Investigating COPPA Notification Compliance

Are App Developers Ensuring Compliance for the Sake of Children’s Privacy?

Mark Brom, Lydia Esbaum, Evan Lemker, Peter Mertka, Sebastian Rivera

ABSTRACT

In 1998, the United States Congress passed the Children’s Online Privacy Protection Act (COPPA), the first bill of its kind that addressed the need to protect the privacy of children. Due to their age, it is crucial that regulation provides some sort of rules and guidance as to what can and cannot be collected from children who are often more susceptible to marketing targeted ads resulting from data collection. COPPA itself requires many different practices be followed by those who collect children’s information, with our study focusing on the notification of collection via an entity’s privacy policy.

In order to comply with what is stated in COPPA’s regulations, three things must be displayed somewhere on a website regarding the data collection of children. First, there must be some sort of contact information, including name, address, phone number, and email address of either all parties collecting data, or of one designated data monitoring officer. Second, there must be a clear description of what kinds of data is being collected from users who are thirteen years old or younger. Lastly, it is necessary that either a direct link to or a process describing how a parent can review or request deletion of their child’s data must be available.

In this study, we begin to investigate how app developers on the Google Play Store with apps directed specifically at this young age group are complying with the necessary notification requirements of COPPA. By utilizing a one-time web crawl, we collect the privacy policies of over five hundred apps that are found in the “Kids” section of the Google Play Store. Using these policies, we can analyze the content to see which portions of notification are being included and to what extent. Using our results, we can better understand just how much of this bill is being followed twenty-five years after its initial passing for a medium that did not exist during the bill’s initial passing.

KEYWORDS

COPPA, Privacy Policies, Google Play Store, Compliance

1 Introduction

On October 21st, 1998, the Children’s Online Privacy Protection act was signed into law, bringing necessary regulation and protection to reign in an ever expanding and evolving online ecosystem. The act went into effect on April 21st, 2000, allowing for commercial websites and online services to ensure compliance with all the aspects of the bill [1]. Twenty-three years later, privacy is still a hotly debated issue and has become increasingly concerning as the number of avenues to collect data expands.

One avenue that hadn’t even existed at the time of passage of the law is that of mobile applications. With the rise of smartphones, tablets, and internet of things device use over the past ten years, it has become much easier for children below the age of thirteen to not only access the internet, but to use it without supervision. With this has come a significant number of mobile applications that have been solely developed and geared towards children. With these apps, developers have the ability to collect wide swaths of information that can be leveraged for profit against the user via targeting marketing and user profiling. This practice, however, is the exact type of behavior that COPPA is designed to protect against, and thus it is necessary to evaluate and ask just how many of these developers are in compliance with the exact rulings of the law?

This question is pertinent to our world today, as new technologies continue to evolve and grow at a rapid rate that is bound to outpace our current legal constraints, so it is key that one of the most prominent and popular mediums of internet access for children is following through with the necessary compliances, as by understanding where companies and developers are failing, it will be possible to provide adequate recommendations as to how these policies can be better enforced, for both current and future technologies.

For this study, we focused on one specific mandate of COPPA, specifically mandate 312.4d. The entirety of COPPA is a large and complex document that outlines numerous requirements and regulations that applicable companies are to follow, but we felt that it would be simplest to identify some of the most explicit requirements of the act itself. By focusing on 312.4d, we can better identify compliance or the lack there of, while also taking into consideration the constraints imposed by this style of audit. A wider scope would lead to a less organized study considering the time requirements of this study. To better understand what we are investigating, it is vital to know what 312.4d says. The exact text of mandate is as follows:

**312.4d (Official Statement): *Notice on the Web site or online service.*** In addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, *and,* at each area of the Web site or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience Web site or online service that has a separate children's area must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the Web site or online service's information practices must state the following:

(1) The name, address, telephone number, and email address of all operators collecting or maintaining personal information from children through the Web site or online service. *Provided that:* The operators of a Web site or online service may list the name, address, phone number, and email address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the Web site or online service are also listed in the notice;

(2) A description of what information the operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available; how the operator uses such information; and the operator's disclosure practices for such information; and

(3) That the parent can review or have deleted the child's personal information and refuse to permit further collection or use of the child's information and state the procedures for doing so [2].

In section 312.4d, websites or online services must include the presence of clear identifiable links tied to information notices regarding children on the site’s home or other landing pages. Each site needs three components: contact information of those collecting the data (names, address, phone number), a section stating what is being collected, and a section devoted to the review and deletion of child’s data. Our web scrape of the Google Play Store should look for these policies and grab them from the web for further analysis. From there, our text segmentation scripts and natural language processing model will identify these three components and determine whether or not an app is in compliance with COPPA. If an app service is missing one of the three components, we can prove that the app is not fully COPPA compliant. Knowing this, we aim to answer the following research questions:

-**RQ1:** How many companies are posting the necessary data collector contact information so that parents can get into contact with the proper data authorities?

**-RQ2:** Which developers are clearly defining what is being collected of children by their applications?

**-RQ3:** What portion of companies in our dataset are providing clear and proper instruction for parents to review and delete their children’s data?

It is necessary that we analyze this compliance because there have been companies in the past that have not followed through on these regulations, thus making it incredibly difficult for parents to assert necessary control and judgement on behalf of their child [3]. The ability to review and understand what sort of information is being collected from your children is one that is vital to ensuring that companies remain accountable to the regulations COPPA provides.

In order to answer these questions, we utilized a three-step process that is able to crawl various sections of the Google Play Store’s “Kids” section. Firstly, we acquire the content of various children’s applications’ webpages from the Google Play Store website. From there, each page’s results is scraped to isolate the company’s directly posted privacy policy thanks to Google Play’s built in privacy policy tab listed underneath each developer’s contact information. From there, each policy is split into manageable one to three sentence chunks so that it can be properly classified by our natural language model. Lastly, each chunk is parsed by a combination of pattern matching expressions and our model in order to directly state to what degree are companies complying with each aspect of 312.4d.

Overall, our results have not been fully developed yet. We are in the process of finalizing the code that will return the final results.

2 Background

We begin our process by first reviewing prior works that have either audited similar laws or investigated different aspects of COPPA itself.

**2.1 Prior Work**

The Children’s Online Privacy Protection Act (COPPA) is a set of requirements that online services must abide by that deal with how data from children under 13 years of age is managed. The purpose of COPPA is to protect children on the Internet by regulating what personal information online services can gather, use, and share about children. COPPA also gives parents control over how their children’s personal information is gathered and shared by attaining verifiable parental consent. COPPA only applies to services that are either directed toward children under the age of 13, services that are directed to the general public but know they have collected information from children under 13, or services that know they have collected information directly from users of another online service directed to children [4].

There have been several prior studies that have analyzed COPPA and apps’ compliance with COPPA, and our group has chosen to loosely model our own project based on one of these studies, “‘Won’t Somebody Think of the Children’ Examining COPPA Compliance at Scale”. Researchers of this study created an automated evaluation framework for the privacy practices of Android apps. Specifically, the top 5,855 apps geared toward children that are governed by COPPA from Google’s Play Store in the U.S. were used in the analysis. Unlike many approaches that aim to identify potential COPPA violations but fail to do so because they do not observe actual violations or do not scale, the framework used in this study allowed researchers to supervise apps’ behaviors in real time and at scale [4].

Essentially, the methodology of the study included retrieving apps from a corpus of free, children-directed apps on the Google Play Store, running each app, and analyzing the information that was collected about each app’s access to personal information and communication to third parties. During analysis, parsing and extracting certain pieces of information, like whether an app accessed Android-guarded resources, was an automated process while obtaining other pieces of information, like checking for personal information in network transmissions, was a manual process. Similar to this approach, our group will be automating parts of our analysis as well as manually analyzing the data. We will also be using apps that are children-directed from the Google Play Store in our project, only we will be examining a mere 500 different applications. Our project complements this study by focusing on whether apps comply with a specific section of COPPA, 312.4(d) Notice on the website or online service, rather than analyzing if any section of COPPA is violated.

Another study that closely resembles the research we hope to do is "Analyzing privacy policies through syntax-driven semantic analysis of information types." This research paper focuses on creating a program that can automatically analyze hard-to-understand privacy policies and generate easy-to-understand summaries of what is being collected and shared in the policy. Our goal is similar to this as we want to create a program that can automatically analyze privacy policies to find the presence or lack of required components under COPPA regulation. While the formerly mentioned research project helps identify key concepts and categories relevant to users' privacy concerns, we aim to identify shortcomings in regulatory requirements relevant to companies covered by COPPA [5].

The researchers in this study designed a program using natural language processing techniques to perform syntax-driven semantic analysis of each part of the privacy policies. These techniques included heavily focusing on information types present in the privacy policy, such as names, email addresses, phone numbers, locations, etc., to identify what pieces of information were being used and how they were being used. Similarly, we will have critical information we will be searching for within privacy policies, such as web links, email addresses, and phone numbers. However, rather than using natural language processing only to understand what the company does with this information, we will be using it to understand whether or not these links and email addresses can be used to access the online notices and data collection contact information that is required under COPPA for companies' privacy policies to contain.

One study that does not directly apply to what we are researching but is structured in such a way that it has served as a huge basis for overall experimental design and construction of this project. Christo Wilson, a professor at Northeastern University worked closely with a student, Maggie Van Nortwick, to develop a method for testing compliance with a similar privacy law, the California Consumer Protection Act, or CPPA. In their paper, “Setting the Bar Low: Are Websites Complying With the Minimum Requirements of the CCPA?” they set out to answer a similar question as is laid our in our work: just how much are companies complying with privacy laws [6]?

In the work, Wilson and Nortwick outline a complex method of scanning the web’s top one million most popular websites to determine whether or not they were following one of the most basic requirements established by the CCPA, that being the need for a link stating “Do Not Sell My Private Information.” This relatively simple requirement gave them a way to determine clear and defined compliance within the bounds of the law so that it could be better understood just how many companies were actually following specified guidelines [6]. This exact method and question formation was a tremendous inspiration for our group’s motivation to investigate a similar question, but through the lens of COPPA. Although not covering the exact same law, the methodology of doing a web scrape before scanning the results for actual compliance of a specific mandate of the law served as a basis for our experiment.

Lastly, another research group at the University of Iowa: The Security, Privacy, and Anonymity Research Team, or SPARTA Lab is investigating a different law but via a similar method. This lab is headed by Dr. Rishab Nithyanand and is currently working on several projects related to online privacy and regulation. Within these projects, there is one aiming to analyze privacy policies just as we are for compliance with regulatory frameworks. Specifically, they use the same natural language processing guided approach we used in our research. However, instead of using it to determine compliance with COPPA, their methods are concerned with determining compliance with the California Consumer Privacy Act (CCPA). This is significant because we will be able to collaborate with members of the research team, such as Maaz Bin Musa, a Ph.D. candidate at the University of Iowa studying under the supervision of Dr. Nithyanand, in order to gain insights into the design and use of different natural language processing techniques to find the key results we are searching for.

**2.2 Applicability**

The key first question to ask before we could even begin collecting privacy policies was to understand who COPPA applied to. Thankfully, unlike some other privacy laws such as the CCPA, the text of COPPA clearly outlines who needs to be in compliance with the specifications. Per the FTC’s rules, COPPA encapsulates all websites and online services (such as mobile apps) that are directly targeted at children who are age 13 or younger. Furthermore, anyone with knowledge of collecting, using, and disclosing personal information of children is also included, even if the data is being collected from a different site [1].

Another key distinction that is necessary when it comes to identifying who COPPA applies to is that the country of origin of the website or app’s controller does not exempt them from the outlines of the law. As long as the website or service is targeted at and used by U.S. children who are 13 years old or younger, they are required to follow all necessary requirements [1]. Thankfully, this meant that our web scrape and app selection did not need to take into account whether or not the app itself was expected to comply to the law. By virtue of the app being available in the “Kids” section of the U.S. version of the Google Play Store, that application is being targeted towards U.S. children. This is because the “Kids” section is explicitly for applications that are marketed at children who are 12 years old or younger. Thus, there is no need to exclude any companies that are collected during our web scrape.

**3 Experimental Design**

In order to answer our research question, we first need to gather the data necessary for the project. To do this, we utilized a combination of a Javascript app and a python program in order to systematically grab each privacy policy from the apps that we were interested in reviewing. From there we segmented each privacy into one to three sentence chunks using various sentence detection algorithms to create a data format usable by our natural language model. Finally, we analyzed each sentence returned by our text filtering to test and see if the chunk was compliance with any of the three regulations we are scanning for. Described below is a description of the exact methods used in our study.

**3.1 Data Collection**

In order to begin such a complex problem such as classifying compliance via text, we knew that we would need to collect data that could help to train our model down the line. Essentially, predictive models depend on labeled data to tell them what a certain piece of text represents. In our case, we needed to construct a model that could identify whether or not a piece of text from a policy was meeting the specifications laid out in either section 312.4d(2) or 312.4d(3). This meant that we need data that took excerpts from real privacy policies and labeled it saying what section it was fulfilling.

This process was split evenly between all five group members, with each group taking ten privacy policies. Each individual then read through each policy to pull out any sentences that directly correlated with either of our two desired sections. This data would serve as the backbone for our model so that it could properly identify different styles of sentences that counted as compliance.

This data was then compiled into a Comma Separated Values file (csv), so that it could be parsed correctly. Each row of this file contained the company that the privacy policy excerpt was from as well as the sentence or sentences themselves that correlated with a section. It was then labeled with a class, either zero or one, with those corresponding to sections 312.4d(2) and 312.4d(3) respectively. We chose to not add section 312.4d(1) to the model as its exact specifications are not suited for model prediction. Since this part of COPPA refers to the need to post the name, email, address, and phone number of a specified data collector, we felt that these pieces of information could better be identified by using a parsing method called regular expressions. These are explained further in section 3.4.

**3.2 Web Scraping**

**3.3 Text Segmentation and Filtering**

We decided to use a library called spaCy, an open-source library for Natural Language Processing in Python in order to split up the large amount of text returned from each app’s privacy policy. This is because natural language models typically perform much better when the analyzed text is shorter. Although using spaCy is not necessary for text segmentation, it includes a lot of features that are quite nice for the process. We utilized spaCy’s load function to connect the prebuilt spaCy pipelines to our Python code. In our case, we installed the English pipeline to help with the breakdown of sentences. A pipeline is a set definition of various functions and steps that is applied to any piece of text fed to it. These functions transform the text from its original format into sentences. This step allows for our data to be normalized no matter its original format. Many privacy policies often utilize bullet points and other different text display options that would normally be unusable for the next step in our project. SpaCy is also able to differentiate parentheses, and other odd markings in the English language and sorts them into proper formats. With the pipeline, we can ensure that our model is being data that is the same, consistent format. The main goal of our text segmentation is to create chunks of three sentences that can be used by our model to analyze a company’s compliance with COPPA. Our program does this by reading each privacy policy into a basic text file, before it is processed into a spaCy object via the English pipeline. The library is able to do this via a function called “nlp”. This creates chunks of sentences from the processed text.

Once this preprocessing is done, we can then extract the sentences and embed them into a list. We do this by taking our spaCy processed list of sentences and extracting the first three sentences from the list and combine the sentences as one large string. This is then stored into a new list within our program. To avoid out-of-bounds errors, which would occur when trying to group three sentences if there are less than three remaining in the spaCy object, we implement a simple checker. The system will always attempt to chunk sentences by three until the end of the spaCy processed list. For example, if we are at the end of a list with only two remaining sentences, we will need to store the two sentences and not attempt to store an a sentence that does not exist due to it being the end of the file.

Finally, once a specific policy is parsed and segmented, it is stored into a new data frame that will contain rows of company name and policy chunk. This data is then utilized during our final step of our experiment.

**3.4 Model Creation, Parsing, and Labelling**

With the data properly retrieved and cleaned, we were able to take each privacy policy and begin classifying to what degree it was in compliance with COPPA standards. This aspect of the experiment utilizes two Python libraries called Tensorflow and BERT. These two packages allow for us to construct a model that could identify our two classes, either section 312.4d(2) or 312.4d(3) based on training data that it received from section 3.1.

This style of model, created by Google, allows for users to take one of their many pre built models and apply it to any natural language processing task via fine tuning and customization. Through this process, a user is able to provide a model much less data than usual and still see surprisingly accurate classification thanks to the base model’s knowledge and definition. From there the model works by vectorizing the text it is provided, essentially taking each word and understanding its position within each sentence and creating lines of words in an attempt to derive patterns or meaning. These vectors contain a complex encoding of each word combined with different tokens that help to identify when a sentence begins and ends. This is combined with a transformer called the WordPiece Vocabulary. This is a text transformer that is used by BERT models to actually identify each word or group of words in order to better maintain key information by understanding when certain words belong together [7].

Once the model is created, we can begin the fine-tuning process. This is done by providing the model the data collected in section 3.1. This allows it to understand what sentences should apply to each section of the law. We are also able to tell it that there should only be two classes identified. Other features that are chosen during the fine-tuning process include batch size, which is the number of inputs considered before updating the model, epochs, which are how many times the program attempts to retrain the model, and validation size, which is what percentage of data should be used to verify whether or not the model is performing as it should. We also emphasize that the model should focus on highest accuracy on the validation data, which means that the model’s priority should be to predict the labels in our validation set as accurately as possible [7].

Combining all of these choices, we are then able to generate a stable model and predict what classes texts are. The BERT library and model actually trains itself multiple times over, constantly trying to improve itself of previous results. As mentioned above, each epoch means that the program attempts to make a more accurate model than prior versions, every time focusing on predicting our validation set correctly. Once this is accomplished, text can be fed into it and it can return a classification.

It is not a simple as saying that a piece of text is either of one section or another, otherwise every single sentence chunk of a privacy policy would get classified as being in compliance with COPPA. That is why our model returns percentages instead. For each policy segment, it returns two numbers, the percent likelihood that this piece of text meets the requirements of section 312.4d(2) and the percent likelihood that the text is meeting the requirements of section 312.4d(3). This then allows us to mathematically determine whether or not a chunk truly does qualify as a compliance. These percentages can be with the range of zero to one, with sentences it is more confident in having percentages of 0.75 or greater.

Using these results, we can determine mathematically whether or not we want to actually classify text as compliant or not. Our program requires at least a fifty percent difference between the two classes in order to be deemed compliant. This is chosen for two reasons. Firstly, chunks that don’t meet either class often have percentages that are roughly equal to each other, meaning that the model cannot tell whether it is one way or the other. This ambiguity translates to a piece of text that meets neither requirement. Secondly, the requirements of COPPA that we are evaluating are relatively straightforward as to what information is needing to be present, thus it is logical to conclude that a piece of text that cannot truly be determined as either class is to vague to possibly qualify as being in compliance with COPPA. This limitation of classification is discussed in section 5.1.

Notably, our model does not interact with the first portion of COPPA that we are intending to analyze. This is because personal information is often just one instance of the required field located somewhere in the policy, thus it would be impractical to train the model to identify whether or not sentences contained this information. This is further true because we were interested to see to what extent companies are complying with 312.4d(1). This is because from our group’s own experiences during section 3.1, we discovered that it was incredibly common for privacy policies to be missing one of the four pieces of personal information: name, address, email, and phone number. Thus, we developed a simpler approach to identify compliance with this specification.

Utilizing a tool available in Python and other coding languages called regular expressions, we can write specific patterns to be matched that can identify the presence of one of these pieces of information. Using the python library re, we implemented four different regular expressions, each corresponding to one piece of data from section 314.d(1). These expressions utilize a pattern matching ability to either optionally look for or definitively target certain characteristics of text that are then returned if a match to our pattern is found. For example, our expression to identify email addresses looks for one or more characters before an at symbol, followed by one or more characters after the symbol. Thanks to the at symbol being used only for emails, we can identify any email contained in a piece of text. This style of process was repeated for name, phone number and address.

Putting this all together means that we can take any privacy policy from a company’s Google Play Store page, split it into proper sentences, and identify exact compliance levels on a company-by-company basis. In the end, we looked at each company one at a time to determine overall compliance.

**4 Analysis**

In this section, we use the results of our three different scripts combined to evaluate and answer our research questions.

**4.1 Presence of Data Collector Information**

These sections are currently blank due to the final script not being 100 percent done by this deadline. Contained within the following sections will be the results of our study as well as visualizations of said results.

**4.2 Data Collection Specifics**

**4.3 Right to Review and Delete**

**5 Discussion**

In this study, we collected the privacy policies of almost five hundred different apps that are available and marketed to children on the Google Play Store in order to determine to what degree they are in compliance with the specifications of section 312.4 of COPPA. In summary, we found that:

**-RQ1:**

**-RG2:**

**-RG3:**

Once again, this section remains blank until we have actually run our final script and improved our model’s accuracy.

**5.1 Limitations**

One of the largest limitations of this experiment is the human element. By virtue of human nature, each member of our group was going to determine what text counted as being in compliance with COPPA requirements differently from one another. This conflicting perception can only be mitigated so much by the discussion we had when collecting data during the steps described in section 3.1. Thus, since it is nearly impossible to get humans to agree on what explicitly counts as meeting the requirements, it stands to reason that a computer model will suffer the same fate since it is trained on the personal bias that each of us introduced. This means that despite our best efforts, without a more rigorously developed and larger training set, our model is limited to only being as accurate as we made it via the training data we collected.

Secondly, our web crawl could only be so effective due to various issues on certain company pages that prevented us from including it in the dataset despite our best efforts. Mainly, the two challenges faced by our web scrape was that some policies would be so poorly defined either within the HTML of the website itself or some other strange exception that it made it impossible to grab the privacy policy from that app’s website despite our best efforts. Secondly, it was not uncommon for us to discover that certain websites were blocking our crawling script entirely. This too was not surprising, as many pages have restrictions on non-human access as to be more protective over who or what is accessing their data, ironically. These two factors meant that we had fewer overall companies to evaluate our results on, which could mean that our findings could show either a higher or lower compliance rate than what was calculated.

Another limitation to this project was that it needed to be very minimal in scope in order to be feasible. COPPA is a wide ranging law that contains many different regulations that could be tested for and evaluated. Section 312.4d appeared to us as the most straightforward to evaluate thanks to how it clearly stated what information needed to be contained in a company’s privacy policy. It was also necessary that we limit the study to only one type of child marketed online service, as there exists hundreds of avenues for children to interact with different websites and services that could be collecting their data. By focusing on apps from the Google Play Store, it gave us a clear goal as to what we wanted to investigate, as well as a baseline understanding that all the data we were hoping to collect would be available all in the same place. It is very possible that future works could build off what we have created to either further investigate compliance with this section, or be applied to a different medium of children’s web access, such as websites, or recently internet of things devices.

**5.2 Recommendations**

The main point that can be taken from this study is that it is vital that we know what companies are actually complying with federal regulations and which ones are lacking. Technology is ever evolving, and it is vital that we stay on the offensive to prevent issues instead of dealing with them once it becomes too late. Thanks to our proof of concept, we believe that it would be possible for federal regulators to create a process similar to our methods in order to better check for compliance. With a larger, more refined dataset, and a more consistent definition of compliance, it is very possible that company’s policies could be screened as soon as they are posted to a service such as the Google Play Store. We hope too that this style of verification can continue as grow alongside technology, so that COPPA can continue to make a difference in protecting the online safety of children. We also desire to see further updates be made to COPPA’s contents so that it can keep with an increasing number of new avenues of data collection. With this being the twenty fifth anniversary of the original passage of COPPA, and ten years since the last comprehensive update, it is critical that lawmakers review what is currently covered in the law and amend it to meet the growing needs of consumers across the United States.

REFERENCES

[1] FEDERAL TRADE COMMISSION, 2020. Complying with COPPA: Frequently Asked Questions. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

[2] CODE OF FEDERAL REGULATIONS, 2013. Part 312 – Children’s Online Privacy Protection Rule. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

[3] O’MELVENY, 2023. FTC Obtains Record Penalties from Video Game Company Amidst Growing Privacy and Consumer Protection Enforcement Trends. http://www.omm.com/resources/alerts-and-publications/alerts/ftc-obtains-record-penalties-from-video-game-company/#:~:text=The%20US%24275%20million%20penalty,affirmative%20consent%20from%20their%20parents.

[4] REYES, I, ET AL. 2018. “Won’t Somebody Think of the Children?” Examining Coppa Compliance at Scale*. Proceedings on Privacy Enhancing Technologies vol. 2018 no. 3* 63-83.

[5] BREAUX, T.D., ET AL. 2021. Analyzing privacy policies through syntax-driven semantic analysis of information types. *Information Software and Technology vol 138*

[6] VAN NORTWICK, MAGGIE, WILSON, CHRISTO. 2022. Setting the Bar Low:  
 Are Websites Complying With the Minimum Requirements of the CCPA?

*Proceedings on Privacy Enhancing Technologies, 2022* (1), 608-628.

[7] SHEKAR, CHANDRA. 2022. *Simple Text Multi Classification Task Using Keras*

*BERT.* <https://www.analyticsvidhya.com/blog/2020/10/simple-text-multi->

classification-task-using-keras-bert/

*Conference Name:ACM Woodstock conference*

*Conference Short Name:WOODSTOCK’18*

*Conference Location:El Paso, Texas USA*

*ISBN:978-1-4503-0000-0/18/06*

*Year:2018*

*Date:June*

*Copyright Year:2018*

*Copyright Statement:rightsretained*

*DOI:10.1145/1234567890*

*RRH: F. Surname et al.*

*Price:$15.00*