A 100-Site Analysis of E-Commerce Company Privacy Policies and Data Security

CS:3640 Introduction to Networks Assignment 5

Elizabeth Elias
The University of Iowa
elizabeth-elias@uiowa.edu

Maria Gauna
The University of Iowa
maria-gauna@uiowa.edu

Madeline Harbaugh
The University of Iowa
madeline-harbaugh@uiowa.edu

Kristin To
The University of Iowa
kristin-to@uiowa.edu

Rishab Nithyanand
The University of Iowa
rishab-nithyanand@uiowa.edu

ABSTRACT

In this study, we developed a web scraper to collect privacy policy information from 100 different online shopping sites covering four categories in order to gain a better understanding of how these websites were using their visitors' data. Using this data and guided by the readings provided in the assignment description, we created and attempted to answer three research questions: (1) How many cookies are being collected by each website? (2) What is the density/readability of each policy, as measured by number of pages included? and (3) Which websites use HTTPS- only, HTTP-only, or mixed HTTP/HTTPS content? Our findings indicated that number of cookies varied widely, with the highest average found in the "Luxury Clothing" category, the densest policies (greatest average number of pages) was also found in this category, and that most sites used a mixed HTTP/HTTPS approach. These conclusions allowed us to develop hypotheses concerning the web privacy practices between categories, as well as for specific sites in our data set.

CS CONCEPTS & KEYWORDS

• Network systems→ Privacy and Data Management

• Computing methodologies→ Financial technologies, targeted advertising, cookies, usage rights and informed consent

1. INTRODUCTION

Most companies with an online presence collect information on individuals who visit their website. Some use this information to create a better user experience, tailoring ads and providing service or content recommendations. The Federal Trade Commission (FTC) is the modern enforcement agency of web privacy in the United States and is tasked with ensuring that these companies responsibly collect and store this data according to user's rights and informed consent. In the ever-evolving landscape of the Internet, this can be challenging, even without accounting for the differences in law from state to state. The creation of these laws and their enforcement is subject to frequent change, introducing discrepancies and making it possible for deceptive practices and exploitative data gathering to take root. To understand why this occurs and how it can be prevented in the future, we utilized a web scraping tool to scrape the privacy policies of 100 online shopping sites across the categories of luxury cars, technology, luxury clothing, and "fast fashion" (low-cost, low-quality clothing). Using this data, we attempt to understand how intrusive each company's data collection is, how thorough and accessible their privacy policy is, and to what extent user choice and rights are being considered.

2. RESEARCH QUESTIONS

2.1 Research Question 1 (RQ1), Research Question 2 (RQ2), and Research Question 3 (RQ3)

To guide our research, we selected three research questions based on the key findings of our class readings [2][3][4][5][6]. RQ1: How many cookies are being collected by each website? RQ2: What is the density/readability of policy, as measured by number of links included? RQ3: Which websites use HTTPS- only, HTTP-only, or mixed HTTP/HTTPS content?

2.2 Motivation & Importance

The assigned readings helped us to create our research questions, providing us with the context necessary to isolate what issues are important in today's web privacy landscape and how the businesses managing e-commerce websites respond to these issues.

We chose RQ1, in large part, because of Van Nortwick and Wilson's [5] exploration of the EU e-Privacy Directive and the General Data Protection Regulation (GDPR), which "require that data collectors receive explicit consent from people before setting cookies in their user agents or collecting personal data". Englehardt and Narayanan [2] also emphasized the impact of cookie collection by explaining how third-party trackers can share users' personally identifying information through cookie syncing (cross-platform data transferal), which can be common practice in sites' privacy agreements.

RQ2 was created as we noticed a wide variance in websites' privacy policy page count; Goldman [3] critiqued the California Consumer Privacy Act (CCPA) extensively for being too long and convoluted for the average consumer to be expected to understand, infringing on their "Right to Know". Van Nortwick and Wilson [5] underline the irony of this observation, as the CCPA mandates that businesses "provide a clear and conspicuous link on [their] Internet homepage, titled "Do Not Sell My Personal Information". It seems a reasonable assumption, then, that more pages in a policy equates to a denser and less readable agreement; we hypothesize that policies with low readability and high density are likely to have lower readership, allowing companies to extract more than the minimal necessary data from a user without alerting them to the fact.

RQ3 was chosen because, when determining the security of a website, one of the first properties that can be observed in the browser is whether the website is securing its users data. HTTPS is a more secure version of HTTP, utilizing encryption and verification. So, it prevents third parties from monitoring the interactions between web browsers and web servers and establishes secure connections. This protects users' privacy and information from being spread. Another way to determine the security of a website is to check for mixed content. Mixed content is when a secure HTTPS connection runs HTTP resources on a browser such as images or videos. Engelhardt and Narayanan [2] describe how this situation could lead to resources being blocked or a warning to appear to the user and impede the full adoption of HTTPS. Therefore, by determining if website is HTTPS-only, HTTP-only or have mixed, we can begin to verify if a website's connection is secure for users.

3. ANALYSIS AND MEASUREMENT METHODOLOGY

3.1 Privacy Policy Collection

First, we compiled a list of 100 websites we wanted to examine **(Supplementary Table 1)**. The list was to be composed of e-commerce websites across the categories of luxury cars, technology, luxury clothing, and "fast fashion" clothing. To ensure all categories were equally represented in the dataset, each category consisted of 25 different company websites. Choosing multiple categories allows us to understand how different sectors of e-commerce websites track user information. We initially used ChatGPT

to generate a list of websites and their hyperlinks. However, some of the GPT-generated sites were replaced manually due to incompatibility with our scraper.

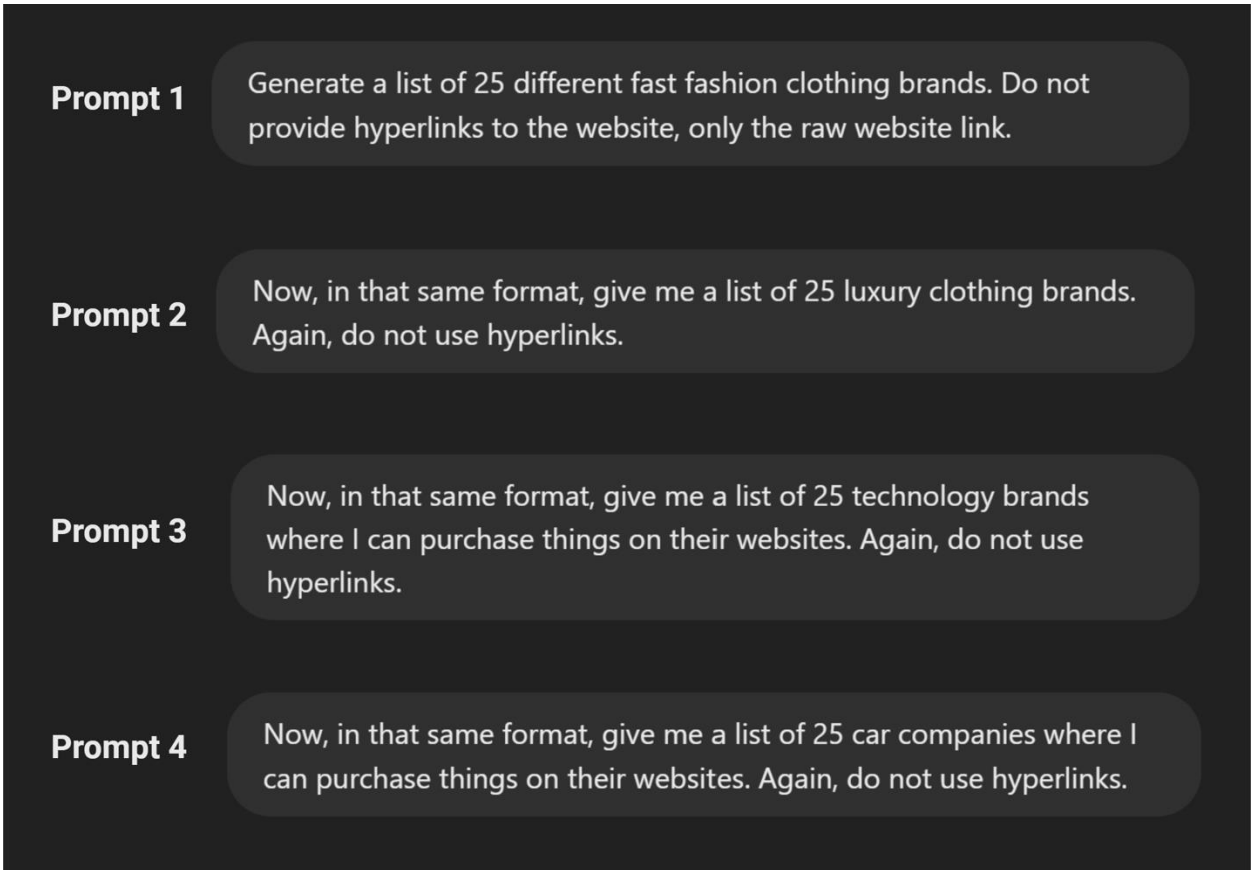


Figure 3.1.1 gives the four ChatGPT prompts used to generate the lists of websites used in this study.

A web scraper was implemented using Playwright and BeautifulSoup4[7][8] to collect the data needed for this study. Playwright was chosen to scrape the HTML file from each website due to its compatibility with JavaScript heavy websites, something many other web scraper libraries lacked. We created a custom Python script, crawler.py, in Python v3.12 that uses Playwright to simulate a Firefox browser and fetch website content. This script also contained a list of keywords, compiled in part from Van Nortwick and Wilson research [5], that we predicted would appear in any hyperlink associated with a website's privacy policy or data handling procedures **(Supplementary Table 2)**.

For each of the 100 websites in this study, the following data was collected:

- The full-page HTML file for each page.
- The number of cookies per site.
- Cookie information, which included each cookies' name, value, domain, path, expiration information, security, httpOnly status, and DNSMPI link if available.

To navigate through each website, beginning from the homepage, the crawler first extracted the HTML file from the homepage and searched for anchor <*href*> tags and tags associated with data analytics using BeautifulSoup4[8]. Using that set of tags, the links associated with each tag were compared to our list of keywords we deemed to be associated with a website's privacy policy. After collecting a list of all hyperlinks on a website's homepage, the crawler visited each link and extracted its' associated HTML content. This HTML content was inspected to identify privacy policy pages and after identifying those pages, the crawler saved the HTML content locally. Additionally, the crawler was used to identify hyperlinks associated with DNSMPI keywords. If the crawler came across such a site, the HTML information for that site was extracted as well **(Supplementary Table 3).**

The crawler also verifies for mixed content by checking if resources on a secure HTTPS site are loaded over insecure HTTP and determines if the website supports HTTPS, HTTP, or both by attempting get requests for each link under both protocols. The

crawler adds this information to the CSV file. Information on the number of cookies, cookies' information, and DNSMPI links collected earlier is also added to this CSV file. Finally, all the data for all 100 websites that was collected by the crawler was added to a CSV file to be used during our analysis.

3.2 Data Processing

Due to the format of HTML files, they are often difficult to read and obtain information from. Therefore, to ensure that our collection of DNSMPI policy information was in a human-readable format, all HTML files collected were additionally converted to a plaintext format.

3.3 Alternate Approaches

There were many open-source scraping tools available to us, so choosing the right one meant considering what kind of information we wanted to collect, how we wanted this information formatted, and what options would be most easily integrated with the language and environment we were using. The main priority was to have a relatively lightweight and fast tool, as we were limited in time due to the nature of this project.

Initially, we attempted to use PoliPy, a web scraper tool developed by the BLUES Lab at UC Berkley. However, we found this to be tool was ineffective on JavaScript-heavy websites, which may have been due to its usage of the Selenium library to scrape data from websites. As JavaScript-heavy sites have recently become more common due to their ability to handle more complex web design, it necessitated we find a tool that could handle such content [11]. This led us to Playwright, which was notable for its capability to handling JavaScript-heavy websites [10].

BeautifulSoup4 was chosen to analyze the HTML file contents as it was lightweight and easy to learn [9]. Additionally, one of the authors had previous experience with the tool, which further contributed to this decision.

In terms of analytical methodology, we could have chosen any number of different research questions to guide what data was gathered. It may have been helpful, for example, to group together fast fashion and luxury clothing into one category, as they are more similar to each other (at least in concept) than the other categories; however, we felt that their notable differences in answering our research questions differentiated them enough from each other to justify their separation.

3.4 Methodology Limitations

Although we completed this work with what we feel were the best methods available given our knowledge and the assignment specifications, we understand that it is unlikely that our work is free of limitations or unconscious bias. Firstly, the scope of our data was restricted to English or English-translatable shopping sites, the number of websites specified in the assignment, and the sites whose frameworks were compatible with the scraping tool we developed. While this was a sizeable list, it is not necessarily representative of all websites, nor all privacy policies. Additionally, we identified privacy policy links with an array of search terms. There may have been privacy policy links we missed that a website labeled using a term we did not predict, which in some cases is purposeful to leave users misinformed about how their data is being sold and shared. Finally, analysis of cookies collected by websites and how that impedes user privacy is difficult, due to the many types and classifications of cookies, with some being more intrusive than others, so we may not have captured the full scope of the privacy policy.

4. RESULTS

This data highlighted domains of many cookies that appeared on multiple websites. The domain of a fast-fashion company, Lulus (lulus.com), was found on most websites **(Figure 4.0.1)**. The websites we analyzed had an average of 22 cookies per site. Hyundai-USA had the greatest total number of cookies at 75, while Mazda-USA and Lexus had the fewest cookies **(Supplementary Figure 1)**. The most frequent cookie, named "ak_bmsc", appeared on 38 different websites, and a total of 987 unique cookies were collected **(Supplementary Table 3, Supplementary Figure 3).**

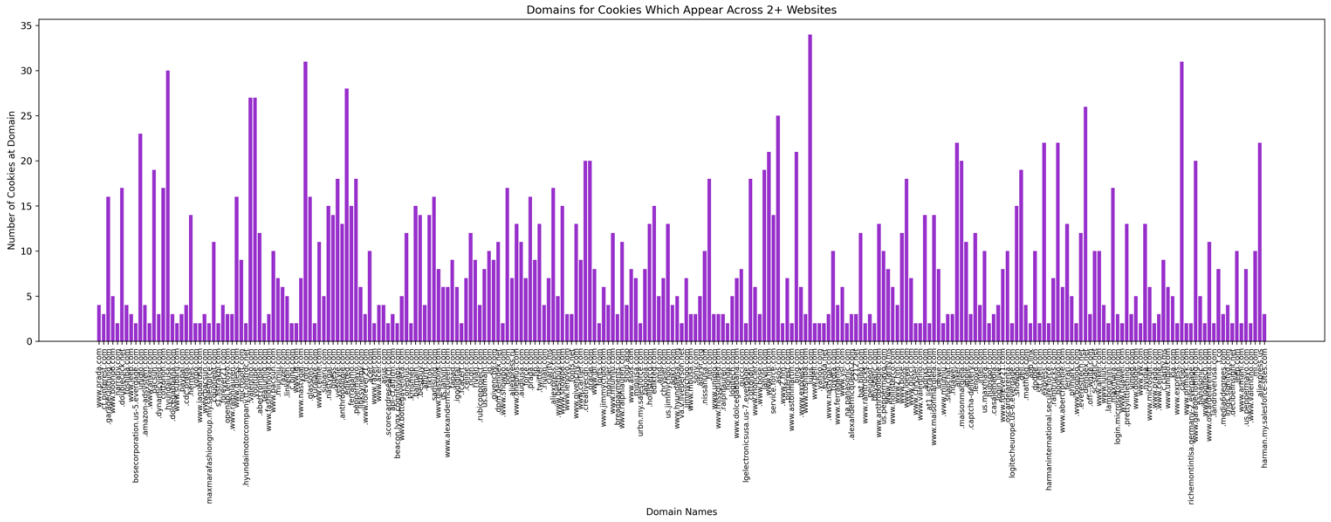


Figure 4.0.1 shows all the domains for which cookies appeared across two or more sites. The most times a cookie appeared on a domain was 75, and the mean times a cookie appeared on a domain was 21.91.

Despite having the largest range of total cookie numbers, the "Vehicles" category had the lowest average number of cookies to number of pages **(Figure 4.0.2)**. The data follows a close to linear trend, with the "Luxury Brands" category showing the highest correlation between the number of cookies and number of pages. When looking at the density of the privacy policy of each website, luxury fashion brand, Oscar De La Renta required an 18-link transversal to collect all information regarding their privacy policy. The websites with the fewest number of pages were the "Technology" brand Mi (mi.com), the "Vehicle" companies Mercedes-Benz (mbusa.com) and Mini Cooper (mini.com), and the "Luxury" Brand YSL (ysl.com), each with only 1 link transversal **(Supplementary Figure 3)**.

Furthermore, we found that more than half of the websites chosen didn't provide a DNSMPI link **(Supplementary Figure 4)**. When analyzing which websites did provide DNSMPI links, we found that "Vehicle" companies were the most likely to provide DNSMPI links, while "Technology companies were the least likely to provide them. [**Figure 4.0.3**]. However, the percentage of sites with DNSMPI links was not significantly different across any of the four categories we included in this study.

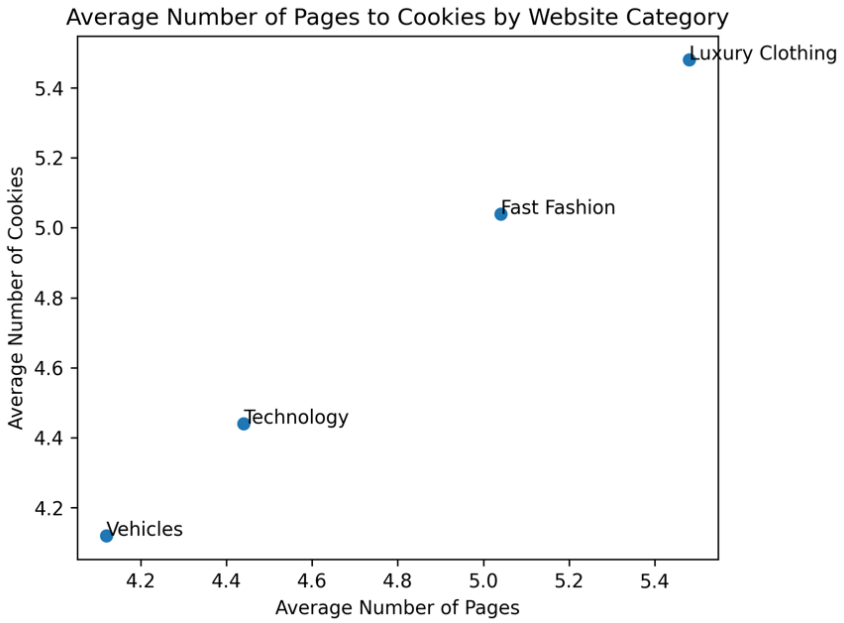


Figure 4.0.2 shows the correlation between the average number of privacy policy pages and cookies by e-commerce category. The "Vehicles" categories expressed the lowest ratio of around 4.1, while the "Luxury Clothing" ratio was the highest around 5.5. The difference between categories was fairly linear.

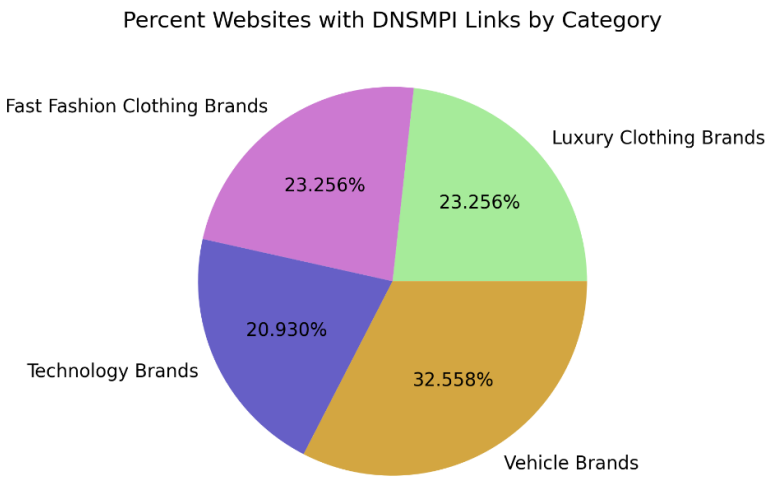


Figure 4.0.3 provides the percentage of websites in each category which contain DNSMPI links. The "Technology" category expressed the lowest fraction of around 20.93%, while the "Vehicle" category fraction was around 32.56%.

We also utilized the websites HTTP and HTTPs policies as a measure of security. Most of the websites allowed for a combination of both HTTP and HTTPS to run their website, and no websites were HTTPS-only or HTTP-only (F**igure 4.0.4B)**. Furthermore, roughly 80% of the websites in this study do not have mixed content on their websites in comparison, with only 5% of websites containing mixed content on their pages (F**igure 4.0.4A)**. However, some websites did not have their content available to us.

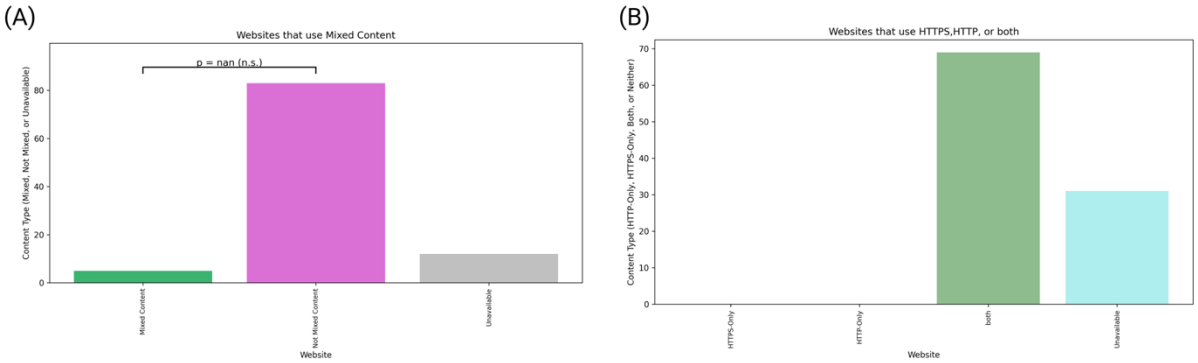


Figure 4.0.4 highlights the protocols websites use for connections with clients and other sites. (A) Represents the number of websites that allow for an HTTPS and/ or HTTP connection, where about 70 websites allow for both HTTP and HTTPS connections. (B) Shows the percentage of websites that allow mixed HTTP/HTTPS content on their website. Roughly 80% of websites did not allow mixed content on their website

5. DISCUSSION

Our web scraper and resulting data when compared between sites and between categories gave us insight into how secure companies were about user data monitoring and inform them via privacy policies and DNSMPI links. In this study, we had initially considered

that a higher number of privacy policies was associated with a more ambiguous privacy policy and a higher number of cookies was associated with a less secure site.

5.1 Number of Cookies Collected (RQ1)

While it was disconcerting that the average number of cookies found on the websites was so high, it is not unexpected. Many e-commerce sites rely on user information to promote content while users visit their site or to determine advertising strategies. However, it would be unwise to assume that all cookies being collected were associated only with the business who owns the site you were on, as our analysis found that nearly 75% of the cookies, we discovered were both not secure and not HTTP Only **(Supplementary Figure 5B, Supplementary Figure 5C).** Also, nearly a quarter of the cookies we analyzed did not expire and continued tracking user data indefinitely **(Supplementary Figure 5A)**. These types of cookies put user's personal information at risk. Shopping websites handle very important user information and data, including large volumes of payment information, and are more likely to be targeted by third parties for that information.

5.2 Number of Links Containing Privacy Policy Information (RQ2)

It was for this reason that we were surprised by our analysis of the "Luxury Brand" companies. Luxury brands were, on average, the websites with the most cookies and the most pages. Because luxury companies are required to handle large transactions, we had expected fast fashion websites would have the highest density of privacy policy pages and highest number of cookies due to them having the least expensive merchandise. This also suggests that luxury brands could be collecting more user data and obscuring their privacy policies by hiding the full policy across multiple pages. We had hypothesized that fast fashion websites would use the greatest number of cookies, as they are known to be insecure in storing customer's payment information. Additionally, the data showed that as the number of links traversed to get to the privacy policy page increased, the number of cookies increased as well. This shows that readability/density of a policy can impact the security of a website as more transversing it takes to get to the privacy policy the more at-risk users are to being exposed to third parties through cookies.

While our scraper determined that many of the websites chosen didn't have a DNSMPI link, this could have been impacted by its difficulty in locating it. This may suggest that these websites should provide a clearer and more readable version of their existing privacy policies. By making the DNSMPI link hard to locate or not providing one at all, this could indicate that a website is not particularly concerned about the privacy of their users; a concerning phenomenon considering their handling of sensitive information. This was somewhat expected, as the CPPA policy is intended to help users be more informed on how companies are handling their personal information.

5.3 Measuring Security through HTTP/HTTPS Content Information (RQ3)

We discovered that despite vehicle brands having less cookies on average and being the most likely category to provide a DNSMPI link, they made up 80% of the websites that had mixed content on their website. This may indicate that while mixed content can cause some errors or impede full HTTPS implementation, it didn't seem to have much impact on the security of the websites. Even without all websites having DNSMPI links present and utilizing potentially risky cookies, it is somewhat reassuring to see that most websites in this study chose to use the more secure HTTPS protocol in at least some cases.

Furthermore, the majority of websites implementing both HTTP and HTTPS isn't unusual as this provides flexibility and accommodation for different websites. However, it raises the important question: why implement HTTP at all if HTTPS is a more secure option? Surprisingly, the internet has not fully adopted HTTPS as the standard, nor has HTTP been entirely phased out. This is especially surprising given that shopping platforms should prioritize security to protect user data. Allowing HTTP connections could expose vulnerabilities and create opportunities for third parties to intercept sensitive information.

5.4 Wider Implications

The information gathered from this research has strong applicability and generalizability. As more and more people shop online [1], companies are responsible for correctly handling enormous amounts of data and helping consumers understand what will be done with it, given their consent. Consistent enforcement of reasonable privacy law is only possible when intelligent legislature is passed by informed citizens and protected by agencies like the FTC, which in turn need sufficient funding, authority, and organization. We expect that research on web privacy will continue to improve and not only make this possible but introduce a standard with fair and ethical practices for businesses and consumers alike.

6. DATA AND CODE AVAILABILITY

All data and code to run this project can be accessed in the following GitLab repository:
https://research-git.uiowa.edu/ecelias/cs3640

7. REFERENCES

[1] Desilver, D. (2023). Online shopping has grown rapidly in the U.S., but most sales are still in stores. [online] Pew Research Center. Available at: https://www.pewresearch.org/short-reads/2023/11/22/online-shopping-has-grown-rapidly-in-u-s-but-most-sales-are-still-in-stores/.

[2] Englehardt, S. and Narayanan, A. (2016). Online Tracking: A 1-million-site Measurement and Analysis. [online] Available at: https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf.

[3] Goldman, E. (2018). An Introduction to the California Consumer Privacy Act (CCPA). SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.3211013.

[4] Solove, D.J. and Hartzog, W. (2014). The FTC and the New Common Law of Privacy. SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.2312913.

[5] Van Nortwick, M. and Wilson, C. (2022). Setting the Bar Low: Are Websites Complying With the Minimum Requirements of the CCPA? Proceedings on Privacy Enhancing Technologies, 2022(1), pp.608–628. doi:https://doi.org/10.2478/popets-2022-0030.

[6] Zimmeck and Bellovin. "Privee: An Architecture for Automatically Analyzing Web Privacy Policies." USENIX Security Symposium, 2014. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-zimmeck.pdf

[7] PyPI. (2024). playwright. [online] Available at: https://pypi.org/project/playwright/ [Accessed 4 Dec. 2024].

[8] Richardson, L. (2019). beautifulsoup4. [online] PyPI. Available at: https://pypi.org/project/beautifulsoup4/.

[9] Birchard, T. (2018). Scrape the Web with Python & BeautifulSoup. [online] Hackers and Slackers. Available at: https://hackersandslackers.com/web-scraping-beautifulsoup/ [Accessed 4 Dec. 2024].

[10] Fimber (2024). Web Scraping With Playwright. [online] Scrape.do. Available at: https://scrape.do/blog/web-scraping-with-playwright/ [Accessed 4 Dec. 2024].

[11] Burnett, D. (2023). Should Content Take Priority on JavaScript-Heavy Sites? - AOK Marketing. [online] AOK Marketing. Available at: https://aokmarketing.com/should-content-take-priority-on-javascript-heavy-sites/ [Accessed 4 Dec. 2024].

Supplementary Information

Supplementary Table 1

Category	Website	Category	Website	Category	Website	Category	Website
Luxury Fashion	www.gucci.com	**Fast Fashion**	www.asos.com	**Technology**	www.apple.com	**Vehicles**	www.kia.com/us/en
Luxury Fashion	www.prada.com	**Fast Fashion**	www.hm.com	**Technology**	www.samsung.com	**Vehicles**	www.ford.com
Luxury Fashion	www.armani.com/en-us	**Fast Fashion**	www.forever21.com	**Technology**	www.microsoft.com	**Vehicles**	www.astonmartin.com/en-us
Luxury Fashion	www.ralphlauren.com	**Fast Fashion**	www.uniqlo.com	**Technology**	www.dell.com	**Vehicles**	www.toyota.com
Luxury Fashion	www.ysl.com	**Fast Fashion**	www.guess.com/us/en/home	**Technology**	www.hp.com	**Vehicles**	www.honda.com
Luxury Fashion	www.moncler.com/en-us/	**Fast Fashion**	www.boohoo.com	**Technology**	www.lenovo.com	**Vehicles**	www.mbusa.com
Luxury Fashion	us.lanvin.com	**Fast Fashion**	www.prettylittlething.com	**Technology**	www.asus.com	**Vehicles**	www.audiusa.com
Luxury Fashion	www.cartier.com/en-us/home	**Fast Fashion**	www.anthropologie.com	**Technology**	www.acer.com	**Vehicles**	www.vw.com
Luxury Fashion	www.alexandermcqueen.com	**Fast Fashion**	www.yesstyle.com/en/	**Technology**	www.lg.com	**Vehicles**	www.nissanusa.com
Luxury Fashion	www.oscardelarenta.com/	**Fast Fashion**	us.peppermayo.com/	**Technology**	www.sony.com	**Vehicles**	www.hyundaiusa.com
Luxury Fashion	us.maxmara.com	**Fast Fashion**	www.lulus.com/	**Technology**	www.panasonic.com	**Vehicles**	www.lamborghini.com/en-en
Luxury Fashion	www.givenchy.com	**Fast Fashion**	www.showpo.com/us/	**Technology**	www.toshiba.com	**Vehicles**	www.polestar.com/us
Luxury Fashion	www.hermes.com	**Fast Fashion**	www.glassons.com/	**Technology**	www.huawei.com	**Vehicles**	www.subaru.com
Luxury Fashion	www.valentino.com	**Fast Fashion**	www.abercrombie.com/shop/us	**Technology**	www.mi.com	**Vehicles**	www.mazdausa.com
Luxury Fashion	www.tomford.com	**Fast Fashion**	www.fashionnova.com	**Technology**	www.oneplus.com	**Vehicles**	www.jeep.com
Luxury Fashion	www.bottegaveneta.com	**Fast Fashion**	www.missguided.co.uk	**Technology**	www.bestbuy.com	**Vehicles**	www.dodge.com
Luxury Fashion	www.dolcegabbana.com	**Fast Fashion**	www.aliexpress.com	**Technology**	www.razer.com	**Vehicles**	www.ramtrucks.com
Luxury Fashion	www.celine.com	**Fast Fashion**	www.nastygal.com	**Technology**	www.nvidia.com	**Vehicles**	www.chrysler.com
Luxury Fashion	www.ferragamo.com	**Fast Fashion**	www.cottonon.com	**Technology**	www.intel.com	**Vehicles**	www.ferrari.com/en-US
Luxury Fashion	www.off---white.com	**Fast Fashion**	www.express.com	**Technology**	www.amd.com	**Vehicles**	www.rivian.com
Luxury Fashion	www.loewe.com	**Fast Fashion**	www.primark.com	**Technology**	www.bose.com	**Vehicles**	www.landroverusa.com
Luxury Fashion	www.balmain.com	**Fast Fashion**	www.edikted.com	**Technology**	www.jbl.com	**Vehicles**	www.jaguarusa.com
Luxury Fashion	www.maisonmargiela.com	**Fast Fashion**	www.pacsun.com	**Technology**	www.oracle.com	**Vehicles**	www.fiat.com/
Luxury Fashion	www.miumiu.com	**Fast Fashion**	www.hollisterco.com	**Technology**	www.logitech.com	**Vehicles**	www.miniusa.com/
Luxury Fashion	www.jimmychoo.com	**Fast Fashion**	www.garageclothing.com	**Technology**	www.anker.com	**Vehicles**	www.peugeot.com/en/

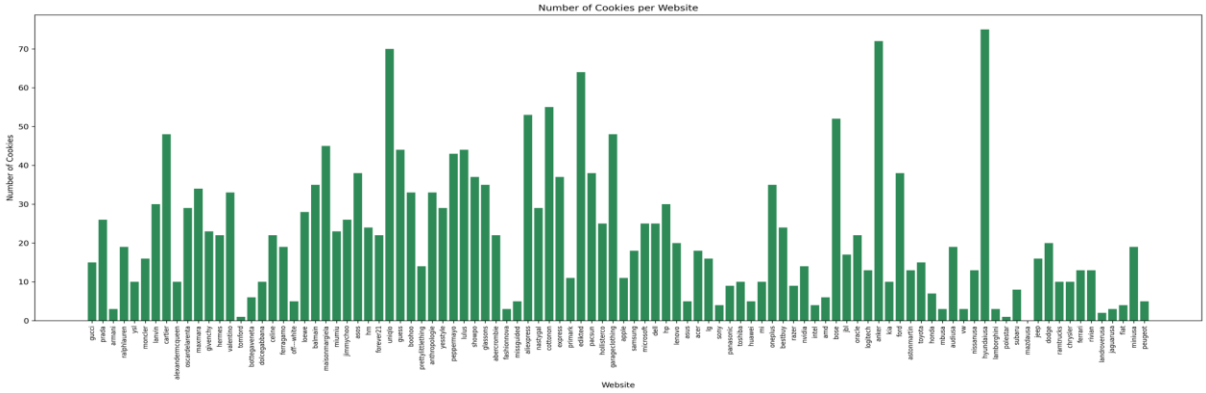
Supplementary Table 2

Keyword Categories	Keywords
Privacy Policy Link Identifiers	"privacy", "cookie", "terms", "user agreement", "service agreement", "conditions of use", "terms of usage", "privacy notice", "privacy policy", "privacy cookies", "ccpa", "dnsmpi", "do not sell my personal information", "do not sell my information", "do not sell my info", "do not sell my personal info", "do not sell or share my personal information", "do not sell / share my personal information", "do not sell/share my personal information", "do not sell or share my information", "do not sell or share my info", "do not sell or share my personal info", "California Consumer Privacy Act", "Your California privacy rights", "CCPA rights", "California privacy disclosures", "Do not share my data", "California opt-out."
DNSMPI Link Identifiers	"ccpa", "dnsmpi", "do not sell my personal information", "do not sell my information", "do not sell my info", "do not sell my personal info", "do not sell or share my personal information", "do not sell / share my personal information", "do not sell/share my personal information", "do not sell or share my information", "do not sell or share my info", "do not sell or share my personal info", "California Consumer Privacy Act", "Your California privacy rights", "CCPA rights", "California privacy disclosures", "Do not share my data", "California opt-out."

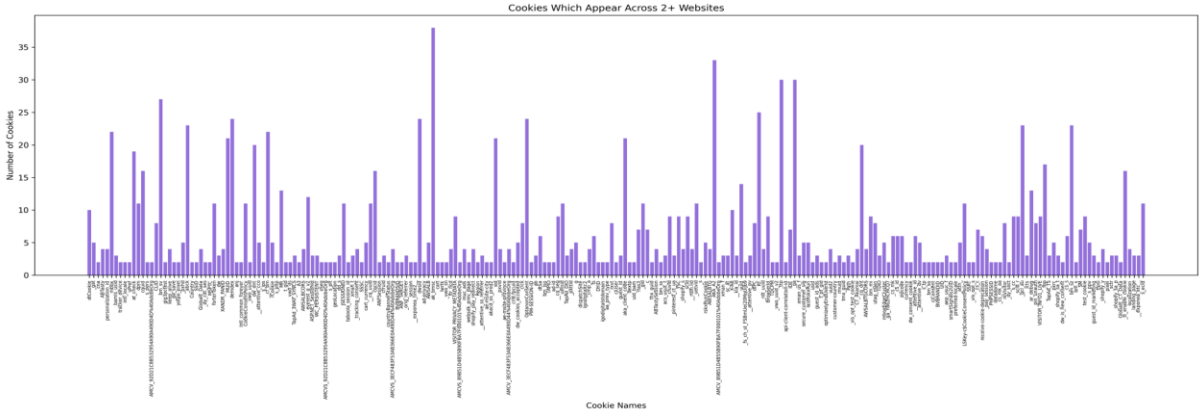
Supplementary Table 3

https://research-git.uiowa.edu/ecelias/cs3640/-/blob/A5/A5/analysis/cookie_summary_data.csv?ref_type=heads

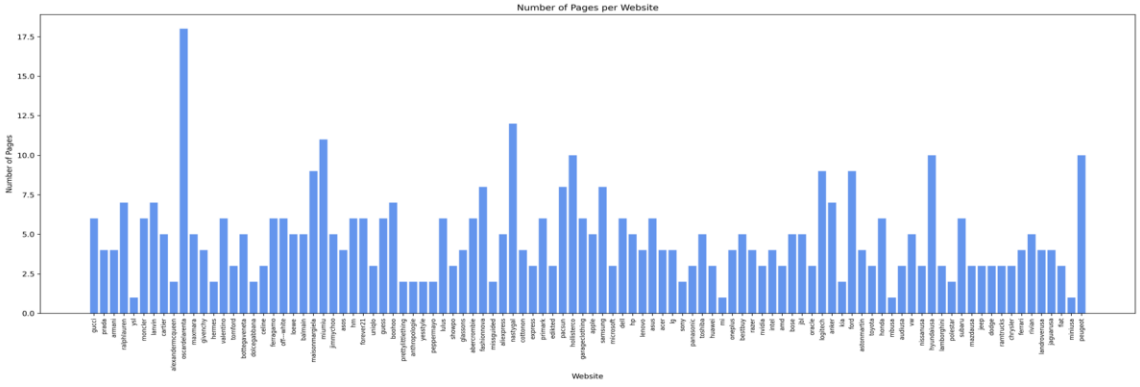
Supplementary Figure 1



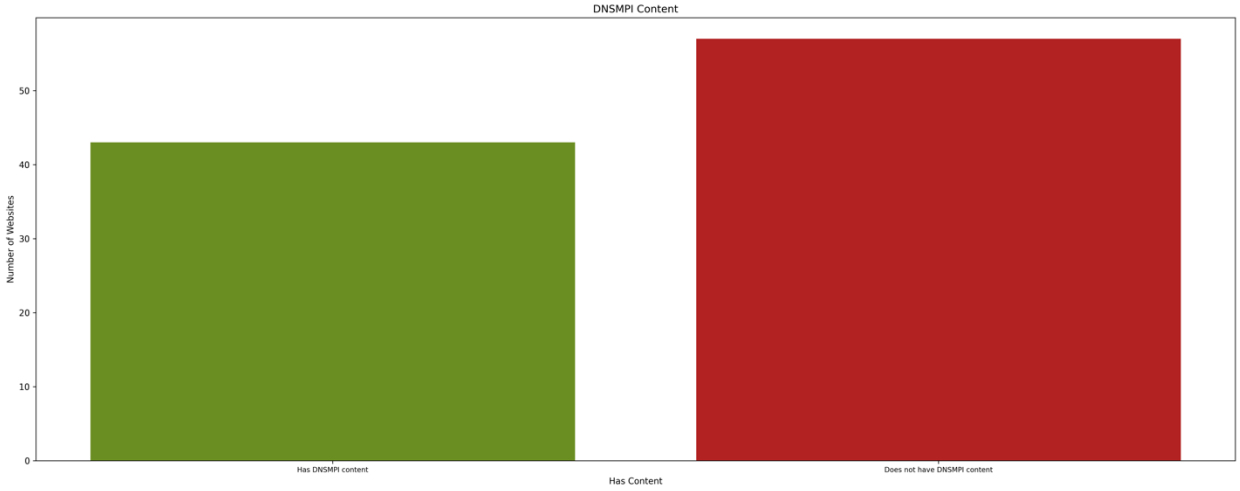
Supplementary Figure 2



Supplementary Figure 3



Supplementary Figure 4



Supplementary Figure 5