HIGH SCHOOL EDITION
Journal of Student Research
Volume 13 Issue 3 (2024)

Exploring the Predatory Practices of Terms of Service Contracts and Privacy Policies

Diego Rivera Álvarez[1] and Johnny López[#]

[1]Commonwealth-Parkville School, Puerto RIco
[#]Advisor

ABSTRACT

This research paper primarily examined how Internet users interact with terms of service contracts and privacy policies. Terms of service contracts and privacy policies regulate the interaction between users and online services and how their data is managed. Despite this, Internet users seldom take the time to read, analyze, and understand these contractual terms. This research paper incorporated numerous studies and surveyed participants to determine the extent to which this ignorance occurs. In addition, the reasoning behind opting not to read terms of service contracts and privacy policies was explored. Lastly, this paper synthesized expert recommendations and participant suggestions to clearly outline multiple methods to increase interaction between users and terms and policies. Information on proactively protecting personal information was also included to expand on simple alternatives to data protection. The conducted research focused on the jurisprudence of the United States. A contextual foundation was built by incorporating articles and research on legislation and judicial precedent. A historical foundation was built by incorporating articles and research on foreign statutes and historic data communication systems.

Introduction

The implementation and utilization of the Internet in various aspects and disciplines of human society are increasing daily. The Internet has become synonymous with modern human life, its influence ranging from private individuals to large organizations and national governments. This observable increase in reliance on Internet-based infrastructure brings with it the transmission and collection of multiple types of data —credentials, health data, private information, conversations, national identifiers, Internet searches, and even user-service interactions. In many cases, the exponential growth the Internet has observed has superseded legal safeguards and regulations. This mismatch in growth equates to the existing way online services collect, utilize, store, share, and sell data. It is necessary to recognize that data has a place in research to advance technologies, services, and society; however, it is also important to note that data can be used to, for example, create and build sharable and sellable profiles of users and track them. In the worst cases, inappropriately stored, encrypted, shared, or sold data can be used maliciously to steal identities, access computer systems, and obtain private information.

Many online services utilize contracts —commonly known as terms of services, terms of use, or terms and conditions— which include privacy policies to establish a written norm between them and their users. Terms of services regulate user behavior within a platform, establish jurisdiction, and control access to judicial or arbitration recourse. Privacy policies outline how services collect, utilize, store, share, and sell user data.

In the United States, no federal law regulates the enactment of terms of services and privacy policies (Klosowski, 2021). Instead, states are left to devise their regulations on the matter. The presentation of terms —including display, text size, color, font, position, and other factors— is principally decreed by different judicial opinions given and applicable in different jurisdictions. Specifically with privacy regulations, only thirteen states have some kind of online privacy legislation as of the time of writing this paper (Folks, 2024). This paper

recognizes that specific niches and data natures are protected by statute against certain persons and institutions; however, most types of data fall under free reign. The closest concept to general privacy regulation is the "notice-and-choice" model originally conceptualized in the late twentieth century and adopted by the FTC. The notice-and-choice model requires online services to provide "notice" on data utilization and empowers users to "choose" whether to accept or reject said use. In reality, the model creates only the illusion of choice —term and policy clauses are circumlocutions hidden behind hyperlinks and the famous "small print." The agreement to contractual clauses, which includes the collection, utilization, storage, sharing, sale, and control of personal user data must be nationally regulated, made to be clear and transparent, and prioritize the user.

Problem Statement

Society has normalized opting not to read terms of service contracts and their privacy policies —contracts that dictate how users can and cannot interact with online services, the data services can collect on their users, and recourses. The reality of the situation, and the excuse many cite, is that regularly doing so is inconvenient and impractical. In some cases, Internet users are seldom aware of the scope and magnitude of data collection they assented to in theory. Some projects —including ToS;DR— have attempted to summarize and spread awareness of the language included in terms of service contracts. Similarly, services and foundations like DuckDuckGo and Mozilla have aimed to allow their users to enjoy a higher degree of privacy online. Tools such as VPNs, temporary email providers, data deletion services, and ad blockers, amongst others, also aim to empower users to exercise a higher degree of control over their personal data.

Purpose

This research paper focuses on the jurisprudence of the United States. It aims to address the problem by exploring online contracting, the privacy norm, suggestions made by experts, and the analysis of a survey conducted by this paper's author. This paper recognizes the vital role knowledge and transparency play in creating and maintaining a safe and informed society and wants to aid in accomplishing that vision. This paper hopes to converge this collectivity of rich information to generate and propose a solution that focuses on protecting the user.

Justification

It is in the public's interest that all factors pertaining to online contracting, privacy policies, and judicial recourse be outlined clearly and legibly. Human society is becoming more reliant on Internet-based technologies. Unfortunately, Internet statutes aiming to protect the user are outdated or nonexistent in many places, which by default permits online services to develop and enforce their own rules. Privacy is one critical element falling behind in this evolutionary process. Research and awareness projects concerning the protection and preservation of privacy and control are crucial to ensuring every online service implements and follows ethical terms and policies, every government enacts protective legislation, and every individual can exercise control over their data.

Research Questions

1. How versed is the average Internet user in terms of service contracts and privacy policies?
2. What legal statutes protect Internet users from predatory terms of service and privacy policy clauses?

3. What can be done to make terms of service contracts and privacy policies more accessible and understandable for the average user?
4. What can be done to make data privacy protections more accessible to the average Internet user?

Research Objectives

1. To understand how Internet users interact with the terms of service contracts and privacy policies of online services.
2. To explore the legal protections Internet users have against unethical and predatory terms of service and privacy policy clauses.
3. To evaluate what can be done to promote the importance of reading and understanding terms of service contracts and privacy policies and assess different methods aimed at increasing the levels of accessibility and understanding towards them.
4. To extrapolate different methods that actively recognize and promote Internet privacy as a right.

Theoretical Framework

Advances in technology bring with them societal and ethical challenges (Cohen-Almagor, 2013). The Internet, a decentralized network which was originally developed as a solution to long-distance communication, is a tremendous example of this fact (Cohen-Almagor, 2013). Amongst its many flaws exists the continual decay in the expectation of privacy in online spaces; the Internet is experiencing an increase in centralization in the hands of private Internet intermediaries and service providers (Belli & Venturini, 2016). In large part, this problem is rooted in the lack of consumer privacy and control legislation —in the United States, no singular national law regulating the collection, storage, and usage of data exists (Klosowski, 2021). Instead, the rights and protections of Internet users are cemented in judicial precedent applicable and varying between jurisdictions of the country (Lovendale & Lam, 2022).

Terms of service contracts are the principal regulator of behavior between users and an online service; due to the lack of legislation or recourse, these service providers have a substantial degree of autonomy to what is included in their terms (Belli & Venturini, 2016). One aspect regulated by these contracts is privacy, through privacy policies, which are based on the notice-and-choice model developed in the 1970s (Obar & Oeldorf-Hirsch, 2018). Originally intended to help users control their data, the reality of the situation is that Internet users do not read terms of service contracts prior to assenting to them (Obar & Oeldorf-Hirsch, 2018; Steinfeld, 2016; Klosowski, 2021).

There is an urgent need for laws concerning the Internet to evolve to encompass the reality of modern times and place the user and their data first (Fox & Lynn, 2020; Klosowski, 2021; Belli & Venturini, 2016). There is also an urgent need to educate the public on the importance of promoting both laws protecting online privacy and existing alternatives that empower users over their data (Fox & Lynn, 2020; Klosowski, 2021; Steele, 2021).

Definition of Terminologies

Terms of service contracts contain the legal terms that outline the nature, scope, limit, and rules of a service; a term first used in 1994 (Merriam-Webster, n.d.). The terminology is synonymous with similar terms like “terms of use” and the broader “terms and conditions” (Husain, 2023). Privacy policies exist within the context of terms of service contracts and outline the collection, handling, usage, distribution, storage, and control of data; in the United States, these policies generally adhere to the Fair Information Practice Principles (FIPP) of the

Federal Trade Commission (Steinfeld, 2016). The FIPP were originally developed by the United States Department of Health, Education, and Welfare back in 1973 and outline the notice-and-choice model, where notice of an action is provided by the entity and choice to permit the action is given to the user (Schwartz & Solove, 2009; Obar & Oeldorf-Hirsch, 2018). In a broader sense, privacy policies and the FIPP draw from top-down approaches to privacy, wherein national governments and service providers exert control; the opposite and less popular approach, bottom-up, refers to cases where control begins at the user level (Obar & Oeldorf-Hirsch, 2018).

Literature Review

Internet History: Internet Milestones and Privacy Concerns

The Internet is coupled with a rich and interesting history. This source outlines and analyzes Internet history milestones, accounting for societal and ethical challenges —for instance, its anonymous nature— stemming from technological advances. The necessity to preserve communication between distant areas, which was not possible through existing electric infrastructure, gave rise to the Internet. Research groups, universities, and telecommunications firms in the United States that were interested in building the Internet came up with and used the early version of it.

As technology developed, the Internet became more widely used, monetized, and integrated into many facets of contemporary culture and daily life. Created by the U.S. Department of Defense in reaction to the Soviet Union's Sputnik satellite launch, the Advanced Research Projects Agency (ARPA) aimed to generate novel research concepts, yield significant technological advancements, and create prototype systems for these concepts. The Information Processing Techniques Office (IPTO), one of the ARPA offices, provided funding for studies conducted by American universities to build communication networks. This office released the first paper that conceptualized the Internet in August 1962. Subsequently, scientists and researchers theorized decentralized systems, which included packet (standard addressed message blocks) networks (adaptive routing procedures with distributed control) and switching (splitting packets to allow for faster transfer). These theories led to the introducing of the first radio transfer system, ALOHANET, and the first advanced computer network, ARPANET. The Internet's decentralized structure and ease of use contributed significantly to its explosive expansion. A variety of computer types with various operating systems could be included in the universal network. The ARPANET project ended in 1990 when the National Science Foundation (NSF) received control of the public Internet backbone.

When encryption programs such as PGP (Pretty Good Privacy) were made available to the public, they raised moral questions. They had social repercussions because they improved privacy at the expense of personal security by giving criminals more power. Because anonymity was permitted, Internet users were not forced to accept social norms and rules of conduct that they saw in other parts of society. The first treaty to handle crimes committed over the Internet was finalized on June 22, 2001, by the European Council and adopted on November 9, 2001. The ethical subject of Internet social networking is highly pertinent today. Although the main aims of social networks are communication and socialization, some users use them to promote violent causes like child pornography and terrorism.

Overall, the Internet evolved from its original conceptualization of being a communication tool, creating with it societal and ethical challenges still observable presently. Originally a state-owned technology, its public backbone was handed over to the NSF in 1990. Technology-enabled tools have two sides: they can both defend and harm their user. Cohen-Almagor indicates this by stating:

[Encryption] presents a technological-ethical challenge with significant social implications as it is also used by Net abusers.…it is used by criminals and radicals who wish to hide their Net identity in order to advance

anti-social behavior. In other words, encryption is a double-sword crypto-assisted anonymity tool: It may enhance your privacy and anonymity but it might also undermine your own security….there is a conflict between anonymity…and trust and accountability….Indeed, anonymity undermines accountability on the Internet: If Netusers can hide their identity and be entirely sure that no one knows they are the agent of mischief, this might be an incentive for some people to adopt norms and codes of behavior that they would otherwise be deterred to adopt. The Internet opened new horizons for criminals and terrorists. (Cohen-Almagor, 2013)

The importance of this source concerning this investigation is the discussion of the abundant history behind the Internet. Technological advancements and scientific collaboration made developing the Internet possible. Emerging from a need to maintain communication over vast distances, the Internet surged and became synonymous with modern human life. This source is relevant to this investigation because it brings contextual information to the discussion. This source also discusses how tools designed to protect users can have retributory effects. Researching the history of things empowers understanding and knowledge of how to act. Through this information, this investigation can include historical facts in its exploratory journey to safe online practices.

Internet User and Data Collection and Retention Policies by Governments and Institutions

Many new problems and conflicts have arisen due to the information flow in our contemporary digital society. This source looks at how organizations, governments, and people gather and use vast amounts of personal data and emphasizes privacy issues that arise when these practices are carried out in secret. Many Americans believe their phone calls, texts, emails, and Internet searches are private. The United States National Security Agency (NSA) was revealed to have been spying on American people in June 2013. Around the world, computer networks yielded 100 billion bits of data to the National Security Agency (NSA) in March 2013. The legal system in the United States was designed to safeguard the privacy of innocent Americans, even while it grants the NSA legal authorization for certain forms of surveillance. The NSA could access almost every communication and piece of personal data.

Some think it is worth it to give up privacy. Big data has proven beneficial and challenging in almost every area of life, including social relationships, healthcare, and retail. Daily, and frequently without realizing it, people trade their privacy for convenience. 74% of Americans said it was important to control who may access their information, according to a 2015 survey. Despite their slowness and memory limitations, early computers could capture vast volumes of data with little guidance on storing and using it.

The practice of saving data for potential future use has been dubbed "big data." The information gathered has several uses, such as tracking, advertising, and profiling. Although "big data" has many beneficial applications, uncertainties and worries exist. The benefits of social media include news, expression, meeting new people, entertainment in general, and staying in touch with loved ones and friends. Privacy is another issue that it raises. Whether done knowingly or unknowingly, people are likely to provide extensive personal information on these websites, which can have many adverse effects. For instance, sharing trip details online can attract robbers, and responses to "online quizzes" can be sold to other businesses for targeting and profiling purposes. On social media, targeted feeds can also help control feelings and responses.

Security becomes a concern when large volumes of personal information are kept on computers. Cybersecurity regulations already in place to safeguard personal data are not always sufficient or followed. According to a 2014 survey, 27% of American businesses did not have a plan for handling a data breach, despite 43% having suffered one the year before. Malware, hacking, theft, misplaced equipment, and even accidents can leave information vulnerable. Many people, particularly young people, think connecting their financial or commercial records with their personal life is okay. Applicants can grant a corporation temporary access to their social media accounts or to look up publicly available information about them.

Numerous options for information protection are provided by technology. Messages are encrypted, so only those with the key can decipher what is written therein. Even though encryption is a crucial security measure, it is not impenetrable. People can utilize encryption on various devices, including laptops, memory sticks, and web browsers. In actuality, most people do not use technology to safeguard their data, primarily due to the intricacy of these solutions; this source clarifies this through the use of statistics:

Technology can help protect an individual's information, but few people take that option. For most people, the use of solutions such as encryption may seem too complicated. No more than 10 percent of adults say they have encrypted phone calls, e-mails, or text messages, according to the 2014 Pew Research study. Even though most adults thought they should be able to use the Internet anonymously, only 9 percent had used a service to browse the web anonymously. People also run into trouble when they do not realize deleting a message or photo does not mean it completely disappears.…People are more likely to take relatively easy steps to protect their privacy, such as clearing their Internet browser history. People may also refuse to provide information that is not necessary for a transaction. Some even provide false or misleading information about themselves in order to preserve their privacy. (Eboch, 2017)

This source is relevant to this investigation because it explores large organizations and governments' mass collection of user data. It also examines technologies that exist to protect data and the ethical dilemmas surrounding it. Lastly, it explores how individuals should be proactive in securing their data. This source is vital to this investigation because it delineates how perception and reality play a huge role in online privacy. It outlines examples where organizations did not adequately protect data and cases where methods thought to promote privacy did not. This source acknowledges data collection's crucial role in research and presents the challenge of balancing collection and privacy. This source helps advance this investigation by presenting historical examples and research on data protection by users and organizations.

The U.S. Postal System Correspondence Privacy Related to Digital Surveillance

Organized data transmissions have historically occurred through postal systems. This study explores the history and legacy of postal privacy, showing how and why lawmakers came to regard it as a norm and highlighting certain parallels between this history and twenty-first-century debates over digital surveillance.

Balancing civil freedoms and collective security is not unique to modern civilization. Officials nowadays frequently defend the monitoring of digital communications by claiming that it is an unavoidable reaction to an existential threat. In contrast, the Post Office Act of 1792 was a legislative measure that rejected the idea that the government had the power to monitor private correspondence in the eighteenth century. From the 1790s until the present, this strategy has influenced American communications policy. Strict sanctions, including the death penalty if the letter included money, were imposed by lawmakers on postal workers who mishandled or opened any letter received through the mail. Because the postal system was perceived as serving the national interest rather than working against it, these policies contributed to the system's increased trust. They created the privacy standard.

The fact that there have been numerous instances of communication privacy infractions throughout American history should be acknowledged, but this does not make the policy decisions any less essential. The policy's past provides a helpful reference for individuals concerned with safeguarding digital privacy today. Conversations regarding digital surveillance today bear a striking resemblance to the language used to discuss what is now known as privacy between the 1770s and the 1790s.

With the advent of new media, the state's duty to preserve privacy has steadily diminished. In contrast to the U.S. postal system, data collection and surveillance are the main economic drivers of the Internet. A bill that President Trump signed into law in 2017 permits Internet service providers, or ISPs, to sell individual users' browser records to advertising without the users' permission. In order to protect their communications from

prying eyes, modern internet users are resorting to encryption. In the mid-1990s and mid-2010s, the U.S. government made several attempts to outlaw solid encryption because of worries that digital technology would result in genuinely unbreakable encryption. Ultimately, rather than liberal civic arguments, the legality of advanced encryption methods was maintained by business interest. Encryption is not the same as privacy; encryption represents privatizing privacy due to a strong presumption of interception. With encryption, the sender and recipient must maintain their privacy without institutional and legal safeguards. Nechushtai writes about the implications of encryption by stating:

However, it is important to note that encryption is not the same as privacy: it represents the privatization of privacy due to a strong presumption of interception. Without legal and institutional protections for the confidentiality of information, securing privacy is once again the personal responsibility of the sender and receiver alone—a state highly reminiscent of preprivacy [*sic*] postal systems. The implications of surveillance in the twenty-first century are substantially greater than they were in the eighteenth century, since the information produced in contemporary online activities is much more personal and sensitive than that produced in early modern postal exchanges, and, unlike handwritten pages, digital records are stored indefinitely…. Transferring the onus of responsibility for privacy from the state to citizens creates a new divide between the individuals and organizations well positioned to ensure the privacy and security of their communications and those that are less so. (Nechushtai, 2019)

The usefulness of this source in relation to this investigation lies on the exploration of a historic example of preserving privacy in communication networks: the United States Postal Service. It explores the belief that failure to uphold civic norms and generate trust in the postal system posed a more significant risk despite the era's war climate. It also explores how, today, public officials routinely justify the surveillance of digital communication to protect national security. This source is essential to this investigation because it compares a historic example to a current problem example. This source also mentions how Internet users have developed ways to combat surveillance. It also mentions instances when the U.S. government attempted to trawl such developments. Lastly, this source outlines the primary motivator behind the lack of privacy protections — profit building — and how it can and has historically been used to push for privacy protections. This source helps advance this investigation by providing insight into the decadence of privacy protections as communication mediums have developed throughout U.S. history.

Increasing Use of Terms of Service Contracts to Self-Regulate Online Services

The concentration of power in the hands of Internet intermediaries is leading to the centralization of Internet governance. Although terms of service agreements are presented as voluntary acceptance through free and informed consent, they unilaterally impose rules. The Internet was first regarded as the place governments had no power over; however, today, increasing reliance on various intermediaries makes the Internet a hyper-regulated environment at the hands of both governments and private platforms.

Modern legal systems are grounded in separation of power theories. In many ways, the Internet opposes this; Internet intermediaries, who play essential roles in ensuring the Internet functions properly, can unilaterally define contractual clauses, modify them at personal discretion, and enforce them. Platforms can also regulate the collection, processing, and sharing of personal and non-personal user data whenever included in their terms of service.

Platforms also enjoy certain judicial powers. Many terms of service define alternative dispute resolution systems —like arbitration— and prohibit participation in class action suits. Terms of service regulatory functions are limited by statutes striking a balance between the protection of users' rights and the contractual autonomy of the intermediaries. In the absence of comprehensive rights, platforms may contractually regulate such services, as explained here:

In the absence of comprehensive fundamental rights protection and consumer protections, private actors providing any kind of internet service may contractually regulate such service in the most economically efficient way, which may not be the most user-interest-oriented. Indeed, this latter approach includes the utilisation of jurisdiction clauses as well as class-action-waiver clauses that can obviously help saving the costs of entering into legal disputes around the globe but can also severely diminish the protection of users' rights…the results of the aforementioned analysis show an imbalance of power between companies and users' rights, demonstrating that the most efficient choices may frequently neglect the full protection of users' rights. (Belli & Venturini, 2016, p. 6)

The researchers recommended that platforms assess the impact of their terms of service and algorithmic implementations on their users' rights. They also suggested that national regulators review terms of service and technical means to enforce them to ensure their conformity with applicable law. Moreover, they highlighted the importance of transparency for platforms while modifying terms of service agreements and the need to facilitate access to traditional court systems.

This source investigated the power that terms of service agreements and privacy policies enshrine on online services. This source noted the facility such services have for unilaterally enforcing their provisions. A comparison of online services to governments was created to portray their unique opportunity to enforce their provisions. In many cases, these services can also inhibit the involvement of judicial bodies through arbitration and class action waiver clauses. One principal goal of this investigation was to encourage the creation of proper policy notices and foment awareness. They also denote the need for online services to be proactive in protecting their users' privacy as human rights irrespectively of existing national law. In addition to this, the researchers noted the need for national regulators to be able to intervene and prevent illicit language from reaching published agreements and policies. This source is essential to the investigative goal of this paper because it uncovers the unique and, in many cases, the extrajudicial way online services can apply and enforce their terms of service agreements and privacy policies. Building a foundation on such applications is one way the findings of these researchers can help advance the present investigation.

Data Privacy Laws in the U.S. and the Importance of Enacting Such Legislation

There is a public interest for enacting data privacy laws in the United States. This investigation explored the state of consumer privacy laws and the need for customer-centric legislation in the United States. In addition to generating profit for companies, data sharing can lead to data leaks or breaches. Consumer data privacy laws can give individuals the right to control their data; however, they must be properly and thoughtfully implemented to accomplish this. For example, in the European Union, the General Data Protection Regulation (GDPR) requires companies to request permission to share data. The GDPR also gives individual rights to access, delete, or control the use of said data.

In the United States, no single, comprehensive federal law regulates how most companies handle data collection, storage, sharing, breaches, or exposure. Instead, different sectoral rules regulate specific types of data:

1. HIPPA (Health Insurance Portability and Accountability Act) regulates the communication of health data between you and certain entities.
2. FCRA (Fair Credit Reporting Act) restricts who can access credit reports, what can be collected, and how.
3. FERPA (Family Educational Rights and Privacy Act) restricts who can request student education records; however, it does not restrict how companies use collected data so long as it is disclosed beforehand.
4. GLBA (Gramm-Leach Bliley Act) requires consumer financial products to explain how they share data and explain customers' right to opt-out.

5. ECPA (Electronic Communications Privacy Act) restricts government wiretaps on telephone calls and other electronic signals and monitoring of employee communications; however, it does not protect against modern surveillance tactics.
6. COPPA (Children's Online Privacy Protection Rule) limits data collection for children under 13 years of age.
7. VPPA (Video Privacy Protection Act), preventing the disclosure of VHS rental records. Application to streaming companies is questionable.
8. FTC Act (Federal Trade Commission Act) empowers the FTC to pursue services that violate their privacy policies and investigate violations of marketing language related to privacy.

Because no federal law regulates online privacy protections, states of the union can opt to introduce their statutes. Unfortunately, only a handful of states have enacted such laws, and these rights only apply to users who live in those states. These laws have similar provisions that give the user some type of notice and choice in controlling their data. Some laws allow for private right of action (right to sue), while others do not contain such provisions. California's privacy protections are considered the strongest in the U.S. Contrastingly, some experts view Virginia's law with skepticism and consider it business-model affirming. State legislators have rejected many state privacy laws because of protections like the private right to action and the right to opt in rather than out.

The investigator noted that well-redacted privacy laws equate to no significant changes to the average user. "Privacy isn't about not using tech, it's about being able to participate in society and knowing your data isn't going to be abused, or you're not going to have some harm down the road because of it" (Stepanovich, 2021, as cited in Klosowski, 2021). The current "notice and choice" norm promises transparency and agency; however, user overwhelmingness tactics facilitate automatic acceptance over manual:

One sticking point of the current opt-out system is notification fatigue. When every app and website is asking you for dozens of permissions, it becomes easier to accept the status quo than to manually opt out of every tracking technology. A review article in Science…in 2015 highlighted just how poorly most people performed in navigating privacy risks, and a 2019 paper described the sort of 'notice and choice' consent that everyone is used to as 'a method of privacy regulation which promises transparency and agency but delivers neither.' All of the experts we spoke with preferred an opt-in consent model and "privacy by default" concepts. Such an arrangement would make accounts private initially…It would be up to you to opt into those settings. (Klosowski, 2021)

Baselines of privacy and easy-to-understand opt-in rules for sharing data would make the user experience more comfortable and reassuring. Following the research process, the investigator concluded that these privacy-related areas deserve to be the standard:

1. Using opt-in, not opt-out, mechanisms for data sharing and sale assent.
2. Limiting data collection to only the bare minimum necessary to provide a service, as well as the ability to see collected data, request its deletion, and prevent its sharing or sale.
3. Provisioning for the private right to sue, or law enforcement mechanisms in the alternative, and preventing discrimination against those exercising their privacy rights.

This source explored the existing legislation at the state and federal levels concerning online privacy in the United States. The source recognized the lack of foundational protections for users. The existence of independent and specific laws regulating particular data management was also discussed. Specific current, proposed, and rejected state laws and their effectiveness were additionally examined. Lastly, foreign legislation like the EU GDPR was consulted. The author wrote the present article with Wirecutter's recurring need to disclaim privacy warnings in their advertised products. This aim aligns with this research paper's quest to seek information on privacy legislation. This source is essential to growing this investigation because it provides research on the current state of affairs regarding online privacy and user rights.

Law and Court Rulings on the Enforceability of Electronic Contracts in the U.S.

This study investigated how various state and federal courts enforce electronic contracts under common law precedents. Examined court cases include *Berman v. Freedom Financial Network* (9th Cir.), *Sellers v. JustAnswer* (California), *Sarchi v. Uber Technologies* (Maine), *Kauders v. Uber Technologies* (Massachusetts), and *Doe v. Roblox Corp.* (California). Multiple state and federal courts have considered whether the way services present terms of services were sufficient to form an enforceable contract with users. In the case of electronic contracts, courts assess whether the user has engaged in conduct that manifests their acceptance of the applicable terms:

No matter the jurisdiction, in order to have an enforceable contract the mutual assent or consent of the parties to the terms of the agreement is essential. This is no less true with electronic contracts, such as website terms of use or the terms and conditions of an app. Because users of websites and apps typically do not receive a physical copy of the contractual terms relating to their use of such sites and apps, courts typically analyze whether the user has engaged in conduct that manifests their acceptance of the applicable terms. The company must show that the contractual terms were presented to the user in a manner that made it apparent the user was assenting to those terms when doing something on the site or app like checking a box or clicking a button. (Lovendale & Lam, 2022)

Browser-wrap agreements occur when terms are disclosed through hyperlinks, and assent is implied through continued service use. Courts do not uphold these because users are frequently unaware that contractual terms were offered or that continued use constituted acceptance of such terms. Having hyperlinks to the terms on every page but not informing the user of their existence or prompting them to take any affirmative action, irrespective of their position within the page or button elements, does not demonstrate assent.

Sign-in-wrap agreements occur when terms are disclosed through hyperlinks at a registration page before users can use a service, and assent is implied through user registration. Courts typically evaluate whether a service provides reasonably conspicuous notice of terms and whether the user takes action that unambiguously manifests assent. Courts have considered factors such as relative and readability of font size, text color, and text location, the obviousness of any associated hyperlinks, whether other elements obscure the textual notice, and even presumed user savviness or age.

Click-wrap agreements occur when terms are disclosed through either hyperlinks or directly —before being able to use a service— and assent is demonstrated through direct acceptance. Courts have generally considered these enforceable because they require affirmative and expressive action.

Scroll-wrap agreements occur when terms are disclosed directly, and assent is demonstrated by making a user scroll through an entire text before being made to accept directly. Courts have consistently found these enforceable due to their prominent nature and required scrolling and affirmative action.

The consensus dictates that browser-wrap agreements are unenforceable, sign-in-wrap agreements need to be individually considered, and both click-wrap and scroll-wrap agreements are generally enforceable. The study found that companies are responsible for providing adequate notice of contractual terms, obtaining user assent, and providing easily reachable terms and policy pages. Additionally, it noted that courts generally enforce click-wrap and scroll-wrap agreements but not browser-wrap and sign-in-wrap agreements.

This relevance of this source in relation to this research paper is its exploration of existing common law precedents set out by different state and federal courts of the United States. Specifically, this source analyzed precedents regarding the enforceability of electronic contracts based on how they are presented to users. The authors intended for the contents of their article to be utilized by lawyers and companies drafting the presentation of terms and policies. Irrespective of this fact, the research compiled contains valuable information on the different presentations of terms and policies. Additionally, the authors discuss how users can enter legally binding contracts and better ascertain their rights. Lastly, the authors cite specific case law relevant to this investigation. The reasons expose the logic behind integrating this source into the present research paper. This

source can help advance this investigation by providing information that aids in understanding basic contract concepts and user rights.

Law and Court Rulings on the Unilateral Modification of Electronic Contracts in the U.S.

This investigation explored the legal foundation and enforceability of terms of service modification clauses. Examined court cases include *Badie v. Bank of America* (California), *DIRECTV v. Mattingly* (Maryland), *Ozormoor v. T-Mobile USA* (6th Cir.), *Manasher v. NECC Telecom* (6th Cir.), *Briceño v. Sprint Spectrum* (Florida), *Klocek v. Gateway* (Kansas), *Knutson v. Sirius XM Radio* (9th Cir.), *Campbell v. General Dynamics* (1st Cir.), *Douglas v. U.S. Dist. Court ex rel. Talk America* (9th Cir.), *Rodman v. Safeway* (9th Cir.), *TradeComet v. Google* (2nd Cir.), *Harris v. Blockbuster* (Texas), and *Liebowitz v. Dow Jones & Co.* (New York).

Over the years, users have challenged the enforceability of terms of services, creating a body of common (judge-made) law. Traditional contract doctrine forbids the unilateral modification of contracts and treats a proposed modification as an offer until accepted. Generally, three elements are required to form a contract: the offeree must have proper notice of the proposed modification, manifest assent in some manner, and enter into a contract in good faith. Multiple courts have ruled on what constitutes proper notice and what does not — in physical mediums. They have considered font sizing, weight, page location, and additional visual factors. In addition, courts have considered the circumstances under which notice was given:

In [*Campbell v. General Dynamics*], an employer attempted to modify an employment handbook by sending a mass company-wide e-mail message containing hyperlinks to the proposed changes to its employees. One of the proposed modifications was a binding arbitration clause. In holding that the modification was not effective, the court focused on the expectations of the employee receiving the modification offer. Given that the mass e-mail message did nothing to communicate its importance and that employment changes at General Dynamics were usually communicated in person by means of a signed writing, the court held that the attempted modification was not binding. (Moringiello & Ottaviani, 2016)

Courts have classified online terms according to whether users are made to click a button to indicate assent (click-wrap) or use hyperlinks and implied assent through continued use (browser-wrap). Courts are more skeptical of browser-wrap integrations but have upheld them when presented in formats that communicate their contractual nature. Similarly, users cannot be made to check for changes to online terms continually. Courts have determined that presenting term modifications through click-wrap formats meets the proper notice requirement. The study presented the following recommendations:

1. The avoidance of language implicative of agreement modifiability without prior notice.
2. Compliance with pre-established terms and conditions, including provisions for modifying them.
3. Providing a means for users to reject modifications by quitting the service without penalty.
4. The use of click-wrap prompts whenever dealing with non-registration websites.

The vitality of this source lies in its exploration of existing common law precedents set out by different state and federal courts of the United States. Specifically, this source analyzed precedents regarding the enforceability of modified electronic contracts based on how such alterations are presented to users. The authors intended for this article to be used by lawyers and companies wanting to electronically modify existing contractual terms and clauses. Despite this, this source compiled valuable information regarding user rights. The authors also compared traditional contract concepts to newer developments occurring in electronic spaces. Additionally, the authors cite specific case law relevant to this investigation. Such reasons present the reasoning behind incorporating this source into the present investigation. This source can help advance this investigation by providing information that aids in understanding basic contract concepts and user rights.

Examination of Privacy Disclosure and User Trust in the Consumer Internet of Things

The present source sought to propose that IoT (Internet of Things) service providers refine and adopt transparent privacy disclosure approaches. Additionally, it aimed to present a framework for testing the effectiveness of privacy disclosures in building consumers' perceptions of privacy and trust and empowering consumers to adopt IoT devices while retaining some level of privacy. Lastly, it wanted to examine user privacy and privacy issues in data collection, management, and dissemination.

Privacy can be defined as an individual's desire for greater control over the collection and dissemination of their personal information. In the privacy context, trust is the user's willingness to be vulnerable when interacting and sharing personal data with an IoT device, associated applications and services, and even connection security. A user's willingness to trust is based on their perception of the organization's trustworthiness, including their belief that the organization will not engage in opportunistic behavior with their data. IoT can be defined as a world where physical objects are seamlessly integrated into the information network and can interact and participate in business processes.

As the number of devices a user connects with increases, so does the type and amount of data collected. While this can be potentially beneficial and convenient for users, it also introduces undeniable risks to their privacy. The Privacy Calculus Theory (PCT) explains that users will disclose information or interact with systems for as long as the perceived benefits outweigh the perceived risks or consequences. There are also arguments that consumers seek benefits despite their privacy concerns and often underestimate the risk of IoT usage on their data privacy. The Protection Motivation Theory (PMT) is also utilized to explore the influence of individuals' threat and coping appraisals on their behavior. A study found that consumers' threat appraisal was significantly influenced by their general and health information privacy concerns. Lastly, the Social Contract Theory (SCT) suggests that organizations dealing with personal data enter into social contracts with users, implying that they will only use it according to social norms.

The connection of devices enabled by IoT can heighten privacy and security challenges, not least excessive monitoring and data mining techniques that may enable data to be made available for purposes for which it was not previously intended. The risk of these challenges is incremented by the extended service chains inherent in IoT of multiple actors, including software vendors, device manufacturers, network operators, cloud service providers, and underlying infrastructure. While consumers may accept a degree of consumer surveillance from the Internet or IoT, they may be equally ignorant about the degree to which their data is being distributed to fulfill their service requirements.

Several dimensions of privacy must be considered and protected, including personally identifiable information (PII), location data, footprint privacy, and data contained in queries. In terms of overcoming privacy concerns, suggestions include increasing consumers' perceptions of control, building trust, and reducing perceptions of risk. To accomplish this, organizations must transparently communicate with users and clarify their controls over their data, what data is collected, and how it is used. There is a need to both adjust the content of policies and develop methods which better inform consumers of how their information is used, such as a privacy label:

We argue that IoT service providers should draw from this recent research on privacy and trust labels to develop an IoT based privacy label. The label should seek to build consumers' understanding of how their data is used and collected to comply with privacy regulation and build positive privacy perceptions, as well as information on the organisation to build perceptions of trustworthiness. All information on the label should be framed in a manner, which demonstrates the benevolence, integrity, and competence of the IoT service provider with regards to protecting consumers' personal data…We [also], recommend the inclusion of physical privacy labels on the box of IoT devices, along with a digital label on the application presented to users at sign-up and an up to date label accessible within the application's privacy features and on the service provider's website. (Fox & Lynn, 2020, p. 132)

With IoT technologies advancing faster than privacy regulations and practices, companies must proactively address consumers' privacy concerns. Fox and Lynn's framework acknowledges that consumers have preexisting perceptions and preferences regarding privacy and trust in technologies, brands, and contexts. They argue that, in line with Social Contract Theory (SCT), the proposed label will foster perceptions of control, trustworthiness, and privacy.

The investigation of the multiple social theories behind how users decide which services to utilize and not utilize and the proposal of a privacy disclosure label are two reasons that make this source essential to this investigation. The researchers explored the Privacy Calculus Theory, the Protection Motivation Theory, and the Social Contract Theory. This source acknowledged how preexisting perceptions and biases held by individuals play an active role in their choosing to utilize the software. Additionally, the researchers explored the numerous components involved in regular Internet transactions and noted how the public is generally unaware of them and their different policies. The present source defined important terms utilized by this investigation. Such definitions will aid in advancing the investigation. This source is vital to this investigation because, utilizing the above data, it designed a framework to make privacy policies more accessible. Most notably, the researchers explored and recommended using labels —similar to nutritional labels found in food items— as a method of clearly and transparently relaying information. This framework and the invaluable research will allow this investigation to reach an informed and worthwhile conclusion.

Uninformed Assent to Terms of Service Contracts and Privacy Policies of Online Services

This source aimed to investigate the prevailing refusal to [attempt to] read and understand the privacy policies and terms of services of online networking services through registration for a fictional service called NameDrop and self-assessment. The four research questions (RQ) addressed are:

1. To what extent will participants ignore privacy and terms of service policies for the fictitious social networking service NameDrop?
2. To what extent will participants overlook "gotcha" clauses in the NameDrop policies?
3. To what extent will participants read privacy and terms of service policies for real social networking services?
4. What attitude about privacy and terms of service policies predict the extent to which participants ignore them?

"Top-down" approaches to privacy (i.e., government and policy) often draw from the "notice-and-choice" model. The notice-and-choice model was designed to put people in control of their data through self-determination and approval. Ongoing efforts to strengthen data protection continue to draw on the old 1970-era framework.

Attempts to offer data control are only meaningful when users have notice of an entity's policies and their respective rights. Unfortunately, the norm is being unfamiliar with privacy and terms of service policies. Websites like "Terms of Service; Didn't Read" and "BiggestLie.Com" acknowledge this truth alongside policymakers.

This source surveyed 543 participants to determine the extent to which individuals ignore privacy and terms of service policies upon joining a service and when they are updated. Participants were first directly assessed on their behavior while joining a fictitious social networking service, NameDrop, and later asked about their usual behavior. On the webpage, participants could either sign up directly (auto-accept) or read the privacy and terms of service policies before accepting or rejecting them. The privacy policy and terms of service texts measured 7,977 and 4,316 words, respectively. Assuming a 12th-grade reading level, each text takes around 31 and 16 minutes to read, respectively. Two "gotcha" (absurd) clauses —relating to firstborn child reassignment and government data sharing— were included to assess comprehension. The investigation found most users ignore terms of service contracts and privacy policies:

The results of this study suggest that individuals often ignore privacy and terms of service policies for social networking services. This behavior appears to be common both when signing up to new services and when policies change for services individuals are already using. When people do read policies, they often remain on the relevant pages just long enough to scroll to the 'accept' button, and in the few instances where detailed reading takes place, almost all participants demonstrate reading times far below the average reading time needed… The role of the clickwrap in facilitating policy acceptance is worth emphasizing. Of the 543 individuals surveyed, 74 percent accepted the privacy policy via the quick-join clickwrap option which allowed participants to by-pass the policy without even requiring a glimpse. (Obar & Oeldorf-Hirsch, 2018, p. 20)

Respective to the initial research questions addressed, the following was found:

1. RQ1 was measured through either the quick sign-up option or the extent read. 399 of 543 participants opted for the quick sign-up option (no agreement or policy was shown). The remaining 144 participants spent a median of 13.60 and 14.04 seconds reading the privacy and terms of service policies, respectively. 411 and 17 of 527 participants completing the self-assessment survey attested to usually and sometimes doing so, respectively. Justification trends include uninterest and inconvenience in reading them, following the collective, fear of missing out, and general hurry.
2. RQ2 was assessed through open-ended questions on NameDrop's privacy and terms of service policies. Only 83 participants showed concern about the policies, of which nine and eleven directly mentioned the first and second gotcha clauses, respectively. 98% of participants missed "gotcha clauses" related to erroneous data sharing. 17 and 37 participants rejected the privacy and terms of service policies, respectively. Seven of the nine who directly mentioned the first "gotcha" clause rejected the policies.
3. RQ3 was addressed by averaging reported time spent reading policies. A median of 2 and 2.35 minutes was reportedly spent reading privacy and terms of service policies, considering only those who did read them. Reading patterns were similar when the policies changed. Three attitude factors were identified: information overload, nothing to hide, and difficulty understanding.
4. RQ4 was answered using a hierarchical regression model for the four outcomes: reading privacy and terms of service policies at initial sign-up and when updated. The more individuals experienced information overload, the less time they reported spending reading them. Having nothing to hide and difficulty understanding did not affect reported reading behavior.

Users frequently disregard terms of service and privacy policies. Almost all participants showed reading times well below the average required reading time in the rare instances of detailed reading, even though none had ever heard of the service before and could attest to its quality. The role of quick sign-up options is also worth emphasizing. People who disapproved of the policies spent more time reading them on average, though not long enough to ensure complete comprehension.

This source conducted a study on terms of service agreements and privacy policies, information which was vital to this research paper. Specifically, this source evaluated the extent to which these are read. A total of 543 individuals were assessed to conduct the study. The investigators found that most participants did not take the appropriate time to read and thoroughly understand the agreements they were entering. This source is essential to the investigation because it provides data on habits related to reading such agreements and policies. The data extracted from this source will allow this investigation to assess alternatives to the current norm. Overall, this source is a great resource and covers the prevalence of trust over research when considering online service agreements.

Eye-Tracking Experiment Assessing How Users Interact with Privacy Policies Online

The study aimed to investigate how users read privacy policies and test the theory of status quo bias in encouraging their reading. It used an eye-tracking methodology to measure the time spent reading privacy policies and

the sections participants read most carefully. Two questions examined included the time users spend reading privacy policies and the policy sections they read most carefully.

Privacy policies are the standard method for online services to regulate user engagement and help users understand how their data is handled and stored. In the United States, online services are compelled to follow the Fair Information Practices guidelines of the Federal Trade Commission. In the European Union, online services are bound by the EU's Data Protection Directive. They outline users' rights and data-control options, setting boundaries between them and the service:

Informed users are empowered users who can better control their online engagements. They are more confident and believe in their ability to affect how websites and services use the data they collect. They are consumers who have a better chance at influencing the conduct of companies that rely on their customers' disclosure of personal information. The more users read policies, the more they are aware of the way data is used and can demand changes, more transparency and more control. The more users engage with the policy and raise concerns and demands to the company- the greater are the chances for change in service and consideration of users' demands. (Steinfeld, 2016, p. 21–22)

Despite these facts, users often ignore privacy policies; they regularly assent to such terms and policies almost automatically. As Steinfeld (2016) notes, "with the way privacy policies are being drafted and managed today, it is unreasonable to expect users to actually become informed" (Steinfeld, 2016, p. 22). Common reasons for not reading privacy policies include complexity, legal or vague language, and length. In 2008, McDonald and Cranor estimated that if all American Internet users read every privacy policy of every new website they visited, they would spend a cumulative 54 billion hours each year —or 40 minutes a day per individual. After considering the presented information, the present study generated three hypotheses (H):

1. Users asked to agree to a privacy policy presented to them by default will read it more carefully than those asked to agree to a policy not presented by default.
2. Participants who are presented with the privacy policy by default will better understand the permitted and prohibited uses of personal data as a result of spending more time reading the policy than participants who are asked to agree to a policy not presented by default.
3. Users who attribute more importance to privacy and privacy policies will read the privacy policy more carefully than users who attribute less importance to the existence of privacy policies or privacy in general.

The study measured two groups of 64 participants: one in which the privacy policy was hidden by default and another in which participants individually marked each policy clause as read. Both groups had the choice to accept or deny the 451-word privacy policy. In the first group, only 13 participants chose to read the policy and spent an average of 24.15 seconds reading it. In the second group, participants spent an average of 59.20 seconds reading the policy. The eye-tracking methodology revealed that, in six of the nine policy paragraphs, participants presented with the policy by default read much more carefully than those who were not.

Following the policy reading, participants answered six yes or no questions that tested their knowledge of the approved policy. The second group participants demonstrated a higher understanding of the policy than the first group. A general questionnaire on the topic was also administered. There was no significant correlation between participant reading time and agreement with "my privacy is important to me" or "I never provide information online unless I have to."

The researchers noted that although companies usually have no incentive to encourage users to read their policies, user demands, government officials, and activist groups may encourage companies to comply and take less desirable steps if the implications of not complying may be even less desirable.

This source investigated how users read and understand privacy policy agreements, which is vital data for the development of this research paper. This source also noted the theoretical empowerment they provide the user. Study participants were tasked with registering with a fictitious online, with only some being presented with the policy by default and made to agree to each clause individually. In order to illustrate a complete picture,

the investigators utilized eye-tracking technology to assess how users visually interact with policy pages. Users who had to consent to each clause were better informed of the policy than those who were not. This source is vital to this investigation because it provides insight into how users interact with agreement and policy pages. This investigation does recognize that the study researchers utilized a shorter-than-normal policy, which could have lessened user intimidation and encouraged reading. This source also studies a more personal method of presenting such policies with the checkbox, which this investigation can use to determine alternatives to the current norm.

Maintaining Online Privacy

The text discusses ways to protect and safeguard individuals' privacy, particularly business owners and managers. There has been discussion pertaining to a person's right to keep their personal affairs secret as early as 1890. In information security, privacy relates to protecting confidentiality, integrity, and availability of information. Privacy is concerned with data (or personal information) collection, storage, processing, and utilization. Personal information includes photos, videos, drawings, and documents.

The NIST article recommended that individuals be mindful of what they are publishing online, that they employ the use of network-level website blockers (which prevent connecting to and sharing data with specific services), that they enable the "do not track" browser setting, and the outright blocking Internet access when and where it is not necessary. The author notes the following respective to "do not track" requests:

When given the option, turn off tracking, which informs websites and browsers that you do not want to be tracked. Some websites may not work without tracking enabled. In those cases, try incognito or private mode for browsing. When you need to use a website that requires tracking, do not use a computer that has access to sensitive information. (Steele, 2021)

A similar note regarding "ad blockers" was additionally shared:

In addition to being annoying, online advertising can deliver malware to your network. Blocking advertisements greatly reduces this risk. Network level ad blockers are easier to manage, but usually more expensive than relying on individuals to add these extensions to their browsers. (Steele, 2021)

This source explored ways to protect and preserve privacy at the user level, which is an important resource for this research paper. The analysis presented in this source was made in the context of data breaches and aimed at businesses. Irrespective of this fact, the source contains information translatable to the context of this investigation. As a result, this investigation decided to integrate this source into its investigation. Preventing data from entering the Internet is one of the best ways users can protect themselves against unwanted data collection. Such initiative makes this source relevant to the research being conducted. This source helps advance this investigation by exploring alternative steps users can take to preserve online privacy.

Materials, Design & Methodology

A computer with an internet connection was utilized alongside the Mozilla Firefox Internet browser for this investigation. In order to find the sources required for this investigation, the Google search engine was paramount for pinpointing the necessary sources to elucidate the research question. Although the internet connection was unstable at times, it proved sufficient to conduct all the required constituents of this investigation. Some sources utilized were peer-reviewed, while others were not; the investigation mentor revised the sources and approved them while confirming their validity. All these components working in tandem created the optimal conditions for the consummation of this project.

The Qualtrics platform was utilized to conduct the study survey created for this investigation electronically. The survey accepted responses from individuals who have previously interacted with terms of service

agreements or privacy policies over Internet channels. Nine questions, divided into three categories —demographics, background, and research— were administered and later analyzed. The complete list of questions administered is enumerated in Appendix A. Before participants could partake in the survey answering process, they were informed of the purpose and scope of the study, the voluntary and anonymous nature of their responses, and the option to indicate their consent to participate. To distribute the survey, a URL and a QR code were generated and later distributed electronically and physically, respectively.

A mixed-method investigation approach was employed in this research paper. This investigation was completed utilizing a documentary analysis design. To populate this research, it was necessary to specify the purpose of each of the eleven sources utilized. Furthermore, it was essential to recognize the sources' design and approach, indicate the target audience, highlight their limitations, and determine the recommendations and findings contained in each. An analytical component outlining the significance of the data presented in the inquiry was generated. A quantitative survey study was conducted alongside the qualitative exploration of existing literature and research on the topic. A descriptive content analysis survey methodology had to be utilized for this investigation to accomplish the established objectives.

Results

The utilized search engine —Google Scholar— proved most useful for the selected sources of this investigation. These results will be organized by publication date (most recent to oldest); however, the number assigned to each will depend on the order in which they appear in the literature review chapter. Source six was very recent (2022) and dealt with information regarding court rulings and opinions concerning the enforceability of electronic contracts in the United States. Similarly, sources five and eleven were very recent since they were published in 2021. Respectively, they dealt with the state of data privacy laws in the United States and maintaining privacy online. Sources three (2019) and eight (2020) were published recently and, respectively, compared the privacy-first approach employed by the U.S. Postal Service to the privacy-last reality of the Internet and examined privacy disclosures and trust in consumer Internet products and services. Source nine was not recent, being published in 2018, and explored and studied uninformed assent to electronic contracts and policies. Source two, a book on Internet users and data collection and retention policies by governments and institutions, was not recent with a publication year of 2017. Likewise, sources four, seven, and ten were not recent (2016). Individually, they researched the increasing use of terms of service and privacy policies to self-regulate online services, examined the unilateral modification of electronic contracts in the U.S., and employed an eye-tracking methodology to assess how users interact with privacy policies online. Lastly, the first source, published in 2013, was also not recent; this source explored Internet milestones and privacy concerns.

The main triangulation utilized was the outline provided by the investigation mentor; in addition, a survey was administered to further expand the available data. A total of 63 individuals participated in this study survey. No notable difference between participant age or education level and time spent reading terms of service agreements or privacy policies was found. Similarly, no notable difference between self-assessed technological literacy and time spent reading terms and policies was found. Eleven participants indicated they did not either know what either terms of services or what privacy policies were. Most participants —79% and 81%— indicated spending less than a minute reading terms of service agreements and privacy policies, respectively.

Length of text ranked first amongst the reasons against reading agreements and policies. The complexity of the text followed second, with the use of legal or vague language next, existing trust in the service, accessibility of the terms and policies, knowing others who already use the service, and another reason ranking last. Other reasons include using similar language amongst policies, needing to accept terms and policies and giving up some privacy to participate in the modern world, and the repetitive and numbing nature of reading terms and policies. Several participants noted the perceived need to accept terms and policies —giving up some privacy in the process— as a consequence of modern society.

During the early stages of the investigation, the main question was:

1. "How versed is the average Internet user in terms of service contracts and privacy policies?"
    - The sections labeled "Uninformed Assent to Terms of Service Contracts and Privacy Policies of Online Services" and "Eye-Tracking Experiment Assessing How Users Interact with Privacy Policies Online," alongside the data collected from the research survey conducted by this investigation, primarily answered this question. The average user is aware of the existence of terms of service contracts and privacy policies yet chooses to forego the reading burden.

As more evidence was collected, an additional question was generated to define further the variables of this investigation (online privacy, data control, terms of service, privacy policy):

2. "What legal statutes protect Internet users from predatory terms of service and privacy policy clauses?"
    - The sections labeled "Increasing Use of Terms of Service Contracts to Self-Regulate Online Services," "Data Privacy Laws in the U.S. and the Importance of Enacting Such Legislation," "Law and Court Ruling on the Enforceability of Electronic Contracts in the U.S.," and "Law and Court Rulings on the Unilateral Modification of Electronic Contracts in the U.S." satisfactorily answered this question. The federative nature of the U.S. permits the existence of varying statutes within different jurisdictions. Certain data types —including health, financial, and educational— are federally protected under specific circumstances; however, no statute regulating general data collection, retention, use, or distribution exists. In regard to specific states, some have taken the initiative to enact such legislation within their borders. The Federal Trade Commission (FTC) is responsible for investigating service violations of their own terms and policies.

The answer constructed led to the third question:

3. "What can be done to make terms of service contracts and privacy policies more accessible and understandable for the average user?"
    - The sections labeled "Increasing Use of Terms of Service Contracts to Self-Regulate Online Services," "Data Privacy Laws in the U.S. and the Importance of Enacting Such Legislation," "Examination of Privacy Disclosure and User Trust in the Consumer Internet of Things," "Uninformed Assent to Terms of Service Contracts and Privacy Policies Online," and "Eye-Tracking Experiment Assessing How Users Interact with Privacy Policies Online," alongside the data collected from the research survey conducted by this investigation, best answered this question. Amongst the recommendations, the following can be found: study impact of terms and policies, promote transparency, involve government institutions, and incentivize user-friendly terms; make data collection functions opt-in by default; utilize labels and videos; improve visual and textual readability; and lower the reading burden.

These recommendations helped formulate the fourth and final question:

4. "What can be done to make data privacy protections more accessible to the average Internet user?"
    - The sources "Increasing Use of Terms of Service Contracts to Self-Regulate Online Services," "Examination of Privacy Disclosure and User Trust in the Consumer Internet of Things," and "Data Privacy Laws in the U.S. and the Importance of Enacting Such Legislation" were able to answer the presented question. Some of the suggestions include making data collection functions opt-in by default, limiting data collection to the bare minimum, provisioning for the private right to sue, creating rule enforcement mechanisms, preventing discrimination against those who exercise their rights, promoting research relating to online privacy.

Discussion & Conclusion

The Internet has exponentially evolved from its original conceptualization as a decentralized communications tool. It was originally a place free of government oversight and rules. As a consequence of the ever-increasing number of intermediaries, services, and platforms integrating themselves into the Internet structure, the Internet has become a hyper-regulated environment. Internet services can unilaterally define contractual clauses, modify them at personal discretion, and enforce them. Internet services can collect, process, store, share, and sell personal and non-personal data. Internet services can define alternative dispute resolutions, like arbitration, and prevent class-action lawsuits. Internet services can accomplish all of this through Terms of Service contracts and Privacy Policies. Terms of service contracts are the primary device utilized to delineate service terms, rules, and policies online. Privacy policies, which exist within terms of service contracts, further regulate the collection, utilization, storage, sharing, selling, and control of data. Despite the incredible importance of reading and understanding these contractual terms, Internet users seldom read them; in fact, reading them is the anomaly.

There exists historical precedence on the prioritization of privacy in data transmission systems. The U.S. Postal Service is an amazing example of a service that has valued and continues to value user privacy in its operations. Data collection is not inherently bad. In fact, it is data that has allowed human society to advance. It is important, however, to permit the individual user to exercise control over their own data. Choosing to share data —and not being made to reject sharing data— should be the norm. Data collection should be limited to the bare minimum necessary to provide a service. Users should be able to control how their data is used, retained, and shared.

This research paper found it important to ascertain why Internet users opt to forego reading terms of service contracts and privacy policies despite claiming to value privacy. Research demonstrated that not showing terms and policies by default is a primary factor in this. The overwhelming nature of the texts is also a contributing factor. Both researchers and Internet users recommend making the texts more accessible, summarizing information, increasing readability and comprehensibility, reducing legal and vague terminology, including infographics and videos, and promoting transparency. Some participants of this paper's study noted the perceived need to accept terms and policies —giving up some privacy in the process— being a consequence of modern society.

This research paper also determined contextualizing the legal nature under which terms of service contracts operate to be essential. The articles noted that many of the ways Internet users are presented these terms and privacy policies are not enough to satisfy the requirements to form contracts; only when users directly interact with them does this occur. Similarly, the articles noted that unilateral modification of these terms and policies generally cannot form binding contracts. It is important to note that judicial opinions vary between different jurisdictions of the United States. Concentrating on privacy policies specifically, no singular federal law regulates general data privacy; however, there are multiple laws regulating specific types of data under specific transactions. While some states have enacted their own statutes, this number is little, they only apply to their residents, and they follow no standard.

In the absence of national regulations preventing extensive data collection practices, Internet users can and should adopt measures to reduce the amount of data they send out. Adhering to the motif of digital permanence is vital. Being mindful of what one publishes, using network-level website and advertisement blockers, enabling "do not track" browser request, and disconnecting from the Internet when the connection is not needed are some steps Internet users can take to better protect themselves and their data online.

Considering the limitations outlined in the preceding chapter, this research paper recommends employing a case study methodology to research terms of service and privacy policy interactions, making sure to diversity participant populations. Additionally, this paper recommends expanding on the literature concerning the importance of protecting privacy online and the importance of user data control. Ultimately, this investigation aimed to explore the predatory practices behind terms of service contracts and privacy policies. Sources

converged to provide an answer: the lack of legal protections towards Internet users —in addition to their own willful and unwilful ignorance— permits the existence of the current normative.

Limitations

For the investigation to come to fruition, the scope of the research question had to be more encompassing to find more information on the subject, which permitted the optimal conditions to answer the research question. If the original research question had not been changed, perhaps the essay would not have been written as well, given that the research question would have been challenging to complete. There were additional internal threats that had to be mitigated in order to preserve the internal validity of the investigation, such as changing various sources that did not meet the quality threshold to correctly elucidate the problem surrounding the conducted research.

Moreover, there were multiple external threats that had to be addressed to preserve the external validity of the inquiry, such as the instability of the institution's Internet connection, a limited database, and swapping of research investigation devices. Additional limitations include the plurality of survey participants belonging to the 0-16 and 17-24 age brackets, the survey distribution mainly occurring in a local private school, and 14 unfinished survey submissions.

Acknowledgments

I would like to thank my advisor for the valuable insight provided to me on this topic.

References

Belli, L. & Venturini, J. (2016). Private ordering and the rise of terms of service as cyber-regulation. *Internet Policy Review*, 5(4). https://doi.org/10.14763/2016.4.441

Cohen-Almagor, R. (2013). Internet History. *Moral, Ethical, and Social Dilemmas in the Age of Technology*, 19–39. https://doi.org/10.4018/978-1-4666-2931-8.ch002

Eboch, M. M. (2017). *Big Data and Privacy Rights* (Ser. Essential Library of the Information Age). Abdo Publishing.

Folks, A. (2024, January 26). *US State Privacy Legislation Tracker*. International Association of Privacy Professionals. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Fox, G., & Lynn, T. G. (2020). Examining privacy disclosure and trust in the consumer Internet of things: An integrated research framework. *The Cloud-to-Thing Continuum*, 123–140. https://doi.org/10.1007/978-3-030-41110-7_7

Husain, O. (2023, March 21). Terms of Service vs Terms of Use vs Terms and Conditions: Identical? *Enzuzo*. https://www.enzuzo.com/blog/terms-of-service-vs-terms-of-use-vs-terms-and-conditions

Klosowski, T. (2021, September 6). The state of consumer data privacy laws in the US (and why it matters). *The New York Times Wirecutter*. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Lovendale, R., & Lam, K. V. (2022, August 10). Recent court decisions shed light on enforceability of electronic contracts in the U.S. *Goodwin*. https://www.goodwinlaw.com/en/insights/publications/2022/08/08_10-recent-court-decisions-shed-light

Merriam-Webster. (n.d.). Terms of service. In *Merriam-Webster.com dictionary*. Retrieved February 1, 2024, from https://www.merriam-webster.com/dictionary/terms%20of%20service

Moringiello, J. M., & Ottaviani, J. E. (2016, May 20). Online contracts: We may modify these terms at any time, right? *American Bar Association*. https://www.americanbar.org/groups/business_law/resources/business-law-today/2016-may/online-contracts/

Nechushtai, E. (2019). Making Messages Private: The Formation of Postal Privacy and Its Relevance for Digital Surveillance. *Information & Culture*, 54(2), 133–158. https://doi.org/10.7560/ic54201

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *SSRN Electronic Journal*, 1–20. https://doi.org/10.2139/ssrn.2757465

Schwartz, P. M., & Solove, D. (2009). Notice and Choice: Implications for Digital Marketing to Youth. *Berkeley Media Studies Group*. https://www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf

Steele, M. (2021, May 28). Maintaining your online privacy. *National Institute of Standards and Technology*. https://www.nist.gov/blogs/manufacturing-innovation-blog/maintaining-your-online-privacy

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior*, *55*, 992–1000. https://doi.org/10.1016/j.chb.2015.09.038