the personal risks of their children as children are given mobile devices and computers at a younger age.

Result Question 2:

The four major risks are co-related as the TOS protects the company and not the user. For example, when a user agrees to the TOS, they consent to forced arbitration clauses, thus in an event where a users' personal information is hacked into a third-party server, the user cannot act against the online service. The TOS agreements may have a monetary cap on how much the user may be compensated for damages, and at times this monetary cap is less than the fees to file the suit. The user may file a suit for damages but may not be compensated in a sufficient amount considering the potential damages they may incur once their personal data is in the hands of malicious actors.

Result Question 3:

Users should consider all steps presented in this project to mitigate risks. Following the information presented in Table 1 and Table 3, the user can have a clearer understanding of sections of the TOS that only protect the online service and not the user. Reading the TOS fully is important because these terms are

legally binding and inescapable. Enabling tools such as Strict Tracking blockers, and “Do Not Track” requests, can also help the user take control of their privacy and data. Additionally, purchasing a virtual private network and creating a virtual machine on the user’s home computer can help maintain privacy, security and anonymity.

Suggested Future Research Topics

As part of this body of work, this project included a five-month test using Microsoft Edge and enabled Strict Tracking Blockers and “Do Not Send Requests.” This type of study can be extended further by conducting a comparative study of various browsers and informing the public about the findings. It is recommended that a further study be made of a comparative analysis of Strict non-tracking results for various web browsers such as Microsoft Edge, Firefox, Duck Duck Go, and Chrome. The results can be compared for each of the web browsers, and these results can demonstrate which browser performs best in managing “Do Not Track” requests and blocking trackers. This analysis may help users determine which web browser is best for their needs in taking control of their information and privacy.

Another topic that requires further research is the emotional and psychological aspects of why users choose to not read the Term of Service agreements. In this body of work, the statistics, and reasons for why users choose to ignore the TOS were intriguing as there are consequences when a user ignores or does not understand the implications of a TOS. Therefore, a

study on the behavioral patterns and psychological reasons as to why users choose to ignore the TOS can be researched to demonstrate why users lack the will to read the TOS. From a behavioral standpoint, this topic can be explored to provide insight on the deep and underlying reasons as to why users choose to agree to terms they ignore and/or do not understand.

REFERENCES

Armstrong, Patricia. (2010). *Bloom's Taxonomy*. Vanderbilt University Center for Teaching. Retrieved February 5, 2022, from https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

Becher, Shmuel I., and Benoliel, Uri. (2019). The Duty to Read the Unreadable. *Boston College Law Review*, Vol. (60), 2255. https://lawdigitalcommons.bc.edu/bclr/vol60/iss8/2

Cakebread, Caroline. (2017, November 15). *You're not alone, no one reads terms of service agreements*. Insider. https://www.businessinsider.com/deloitte-study-91-percent-agree-terms of-service-without-reading-2017-11

Federal Trade Commission. (2019, July 24). *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Federal Trade Commission. (2019, September 4). *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*. https://www.ftc.gov/news-events/news/press-releases/2019/09/google youtube-will-pay-record-170-million-alleged-violations-childrens-privacy law

Federal Trade Commission. (2014, May 8). *Snapchat Settles FTC Charges That Promise of Disappearing Messages Were False*. https://www.ftc.gov/news-events/news/press-releases/2014/05/snapchat settles-ftc-charges-promises-disappearing-messages-were-false

Good, N., Grossklags, J., Hoofnagle, C. J., Mulligan, D. K., Turow, J. (2007). The Federal Trade Commission and Consumer Privacy in the Coming Decade. *University of Pennsylvania ScholarlyCommons*, Vol. (3), 723-749. https://repository.upenn.edu/asc_papers/394

Hans, G.S. (2012). Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era. *Michigan Telecommunications and Technology Law Review*, Vol. (19), 163. http://repository.law.umich.edu/mttlr/vol19/iss1/5

Kidken Edu Solutions. (n.d). *Bloom's Taxonomy*. Retrieved February 6, 2022 http://www.kidkenmontessori.com/blooms-taxonomy/

Koenig, Thomas H., and Rustad, Michal L. (2014). Fundamentally Unfair: An Empirical Analysis of Social Media Arbitration Clauses. *Case Western Reserve Law Review, Vol*. (65), 341. https://scholarlycommons.law.case.edu/caselrev/vol65/iss2/5/

Nelli, Sabeer. (2022, March 3). *Most People Never Actually Read Terms and Conditions, But It's a Major Data Risk*. Yahoo Finance. https://finance.yahoo.com/news/most-people-never-actually-read 170000324.html

Paul, Kari. (2019, December 28). *A Brutal Year: How the 'Techlash' Caught up with Facebook, Google and Amazon*. The Guardian. https://www.theguardian.com/technology/2019/dec/28/tech-industry-year in-review-facebook-google-amazon

Pulvermacher, Katie. (2021, September 15). *Who Really Reads "Terms and Conditions"?* The Advance-Titan. https://advancetitan.com/opinion/2021/09/15/who-really-reads-terms-and conditions?return

Schaub, Florian. (2017, October 9). *Nobody Reads Privacy Policies – Here's How to Fix That*. The Conversation. https://theconversation.com/nobody reads-privacy-policies-heres-how-to-fix-that-81932

Shonk, Katie. (2022, January 24). What is an Arbitration Agreement? The Ins and Outs of Contractual Agreements to engage in arbitration. *Daily Blog Program on Negotiation, Harvard Law School*. https://www.pon.harvard.edu/daily/conflict-resolution/what-is-an arbitration-agreement/

ToS;DR. T*erms of Service: Didn't Read "I have read and agree to the Terms" is the biggest lie on the web. We aim to fix that*. (2012). Retrieved February 10, 2022, from https://tosdr.org/en/frontpage

Terms of Service. (2018, May 1). Pinterest. Retrieved February 2, 2022, from https://policy.pinterest.com/en/terms-of-service

Terms of Service. (2021, November 15). Snapchat. Retrieved February 2, 2022, from https://snapchat.com/en-US/terms

Upcounsel. (2020, November 16). *What is a Terms of Service Agreement?* Retrieved March 3, 2022, from https://www.upcounsel.com/terms-of service-agreement

Vida, Adam. (2019, March 12). *Best Practices for Sharing Information with Third Party Systems*. FedTech Magazine. Retrieved February 5, 2022, from https://fedtechmagazine.com/article/2019/03/best-practices-sharing information-third-party-systems