CSEC 793 Capstone in Computing Security
Project Report

# PROTECTING CONSUMER DATA: WHAT CAN BE DONE?

April 8, 2024

Dani Saba
Department of Cybersecurity
College of Computing and Information Sciences
Rochester Institute of Technology
dls8878@rit.edu

# 1 Abstract

With the internet growing and transforming the way companies do business, consumers can get lost in online transactions, terms of use, and privacy policies. The research for this project is based on work done that proves privacy policies are complex, consumers do not understand what companies are doing with their data, and consumers are not aware of their options to opt out of data sharing. This capstone project aims to discuss the regulations put into place to protect consumers, what to look for in privacy policies to help consumers take control of their data, and shows an example of how to make this information available to consumers to spread awareness of these options with a proof-of-concept website that showcases how to make this information available to the general public in an easy-to-digest format.

# 2 Introduction

Corporate privacy policies are known to be long, complex, hard to read, and hard to digest, even if they follow regulations and privacy policy standards. This leads to the average consumer being confused as to how their information will be collected, stored, and shared when they use a service or access a website. This can lead to organizations having less business and less consumer trust due to a lack of clarity from businesses and a lack of understanding from consumers. In research done by Earp, et. al [1] they discuss how privacy policies are too "convoluted" and hard to understand, which is also backed by research done by Vail et. al [2], in which it is shown that the majority of the U.S. population does not have a high enough technical ability to be able to fully digest privacy policies and understand the legal language and technical terminology. This is a huge problem since users look towards privacy policies as a measure of how much trust they should have in an organization, looking for ways their information is used and their information is secured is a starting point for most individuals looking to use a service [3].

Consumers should be able to read a privacy policy and understand the rights and expectations they have regarding the use of their information, how many people can access their information, how their information is secured, and how the promises in privacy policies are enforced. This can be done by educating users on opt-out procedures and regulations companies have to follow regarding consumer data. The following paper will discuss the literature that inspired this work, regulations that companies have to follow regarding consumer data, example opt-out procedures found in privacy policies online, and will go through a proof-of-concept website that will provide availability for people to see this research in a more understandable format.

By arming consumers with the knowledge to protect their data, they can make informed decisions about where they shop online, what services they use, and what can be done to minimize their internet presence and online footprint. Minimizing confusion over these complicated policies that consumers cannot understand is the starting point for creating

more digital literacy for the average internet user when it comes to complicated policies that determine how their data will be used and how much they should trust a service. Consumers will be able to understand their rights and company obligations and have a little more peace of mind about what they can do to have any control over their data.

## 3 Definitions

| | |
|---|---|
| Data Controller | "The natural or legal person, public authority, agency, or other body which...determines the purposes and means of the processing of personal data..." [4]. This means the data controller is the person who collects your data and decides the 'why' and 'how' personal data is processed |
| Data Subject | A data subject is the person whose data is being collected and processed |
| Data Processing | The collection and manipulation of data |
| Rectification | the action of putting something right. In the context of this paper, it refers to data rectification, which means correcting information that was collected and is wrong |
| Erasure | Securely and permanently deleting |
| Restriction of Processing | Limiting the way an organization uses a consumer's data |
| Minimum Use Disclosure | The minimum amount necessary to achieve the purpose for which it is being used, requested, or disclosed |
| Data Portability | Allows individuals to obtain and reuse their personal data for their own purposes across different services |
| Child | A person under 13 years old |

## 4 Literature Review

As time continues, more regulations are introduced that change the scope of data collection and what privacy policies need to be included in them, however, privacy policies do not get any clearer. It is a common theme in all of the reviewed literature that privacy policies are hard to read, complicated, or decrease consumer trust in a service because of lack of clarity. Therefore, research has been done as to what makes a good privacy policy, how privacy policies can be changed to promote better readability, and why people do not understand privacy policies. However, there has been no attempt to address the problem of information

available to the people, and how they can protect their data. Therefore, the works that will be explored in this paper serve the purpose of further emphasizing the importance of the research done during this capstone and show how this work should be continued in the future to promote consumer rights and data.

## 4.1 How Unreadable Are Privacy Policies?

In *An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies* by M. Vail et. al, it is explained that the majority of privacy policies require an average reading level of a sophomore in college. Although people indeed possess this reading level [5], in an article by Madison Dapcevich, she writes that it is true most Americans have a reading comprehension level under their educational level [6]. Although the work done by Vail et. al is quite old, the education level of American people has not changed an extreme amount and they still read below their educational level, which backs the work done in this paper and shows that people cannot comprehend the legal terms and long-winded explanations in privacy policies. The study performed by Vail et. al proves that privacy policies could be formatted in an easier-to-read format through a study comparing typical privacy policies and privacy policies that are presented in alternative formats. In an interesting turn, almost all participants found the alternative privacy policies to be easier to read but trusted the typical privacy policies more, because they were more familiar to them. This is an interesting study that shows privacy policies could be written clearer in the future, and consumers could be directed towards opt-in/opt-out procedures, as well as categorize important information for ease of access to them.

In *Examining Internet Privacy Policies Within the Context of User Privacy Values* by J.B. Earp, et. al, it is said that privacy policies could be better tailored towards customer interests to influence how much business the organization gets [1]. By this, it is meant that consumers have different needs when it comes to privacy values, and if those were reflected more in policies, a consumer would be more likely to use that service. This study goes on to figure out what the most important aspects of websites are to consumers, concluding that company name, opt-out information, and privacy policies were what raised trust in services for consumers. This backs the research that is done in this capstone by proving that privacy policies and opt-out information are important to consumers by emphasizing in the paper that consumers want information about security, data collection, and consent in their policies. This study will be built on by showing where users can find that information, and what regulations are enforced when it comes to the security of their information.

In previous works exploring privacy policies, another important detail that is pointed out is that users do not actually know where their information goes after it is given away. In a journal article by J. Rapp et. al, she expresses that few consumers actually know how widespread their data is after they give it away, which is disastrous to protecting consumer privacy [7]. She also states that this problem is exacerbated by long privacy disclosures, which consumers do not want to read, and thus do not understand fully what is happening

with their data. This leads to consumers being scared about what is happening with their data, and fearing the online profiles businesses manage to capture and create using browsing data, previous purchase information, and website clicks from the consumer.

## 4.2 Consumer Trust and Perception of Privacy

Building off of research about the readability of privacy policies, many authors go on to talk about how consumer interests and trust shape the way consumers view companies and services, and what privacy policies can do to increase trust for consumers. These works are important to this study because it goes to show that consumers value specific aspects of privacy policies, and if they do not see what they value reflected in the privacy policy, they will not use a service. For example, in *The Role of Privacy Policy on Consumers' Perceived Privacy* by Y. Chang et. al, it is said that consumers generally trust a service or website more if there is the option to opt out of information sharing since it puts a choice into the consumer's hand [8] [7]. Consumers generally trust services more when they see that they have a choice in whether their data gets shared, who it gets shared to, and how their data gets used [1]. In another survey done by Kuang-Wen et. al, it was said that people would be more willing to provide information online if they knew their information would not be misused, showing a correlation between willingness to provide personal information and privacy concerns [3].

Through all of the studies that go into consumer trust and privacy perceptions, the end line is that consumers are more likely to use a service if they have a guarantee their information will be protected, usually through some enforcement. Chang says that "enforcement has the strongest effect on perceived effectiveness of privacy policy, followed by access, notice, and security" [8]. They also mention that enforcement clauses show consumers assurance that their data will be safe, through some guarantee of an action that will be taken to secure their information. This follows the U.S. Federal Trade Commission's five principles of fair information practice, which were shown by Kuang-Wen et. al to be utilized in the creation of most privacy policies, which are as follows: notice, choice, access, security, and enforcement. These are all also values that align with consumer values in websites and policies.

## 4.3 Regulations and How They Impact Privacy Policies

The California Privacy Rights Act (CPRA), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and more regulations continue to impact the way privacy policies are written and what information is contained inside of them. In a work done by Anton et. al, it is explained that privacy policies were complex and hard to read *before* the introduction of regulation, and regulation only served to make privacy policies more complex, with the added bonus of ensured security [9]. It was also explained that the enactment of HIPAA and transparency about data practices in

privacy policies can make websites more susceptible to data breaches. In another work by Linden, it is shown that after the enactment of the GDPR, privacy policies became longer but covered the same content, meaning that it went more in depth on the same topics as before the GDPR, probably to try to ensure deeper understanding [10].

After the introduction of regulation, it was shown that many privacy policy languages did not account for regulation, making four out of 18 researched language types capable [11]. Out of these four, it was shown that three of them were extremely similar to each other as they built off of one another. This research goes to show that many privacy policies are built using language that is not compliant to regulation. This research also concludes that only the four compliant languages should be further researched into to find out ways to empower users to enforce privacy policy preferences. This study, done by Leicht and Heisel, is good groundwork into formalizing privacy policy language to make it more understandable by the public. However, that is unfortunately out of scope for the capstone research done in this paper.

### 4.4 Solutions

Unfortunately, most of the research into privacy policies and regulations done by previous studies goes to show the flaws within policies and why consumers do not understand the language used in policies, but does not venture out into finding possible solutions. It is all research done to point out how they could be improved, while making minimal claims as to what would help consumers understand better. One possible solution is to organize information in privacy policies by categories, another is to explain privacy policies in terms of "goal statements" where the goals are laid out plainly [2]. Lee concluded in his study that people themselves do not know what they would want in privacy policies, being torn between strict and flexible policies and not knowing whether they would want legislation involved to help normalize privacy policies [12].

One interesting solution that was explored was not to change privacy policies, but to give consumers a tool that could help them calculate the privacy risk associated with releasing specific information from a consumer, along with the probability of this risk occurring [13]. This work is ongoing, but seems like it could be an interesting solution to enable consumers to protect their privacy. Though it is worth noting that this solution quantifies risks associated with data, which could be a flawed way of assessing risk and create inaccurate measurements. It would be interesting to see this work continue and see how this could help consumers, as it is a tool that helps solve the issue of availability in privacy solutions for consumers. This relates to the capstone research done in this paper as well as it describes available solutions to consumer privacy protection which will be explored.

By showing consumers what their rights are, it will help provide them with a basis for their trust in services and websites, and help give them a better internet posture when looking at privacy policies. As well as this, it is important that consumers know what information they can control. By showing them opt-in and opt-out procedures and where

they can be found, it will assist consumers with having a starting point to go off of when reading policies or browsing websites to find the opt-outs that are commonly hidden, and will help them have control over their data. Finally, the proof-of-concept website will put it all together in a more available platform. Without previous works to find the flaws in privacy policies and why consumers trust them, this capstone project would not have the groundwork to build off of.

# 5 Regulations

Regulations are laws that are put into place by a regulatory agency or government to determine a set of requirements for specific issues. In this section, regulations that impact data collection and privacy policies will be examined and the requirements they put into place to protect consumers and their data will be explained.

## 5.1 GDPR

The GDPR (General Data Protection Regulation) is a regulation about information privacy that was created in the European Union and applies to any company that does business in the European Union. This regulation is one of the most prominent online human rights laws because it has been relevant since its passing date on May 25, 2016. It proposes seven principles: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. In the scope of this research, only the principles which cover data collection will be explored.

### 5.1.1 Data Controller Responsibilities

In the GDPR, data controllers have responsibilities laid out that they are required to follow to create a safer environment for consumers. One of these requirements is to create and maintain a privacy policy to inform customers about how companies handle their personal data. This ties in very closely with the controller's requirement to be transparent regarding the communication of the rights of data subjects. Typically this is done within a privacy policy, which is why they are often lengthy. Another requirement of the controller that often shows up in privacy policies is that the controller must provide information about where personal data is collected from the data subject, and what data is explicitly not collected. It is the responsibility of the controller to show that the data subject has consented to the processing of their data and to make the data subject aware that they can withdraw this consent at any time. Lastly, when it comes to data handling, the data controller must communicate the rectification of data, erasure of data, or any restriction of processing [4].

### 5.1.2 Consumer Rights

Data subjects have explicit rights granted to them under the power of the GDPR. These rights are the right to obtain the data the controller has concerning them, the right to complete incomplete data obtained by the controller, the right to erase data concerning them, the right to restrict processing of the data, and the right to object to the processing of personal data. Some of these rights are conditional, meaning they have conditions to fulfill before the data subject can enact this right. Processing restriction can only be done if the data is inaccurate, the data subject does not want to erase the data, the controller no longer needs the data but is required to keep it (i.e. legal reasons), or the data subject has objected to the processing on legitimate grounds. Objecting to processing can only be done if the processing is for marketing, profiling, a task carried out in the public interest, or the data subject's legitimate interests. Specific reasons for objecting to processing must be given [4].

## 5.2 HIPAA

HIPAA (The Health Insurance Portability and Accountability Act) is a federal regulation that was signed into effect on August 21, 1996, and applies to specifically electronic patient health information. HIPAA covers health plans, health care providers, and health care clearinghouses, but does not cover life insurers, employers, workers compensation carriers, schools, state agencies (i.e. child protection services), law enforcement agencies, and municipal offices. The HIPAA privacy rule is the rule that sets the standards for protecting health information, its use, and disclosure. The health information that is covered includes medical records, treatment conversations, information about health insurance within computer systems, billing information at clinics, and other health information held about the data subject online [9].

### 5.2.1 Data Controller Responsibilities

Explicit data controller responsibilities include implementing minimum use disclosure and having procedures in place to limit access to patient health information. Data controllers need to explicitly state that health information cannot be used or shared without the data subject's written permission unless HIPAA allows it. HIPAA only allows people to look at electronic patient health information if it is to help with treatment, help with payment, help family members or relatives who are involved with the patient's care, make sure doctors can give the best care they can, protect the public health (i.e. reporting when there is a flu), or make reports to the police [9].

### 5.2.2 Consumer Rights

The privacy rule of HIPAA gives people the right to see their health records, have corrections made to the data, receive notice about how the health information is being used or shared, and get reports on when and why the health information was shared. It also allows patients the right to give permission before any health information about them can be used or shared for certain purposes (i.e. marketing) [9].

## 5.3 COPPA

COPPA, or the Children's Online Privacy Protection Act, was enacted on October 21, 1988. This act is a federal law that imposes requirements on websites that collect data on children. Some companies get around COPPA by banning children from their service, so that they do not have to worry about complying with the regulations.

### 5.3.1 Data Controller Responsibilities

This act makes it unlawful for websites or online services to collect and maintain personal information about children. The data controller must provide notice (usually through a privacy policy or terms of service) about what data it collects from children, how it uses the information, how it discloses the information to other parties (if applicable), and if there are any changes made to the policy for collection/use/disclosure. It is the responsibility of the data controller to provide notice and obtain parental consent prior to the collection, use, or disclosure of personal information from a child. The notice must be written clearly and easy to understand. Companies must ensure that there is a means for parents to view the personal information collected and refuse to permit the use of the data. It is explicitly written in COPPA that the notice needs to include a hyperlink to the online notice of its information practices, a place for parents to provide consent, and a notice that the parent's contact information will be deleted if the parent does not provide consent. It is also the data controller's responsibility to delete children's personal information after it is no longer necessary to keep, and to ensure the confidentiality, security, and integrity of the data collected from children is protected [14].

### 5.3.2 Consumer Rights

Parents of children have the right to review information provided by their children, can permit the use or future collection of information on their child, and direct the data controllers to erase the personal information collected from the child.

## 5.4 GLBA

GLBA (The Gramm-leach Bliley Act) was enacted on November 12, 1999 and was an act that reformed the financial services industry by addressing the privacy of consumer

personal financial information. Enforcement of this act is conducted by the Federal Trade Commission and other government agencies such as the Consumer Financial Protection Bureau. This law applies to businesses that are "significantly engaged" in providing financial services to consumers, including debt collectors, real estate appraisers, car dealers, higher education institutes, and more [15].

### 5.4.1 Data Controller Responsibilities

Financial institutions are required to give notice of their privacy policies to their customers annually, before disclosing any financial information to third parties, and must allow the consumers to opt-out from disclosure to the third parties. They also must tell their customers about their information-sharing practices. Account numbers are not allowed to be shared for marketing purposes. Data controllers may only obtain financial information legally and are prohibited from obtaining information by false pretenses [15].

## 5.5 NY DFS 500/23 NYCRR 500

The NYCRR 500 (New York Codes, Rules, and Regulations) is a document that covers cybersecurity requirements for financial services and financial institutions. It most recently had amendments on November 1, 2023, which added data retention regulations. Covered entities include state-chartered banks, licensed lenders, private bankers, foreign banks operating in New York, mortgage companies, and insurance companies [16]. While this regulation is more on the technical side and calls for cybersecurity controls rather than privacy policies and regulations specific to data collection, use, and disposal, it is still important in that the regulations protect New York's financial services industry against data breaches and cyber-attacks.

### 5.5.1 Data Controller Responsibilities

Under the NYCRR 500, risk assessments are required for customer data privacy to ensure that the data is safe and privacy is being maintained. It requires policies and procedures to be developed for the secure disposal of nonpublic information that becomes unnecessary for business operations. It also requires written policies to be developed for data governance, classification and retention, customer data privacy, and third-party service provider management for the sake of consumer safety [17].

## 5.6 CCPA and CPRA

The CCPA (California Consumer Privacy Act) is a California state statute that was created to improve the privacy rights and consumer protection for residents of California and was enacted on June 28, 2018. It was followed by the CPRA (California Privacy Rights Act) which was enacted on November 3, 2020, and improves on the CCPA.

### 5.6.1 CCPA

The CCPA applies to businesses that have annual gross revenues in excess of $25 million, buy, receive, or sell the personal information of 50,000 or more consumers, or derive 50% or more of annual revenues from selling the personal information of consumers. The CCPA included the right to know what personal information is collected, how it is used and sold, the right to delete personal information held by businesses and business providers, the right to opt out of the sale of their personal information, and the right to withdraw consent at any time. It also included that people under the age of 16 can only opt in with consent, and children can only opt in with parental permission. There is also a right to non-discrimination if a customer exercises a privacy right within the CCPA, meaning that a business cannot raise prices for someone just because they opted out of the sale of their information. Businesses are required to provide a "do not sell my info" link and must respond to requests without delay [18].

### 5.6.2 CPRA

The CPRA built off of the CCPA in a few ways. First, it increased the power of the right to deletion and requires that when a deletion request is received, data controllers must notify third parties that have the shared information and instruct them to comply with the deletion request as well. It also adds a new category for "sensitive personal information" which includes social security, IDs, passport numbers, driver's licenses, account log-ins, geolocation data, and financial accounts, which are all classified as "personal information" in the CCPA [19].

The CPRA also adds the right to correction of information, the right to limit the sensitive personal information collected, the right to access their information, the right to opt out, and the right to data portability. Consumers can request personal information, collection sources, collection purposes, what third parties have access to their personal information, and information that has been corrected, if any. Businesses have to clearly inform consumers about how they collect and use personal information and how they can exercise their rights, can only collect personal information for legitimate disclosed purposes, collect relevant information, and take reasonable precautions to protect consumer's personal information from security breaches. It also has similar clauses to the CCPA, such as not penalizing consumers for enacting their rights, and providing easily accessible ways to request their information, delete it, correct it, or opt out of its sale [19].

## 5.7 How Does This Protect Consumers?

With acts such as these in place, people have the option to protect their privacy and digital footprint. It is easier for consumers to request their data be deleted from many services and websites, and can opt out of data collection or sale of their data if they are equipped with the knowledge that those options are available to them. By opting out and deleting

online personal data, consumers can be more protected against information getting into the wrong hands, such as financial information, account logins, home addresses, names of relatives or children, and so forth. Consumers are also armed with the knowledge that they always have the right to check how their information is being used, which leads to easier determining what services a consumer wants to become a customer of. Protecting this information is getting more important as the internet transforms the lives of many consumers daily and more people are figuring out how to tap into the potential of online data to mine information about consumers and their habits and use this data maliciously. Regulations are put into place to protect the privacy of consumers, and it is important to use these available regulatory practices to protect themselves and their data.

## 6 Privacy Policies

A privacy policy is a policy developed by companies and data collectors to explain how they plan to use any personal information that is collected through the service or website. These are mandated by many federal and state laws, which protect consumer privacy by regulating the explicit and clear explanation of any collection, use, sharing, modification, and deletion of data a service or company performs. Most of the time, these can be found at the bottom of a website in small text as a hyperlink.

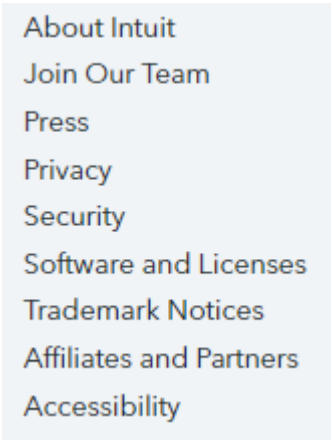



Figure 1: Intuit Privacy Policy Hyperlink
[20]

Clicking these hyperlinks will bring consumers to a page with the privacy policy. In the privacy policy, a consumer can expect to see an overview, of what information the company collects, how they collect it, how the information is shared, how to exercise privacy rights, links to opt-out or data deletion, and more details about contact information, policy changes, and more. The layout will vary from company to company, from policies with

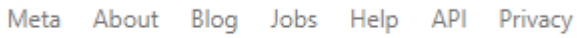



Figure 2: Meta Privacy Policy Hyperlink
[21]

images and drop-down menus to a wall of text that might be hard to decipher. For example, below it can be seen that Instagram and TurboTax prefer to have their privacy policies done in drop-down menus to make it easier for a consumer to find what they are looking for.

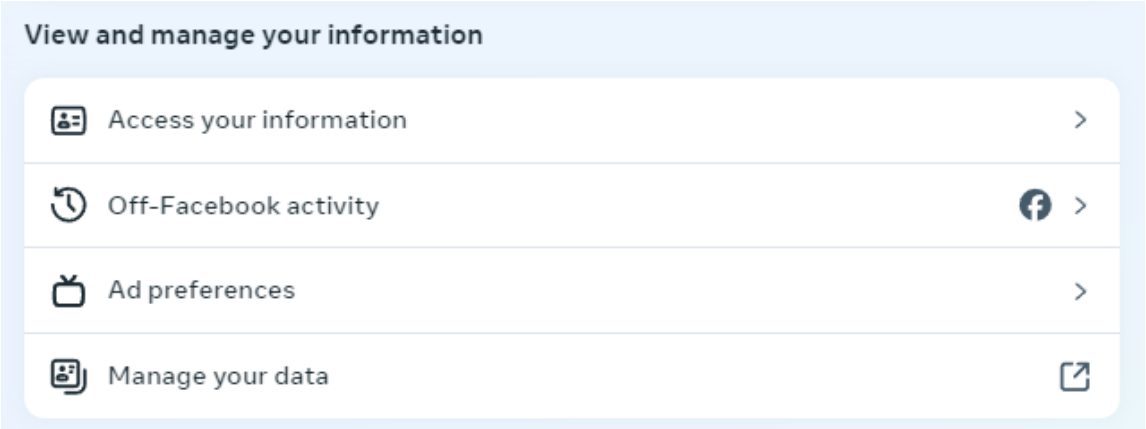



Figure 3: Instagram Privacy Policy Data Viewing
[21]

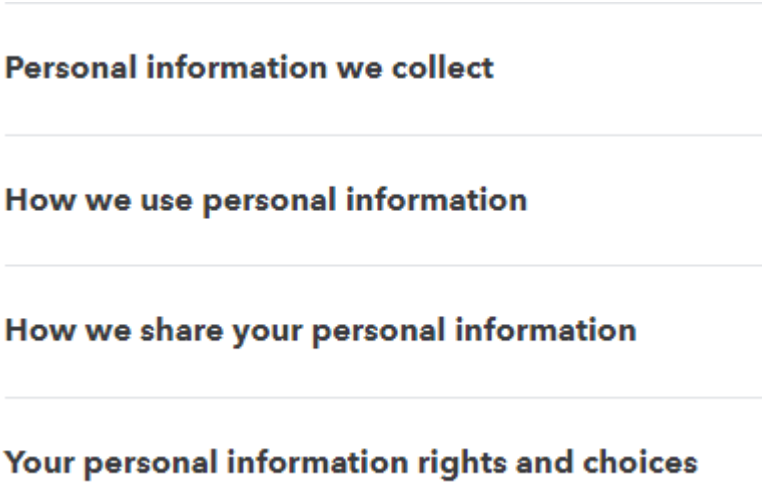



Figure 4: TurboTax Privacy Policy Data Viewing
[20]

Other companies prefer to have their privacy policies as a wall of text on a page rather than in a more readable format like in the figures above. However, if a consumer knows what they are looking for, privacy policies become less daunting and easier to navigate. Even if the privacy policy is lengthy, it is still required to be clear about what information it collects and how to delete data and explicitly state that opting out is an option that is available for consumers. The importance of explaining regulations and consumer rights is so that consumers will be able to use this knowledge to search privacy policies effectively and exercise these rights.

### 6.0.1 What Is A Consumer Looking For?

For a consumer looking to take control of their data, they should aim to look at any opt-out procedures they can and data deletion practices. One of the best ways to do this is to just search the privacy policy for words containing "opt-in", "opt-out", "delete", "deletion", or other keywords that will lead the consumer to exactly what they want to look at. This works because no matter the service, a consumer will have rights that are explicitly stated and the consumer will be able to exercise these rights. For example, the data control sections of the privacy policies for Instagram, TruePeopleSearch, and TurboTax are shown below. These services are all completely different, being a social media platform, data broker, and tax assistant, but they are all required to have information on opt-out procedures and data deletion.

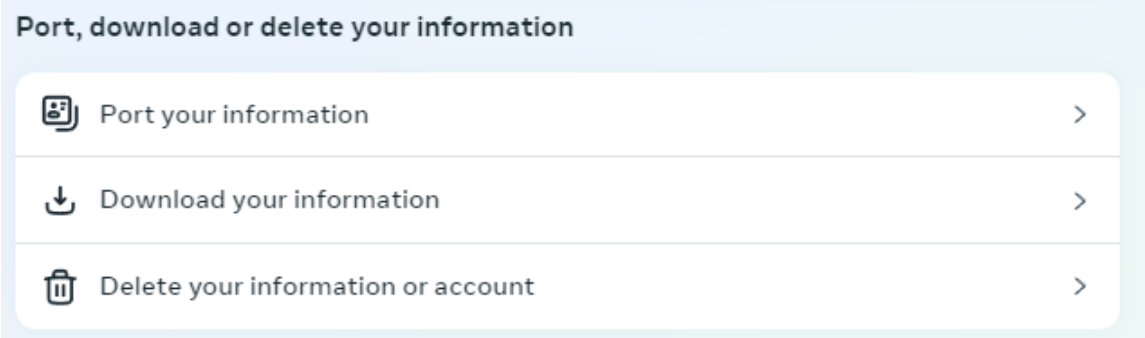



Figure 5: Instagram Information Disposal
[21]

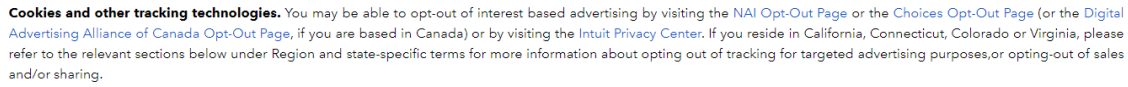



Figure 6: Intuit Opt-Out
[20]

**Advertising Opt-out:** As a consumer, you have choices as how we handle personal information related to your activities on the website. You have a choice to opt-out from the digital advertising data that is gathered during your visit by visiting http://optout.aboutads.info/ . Please note, your personal information content and advertising opt-out are handled differently and are separate activities initiated by the consumer.

Figure 7: TruePeopleSearch Advertising Opt-Out
[22]

**Delete** : Upon request we can block the records we have control over in our database from being shown on our Applications. You can request for your personal information to be blocked from being searched using the link below. Unless otherwise required by law, we will only accept opt-out requests directly from the individual whose information is being opted-out and we reserve the right to require verification of identity and reject opt-out requests in our sole discretion. Of course we are unable to remove any information about you from databases operated by third parties. We may need you to provide additional information to verify your request, such as providing data elements so that we can confirm they match the information already maintained by us. We will not use this additional information for anything other than handling your request. We do not accept opt-out requests via fax or mail. To manage or remove your public records from our database, please go to https://www.truepeoplesearch.com/removal . Please note that changes you request may not be effective immediately. Note that despite any request for removal of personal information, we may need to retain certain information for recordkeeping purposes and there may also be residual information that will remain within our databases and other records, which will not be removed or changed.

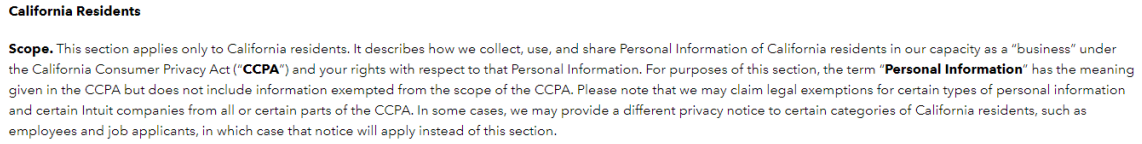
Figure 8: TruePeopleSearch Data Deletion
[22]

By finding these options, a consumer can delete their information from a data broker website, delete all the information associated with an old social media account, or make sure their financial information does not become public in a data breach. It can be seen that data deletion and management is an extremely powerful tool that consumers can use to keep control over their data and internet footprint. By exercising these rights, consumers can make sure the internet holds as little information about them as possible.

### 6.0.2 Regulations In Privacy Policies

Most regulations state that privacy policies are a requirement, however, most privacy policies will also have sections dependent on privacy per state, region, or age. This is because an online service does business everywhere, so it has to make sure it caters to all of the privacy laws for each region it does business in. This can be seen in TurboTax's privacy

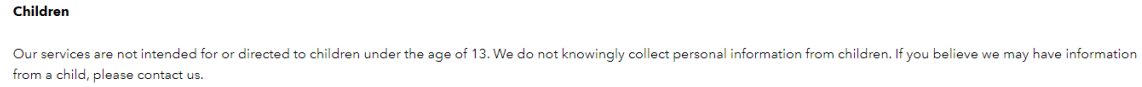
policy, for example, where they cover their bases when it comes to CCPA, COPPA, and since it is a financial company it covers GLBA as well.



**California Residents**

**Scope.** This section applies only to California residents. It describes how we collect, use, and share Personal Information of California residents in our capacity as a "business" under the California Consumer Privacy Act ("**CCPA**") and your rights with respect to that Personal Information. For purposes of this section, the term "**Personal Information**" has the meaning given in the CCPA but does not include information exempted from the scope of the CCPA. Please note that we may claim legal exemptions for certain types of personal information and certain Intuit companies from all or certain parts of the CCPA. In some cases, we may provide a different privacy notice to certain categories of California residents, such as employees and job applicants, in which case that notice will apply instead of this section.

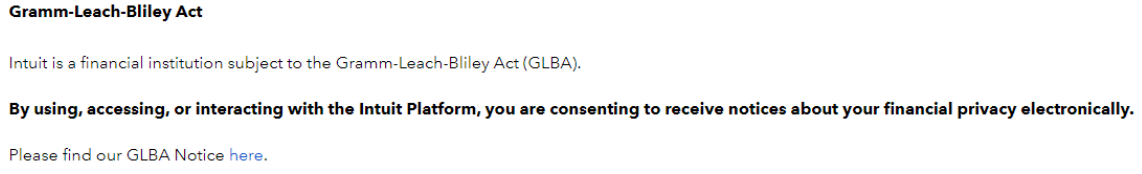
Figure 9: Intuit CCPA
[20]



**Children**

Our services are not intended for or directed to children under the age of 13. We do not knowingly collect personal information from children. If you believe we may have information from a child, please contact us.

Figure 10: Intuit Information On Children Notice
[20]



**Gramm-Leach-Bliley Act**

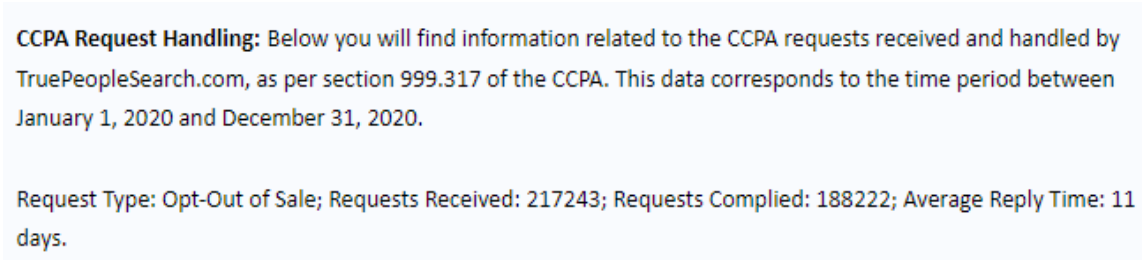
Intuit is a financial institution subject to the Gramm-Leach-Bliley Act (GLBA).

**By using, accessing, or interacting with the Intuit Platform, you are consenting to receive notices about your financial privacy electronically.**

Please find our GLBA Notice here.

Figure 11: Intuit GLBA
[20]

TruePeopleSearch also covers CCPA requests, COPPA, and the "Do Not Sell My Info" link that was covered by CCPA in its privacy policy as seen in the figures below.



**CCPA Request Handling:** Below you will find information related to the CCPA requests received and handled by TruePeopleSearch.com, as per section 999.317 of the CCPA. This data corresponds to the time period between January 1, 2020 and December 31, 2020.

Request Type: Opt-Out of Sale; Requests Received: 217243; Requests Complied: 188222; Average Reply Time: 11 days.

Figure 12: TruePeopleSearch CCPA Handling
[22]

**Opt-Out:** You have the right to opt out of the sale of your personal information to third parties. From January 1, 2020, you can exercise this right through the "Do Not Sell My Personal Information" link in the footer of our Applications . We do not sell the personal information of minors. Please note that a request to opt-out is, in effect, a request to have your profile removed from the Services.

Figure 13: TruePeopleSearch COPPA and "Do Not Sell My Info"
[22]

Through this, it can be seen that privacy policies cover all of their bases when it comes to regulations, making sure to include regulations that impact consumers in different locations, and ensuring that it provides clear notice of opt-out procedures and data collection/handling. Consumers should know their state-to-state rights since residents of different states have different regulations and requirements when it comes to privacy. They may be able to search for and enact these rights within these sections of privacy policies that go over specific state residents or specific regulations and requirements. Exercising consumer rights can decrease the risk of harm from a data breach, decrease the results returned from searches of the data subject online, and protect data that is exposed from using an online service. As well as this, consumers will be able to search a privacy policy to find how their data is being used, and can use those metrics to make more informed decisions about what services they use and how they use those services.

## 7 Awareness and Usability

To promote awareness of consumer rights, a website was created which can be found at https://consumerprivacy.cs.house/. This website was designed to help show consumers the contents of this paper in a more usable and less daunting format. With the creation of this website, the goal was that more consumers would recognize their rights when it came to privacy because they had a helpful resource to reference if they were confused about their rights or how to search a privacy policy to find the correct procedures they wish to participate in. This website is a proof of concept, so it is not a perfect example of what someone should make to promote this, but rather a demonstrational piece used to showcase how someone might go about making this information more public and readable.

First, you will find the landing page of the website. This page includes a brief overview of the project and research questions to be answered, as well as why the website itself is important. At the top left of every page is the tabs bar, where consumers can click through regulations, privacy policy, and the paper tab to find different information which will be covered below.


Figure 14: Website Landing Page


Figure 15: Website Tab Bar

At https://consumerprivacy.cs.house/regulations.html, the regulations that are covered in this paper are listed in a bulleted and easy-to-read format where you can click on the regulation to get more information, and it is all summarized neatly. As well as this, links to the regulation are listed so consumers can read the regulation or search for specific rights that were covered in the paper.

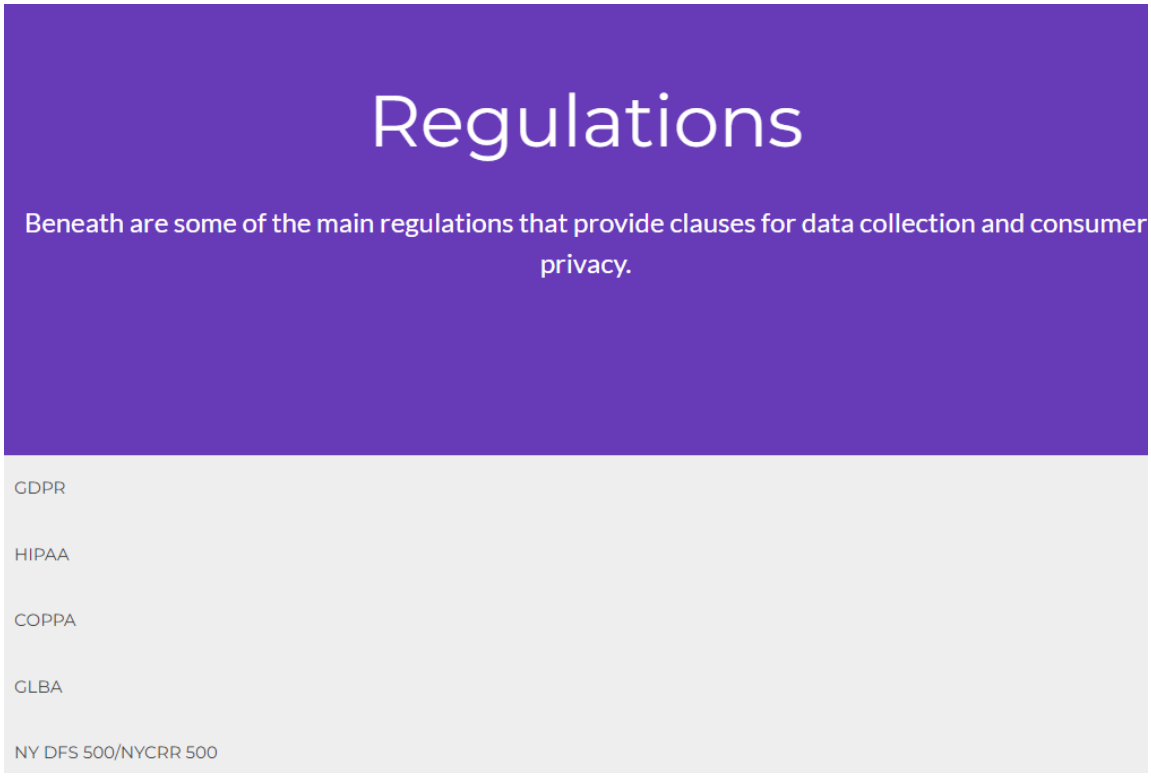



Figure 16: Regulations Landing Page

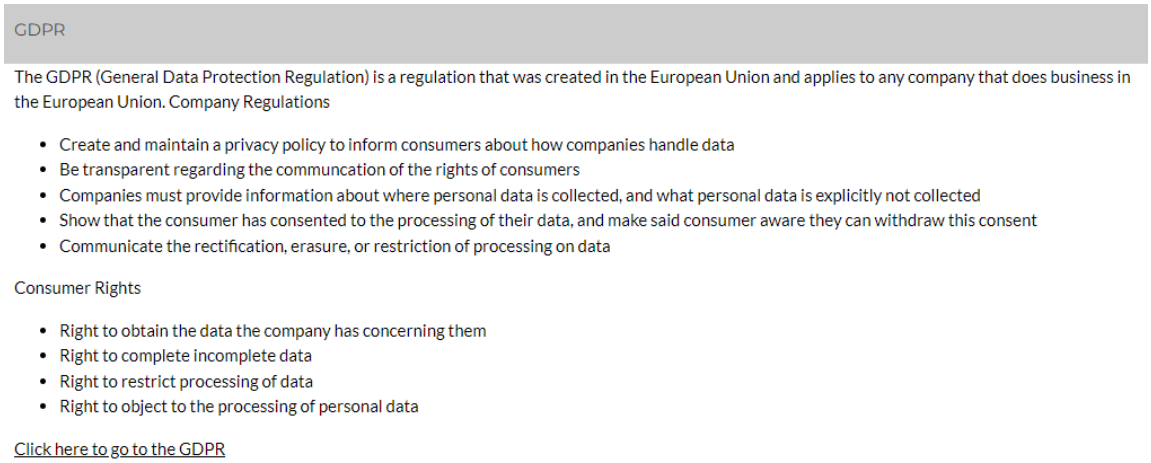



Figure 17: Opened Regulation Accordion

At https://consumerprivacy.cs.house/privacy.html, consumers can find information about privacy policy opt-out procedures and examples. This tab explains why privacy policies are important, where to look for in privacy policies to find applicable rights and the example images that were explained in section 6.


Figure 18: Privacy Policy Landing Page

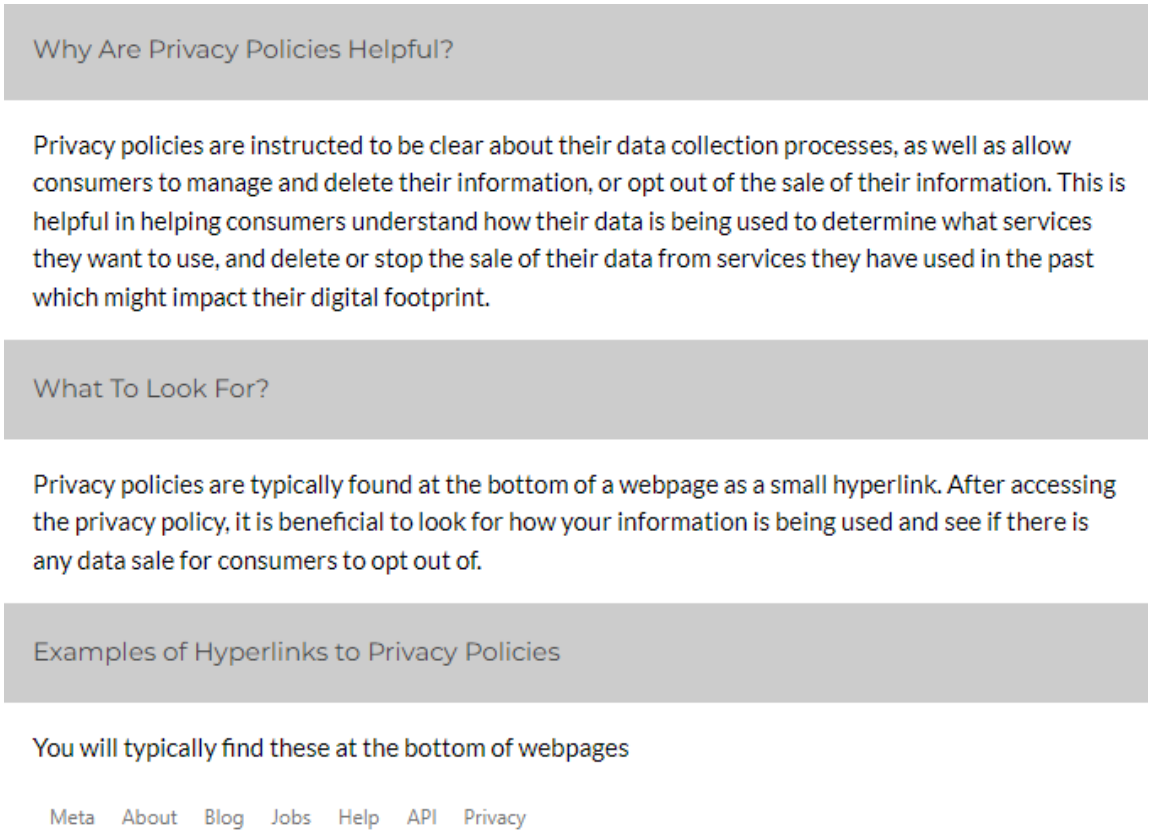



Figure 19: Opened Privacy Policy Accordions

Lastly, there is a page where website visitors can download and read the paper for themselves, either by downloading the paper or scrolling down to find an embedded PDF that they can read at https://consumerprivacy.cs.house/paper.html. This is an important addition so consumers can fact-check all of their information through the proper avenues, the paper itself, and the regulations.

This website will be covered more in future works.

# 8 Conclusion

Drawing to a close, it is instrumentally important to give consumers an idea of what control they have over their data online. Throughout this work, the aim was to discuss some of the major regulations that protected consumer privacy and gave them control over their data and discuss where consumers can find these controls within privacy policies. By arming consumers with the knowledge to opt out of the sale of their data and to delete their data

where appropriate, they can protect themselves from the dangers of data breaches, account compromises, and having a traceable digital footprint.

It was shown that regulations protect consumer data by requiring notice of how companies use the data, allowing consumers the ability to give and withdraw consent for data collection and sale, allowing consumers to restrict data processing, deleting data once it is no longer necessary, and more. These regulations can be found at the state and federal levels, with most states having some privacy law to protect consumers and their sensitive information. Regulations are extremely important in laying the groundwork for companies to build off and make consumers feel safe, and these laws have inspired the creation of other laws, such as the CPRA building off of the CCPA to protect Californian safety as best they can. the CPRA states that California has an interest in mandating laws that allow consumers to understand how their information is being used and for what purpose, by adding disclosures around data management practices [19]. It is the hope that more states will follow suit to protect consumer privacy as best they can.

It was also explained where to find opt-out and data deletion practices in privacy policies, by examining privacy policies such as those from Intuit, Meta, and TruePeopleSearch. These privacy policies are used as examples to showcase how even in different websites and services, most are required to have data deletion practices and opt-out procedures, and all of them are required to talk about the use of consumer data. By showing a social media platform, tax platform, and data broker platform, a wide range of services has been covered to provide consumers with the best idea of where they can find these practices and what different privacy policies will look like.

## 9 Future Works

If this project had a longer time frame, something that could be accomplished with the additional time would be to improve upon the website. As it is strictly a proof-of-concept, it is not the most readable or user-friendly. It would be a nice improvement to fix the styling of the website to make the information more readable, as currently, the limitation of the website is that it is the paper in a bullet point format.

In the future, it would be interesting to do more research on how we can create more awareness and visibility for this issue. the main facet of this project was discovering the ways consumers can be in control of their own data and detailing consumer rights. Now following this, the proof-of-concept website was created (https://consumerprivacy.cs.house/) to help promote this issue and provide awareness and an aspect of usability. To continue this research would be extremely beneficial. Finding out ways to provide consumers with easily accessible information about their rights is incredibly important, and even improving on and promoting the website would be an easy project to take on in the future to continue this research and make sure it reaches people. With more time, the next step of this research would be to perform a survey to discover how well consumers can understand the proof

of concept website that was created at https://consumerprivacy.cs.house/ and to see if consumers would use such tools if they were widespread and available for use. The results of this survey could power the future work laid out here.

Another project that would be interesting to see would be if it is possible to standardize privacy policies and make them simpler for consumers, as work has been done detailing why privacy policies are complicated and demonstrations of standardization options for privacy policies have been promoted in the past. It would be incredible if privacy policies could be standardized for the sake of consumer clarity because although the content of many of them is similar based on regulations, they are all laid out differently which can cause confusion among consumers.

## 10 Acknowledgment

I would like to thank my advisor Viviane Stover and my professor Dr. Sumita Mishra for their guidance and I appreciate the support from my peers.

## References

[1] J. Earp, A. Anton, L. Aiman-Smith, and W. Stufflebeam, "Examining internet privacy policies within the context of user privacy values," *IEEE Transactions on Engineering Management*, vol. 52, no. 2, pp. 227–237, 2005.

[2] M. W. Vail, J. B. Earp, and A. I. Anton, "An empirical study of consumer perceptions and comprehension of web site privacy policies," *IEEE Transactions on Engineering Management*, vol. 55, no. 3, pp. 442–454, 2008.

[3] K.-W. Wu, S. Y. Huang, D. C. Yen, and I. Popova, "The effect of online privacy policy on consumer privacy concern and trust," *Computers in Human Behavior*, vol. 28, no. 3, pp. 889–897, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747563211002767

[4] intersoft consulting. General data protection regulation. [Online]. Available: https://gdpr-info.eu/

[5] K. Barrett. (2023) Census bureau releases new educational attainment data. [Online]. Available: https://www.census.gov/newsroom/press-releases/2023/educational-attainment-data.html

[6] M. Dapcevich. (2022) Do more than half of americans read below 6th-grade level? [Online]. Available: https://www.snopes.com/news/2022/08/02/us-literacy-rate/

[7] J. G. Justine Rapp, Ronald Paul Hill and R. M. Wilson, "Advertising and consumer privacy," *Journal of Advertising*, vol. 38, no. 4, pp. 51–61, 2009. [Online]. Available: https://doi.org/10.2753/JOA0091-3367380404

[8] Y. Chang, S. F. Wong, C. F. Libaque-Saenz, and H. Lee, "The role of privacy policy on consumersâ perceived privacy," *Government Information Quarterly*, vol. 35, no. 3, pp. 445–459, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0740624X17301946

[9] A. I. Anton, J. B. Earp, M. W. Vail, N. Jain, C. M. Gheen, and J. M. Frink, "HIPAA's effect on web site privacy policies," *IEEE Security & Privacy*, vol. 5, no. 1, pp. 45–52, 2007.

[10] T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz, "The privacy policy landscape after the GDPR," in *Proceedings on Privacy Enhancing Technologies*, 2020, pp. 47–64.

[11] J. Leicht and M. Heisel, "A survey on privacy policy languages: Expressiveness concerning data protection regulations," in *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, 2019, pp. 1–6.

[12] B. LEE, "Users' perspective on regulation to protect privacy on the web," *The International Information Library Review*, vol. 32, no. 3, pp. 379–402, 2000. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1057231700901528

[13] M. Barhamgi, M. Yang, C.-M. Yu, Y. Yu, A. K. Bandara, D. Benslimane, and B. Nuseibeh, "Enabling end-users to protect their privacy," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ser. ASIA CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 905â907. [Online]. Available: https://doi.org/10.1145/3052973.3055154

[14] C. of Federal Regulations. (2024) Children's online privacy protection rule. [Online]. Available: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

[15] F. T. Commission. Gramm-leach-bliley act. [Online]. Available: https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act

[16] N. Y. S. D. O. F. SERVICES, "Cybersecurity requirements for financial services companies," https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500$_0$.*pdf*.

[17] N. Y. STATE, "Second amendment to 23 nycrr 500," https://www.dfs.ny.gov/system/files/documents/2023/12/rf23$_n$*ycrr*$_p$*art*$_5$00$_a$*mend*02$_2$0231101.*pdf*.

[18] C. P. P. Agency. California consumer privacy act regulations. [Online]. Available: https://cppa.ca.gov/regulations/pdf/cppa$_r$*egs.pdf*

[19] snowjake. (2020) The california privacy rights act of 2020. [Online]. Available: https://thecpra.org/

[20] Intuit global privacy statement. [Online]. Available: https://www.intuit.com/privacy/statement/

[21] Privacy policy. [Online]. Available: https://privacycenter.instagram.com/policy/

[22] Truepeoplesearch privacy policy. [Online]. Available: https://www.truepeoplesearch.com/privacy