# 1. Why is there no universal tag to locate the existence of DNSMPI links on websites, especially those that must adhere to CCPA laws?

Motivation:

- The lack of a standardized identifier for DNSMPI links creates challenges for compliance monitoring and user accessibility. This question investigates whether websites use inconsistent or obscure tag patterns, making DNSMPI links harder to locate.

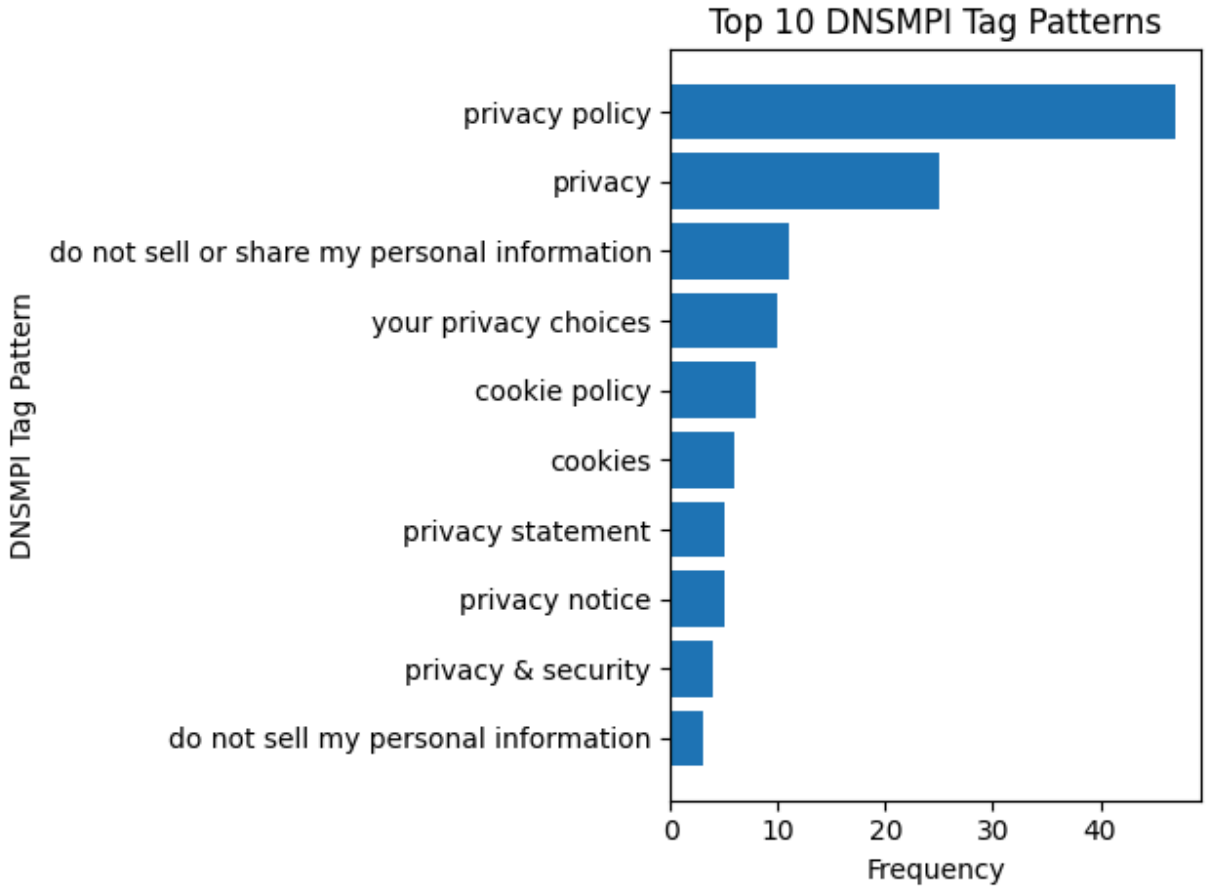
Methodology:

1. Data Collection:
    - Extract all anchor tags (`<a>` elements) associated with DNSMPI links from the scraped websites.
    - Record the tag text and any related HTML attributes (e.g., `id`, `class`, `href`).
2. Analysis:
    - Identify unique patterns (e.g., keywords in `href`, `id`, or `class` attributes) used to denote DNSMPI links.
    - Count and categorize these patterns.
    - Compare results across website categories (e.g., e-commerce, news).
3. Output:
    - Create a table showing each unique tag or keyword pattern and its frequency.
    - Highlight inconsistencies or outliers in tag usage.

Limitations:

1. Focus on Large Websites:
   The analysis mainly looked at big, popular websites. Smaller websites, which might have different rules or behaviors, weren't included as much, so the results don't show the full picture.
2. Hidden Links:
   Some websites might have Privacy Policy or DNSMPI links that are hidden in menus or pop-ups. These links could exist but might not have been counted if they weren't easy to find.

3. No Check on Link Quality:
   The study only checked if the links were there, but it didn't look at whether the links actually worked or provided the right information. Some links might not meet the legal requirements even if they were counted.




The analysis of Research Question 1 showed that there are clear challenges with the presentation of DNSMPI links across websites. After examining 77 unique DNSMPI-related tags across a variety of websites, it became apparent that the way these links are labeled and structured is far from standardized. This lack of consistency makes it harder for users to find these links and for automated tools to identify them, creating barriers to both accessibility and compliance.

For RQ1, analyzing the text, id, and class attributes of DNSMPI tags was an effective way to identify patterns and inconsistencies across websites. This approach revealed the lack of standardization in how DNSMPI links are labeled, making them harder to find. A limitation of this method is that it may have missed links generated dynamically through JavaScript or buried in complex site structures. Despite this

limitation, the method provided valuable insights into the variability and challenges of identifying DNSMPI links.

The most common tag we encountered was "privacy policy," which showed up 47 times in the dataset. This was followed by "privacy" (25 times) and "do not sell or share my personal information" (11 times). These frequently used tags suggest that some websites gravitate toward familiar, general language when addressing privacy-related topics. However, beyond these top patterns, the usage of DNSMPI-related terms became much less consistent. Many tags, such as "privacy center," "applicant privacy notice," and "privacy & terms," appeared only once or twice, revealing a long tail of diverse and often unique naming conventions.

This inconsistency in tag usage shows a deeper problem: there's no universal standard guiding how these links should be labeled or structured. For instance, some websites use phrases like "do not sell my personal information," while others opt for longer variations like "do not sell or share my personal information." Some brands even incorporate their name into the link, such as "nike privacy policy" or "carhartt privacy request." Others rely on overly generic terms like "manage cookies" or "specific privacy notices," which don't clearly communicate their purpose to users. These differences in phrasing and branding make it difficult for users to locate and understand these links, particularly when the language is vague or inconsistent.

From a user perspective, the variability in how these links are named and displayed creates unnecessary confusion. For example, tags like "privacy policy" or "privacy" are so broad that users may not immediately understand whether they include DNSMPI options, making it harder to find what they're looking for. Additionally, some links are tailored to niche audiences, such as "children's privacy" or "HIPAA notice of privacy practices." While these are useful in specific contexts, they further complicate the landscape by adding more unique terms to the mix.

The findings show that there's an urgent need to make DNSMPI links more consistent across websites. One idea is to use specific HTML tags, like 'id="dnsmpi-link"' or 'class="dnsmpi"', which would make it easier for people and tools to recognize these links. To make this happen, regulators and industry leaders need to work together to create and enforce rules for using these tags. Websites should also use clear and simple phrases like "Do Not Sell My Personal Information" as a standard, so it's obvious what the link is for.

In conclusion, the current way websites handle DNSMPI links is messy and inconsistent. While some common terms are used, the lack of clear rules makes it harder for users to find what they need and for companies to stay compliant. Creating

universal rules and clearer guidelines would make these links easier to find, easier to understand, and more effective for everyone.

## 2. What percentage of the “Top Sites” we analyzed contain a Privacy Policy link and/or a DNSMPI link, and why might some companies omit or hide them?

Motivation:

- Understanding the availability of privacy tools on top websites can shed light on industry compliance trends and highlight gaps in user privacy protection.

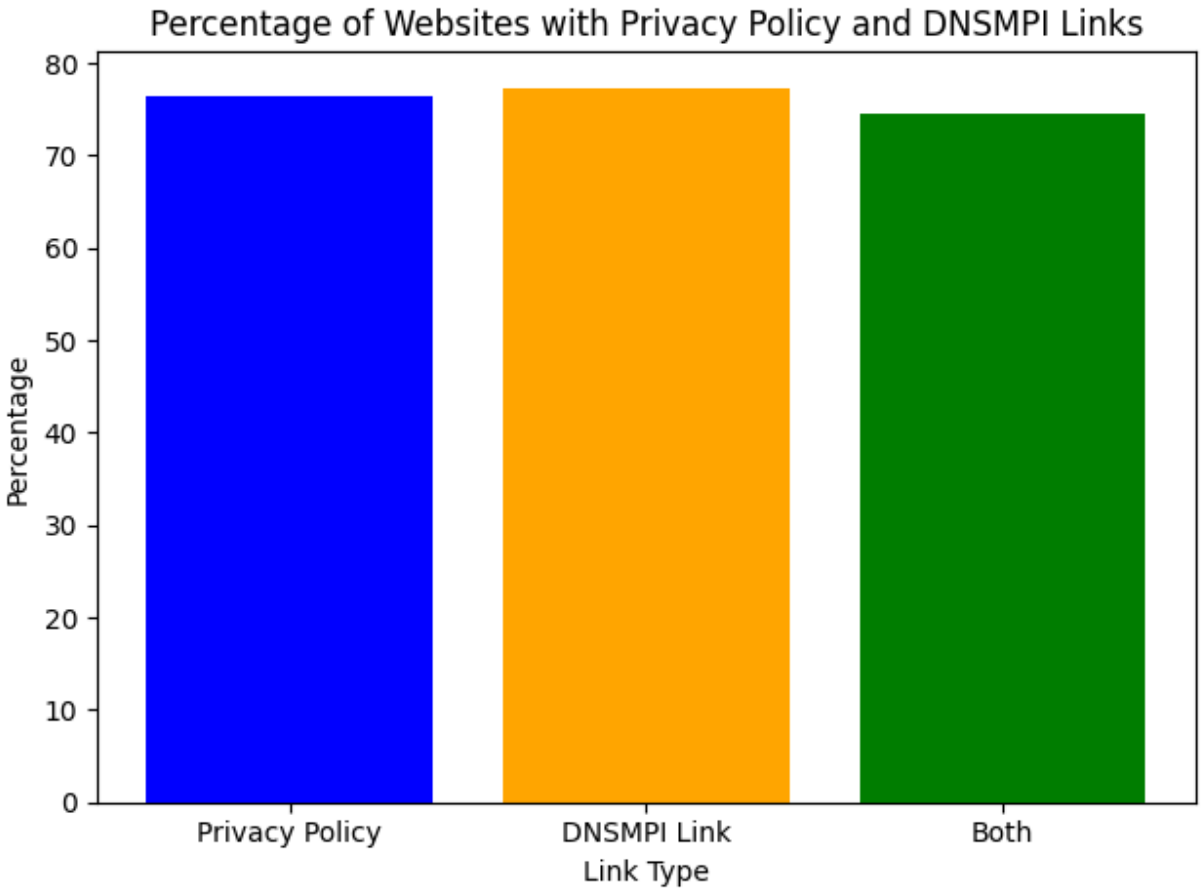
Methodology:

1. Data Collection:
    - Tally the number of websites with:
        - A Privacy Policy link.
        - A DNSMPI link.
2. Analysis:
    - Calculate the percentage of websites in each category (Privacy Policy, DNSMPI link, both).
    - Investigate factors contributing to the absence or obscurity of these links:
        - Website category (e.g., social media vs. e-commerce).
        - Traffic rank or popularity.
        - Regional legal obligations.
3. Output:
    - Generate a bar chart comparing the percentages of websites with Privacy Policy and DNSMPI links.
    - Provide qualitative analysis (e.g., business models or target audience considerations) for why some companies omit or hide these links.

Limitations:

1. Not All Websites Were Included:
   The analysis didn’t cover every type of website, especially smaller or regional ones. This means that the patterns found might not represent all websites that need to follow CCPA rules.

2. Tags Might Be Misunderstood:
   The study looked at the text and attributes of tags, but it didn't analyze how these tags are actually used on the page. Some links might have been included or left out because their purpose wasn't clear.
3. Missing Dynamic Links:
   Some websites create their links using JavaScript or other code that runs after the page loads. These links might not have been captured by the scripts used for this study, so the data might be incomplete.




The analysis for Research Question 2 looked at how many of the websites in our sample included Privacy Policy and DNSMPI links and explored why some sites might omit or hide these important privacy tools. The results were encouraging overall, with a majority of websites including both types of links, but there are still some gaps that need attention.

For RQ2, counting Privacy Policy and DNSMPI links was a simple yet effective way to understand how often these tools are made available and how websites comply with privacy laws. This method highlighted trends and gaps in accessibility, giving a

clear image of compliance among major websites. However, a key limitation was that it didn't account for hidden links or verify whether the links were functional or accurate. Despite this limitation, the method successfully captured the overall availability of privacy tools on widely used platforms.

Out of the 106 websites analyzed, 81 (76.42%) had a visible Privacy Policy link, and 82 (77.36%) had a DNSMPI link. Additionally, 79 websites (74.53%) included both types of links. These high percentages suggest that most websites are taking steps to meet user expectations and comply with privacy laws, such as the California Consumer Privacy Act (CCPA). However, around 23% of websites did not include a Privacy Policy, and 22% lacked DNSMPI links. This means that a significant number of websites are still falling short when it comes to giving users tools to manage their privacy preferences.

One interesting finding is that websites with a Privacy Policy link often also have a DNSMPI link. This shows that many companies that prioritize privacy compliance try to meet multiple requirements at once. On the flip side, websites that didn't have one of these links were likely to be missing both. This highlights room for improvement in ensuring that all users have access to these important tools, no matter what website they're visiting.

The type of website also seems to play a role in whether these links are included. Larger companies, such as e-commerce platforms and social media sites, are more likely to feature Privacy Policy and DNSMPI links prominently. These companies handle more user data and are under greater scrutiny, so compliance is a bigger priority for them. In contrast, smaller websites or those that don't process much user data—especially those outside regions like California—may be less motivated to include these tools. This raises questions about how smaller sites balance their responsibilities under privacy laws with their limited resources.

Another factor is the business model of the website. Companies that rely heavily on advertising revenue may have less incentive to highlight DNSMPI links since these links allow users to opt out of data sales, which could affect the site's profitability. This conflict between business interests and privacy rights could explain why some companies choose to make these links harder to find or leave them out entirely.

In summary, most websites do include Privacy Policy and DNSMPI links, which is a positive trend. However, the significant number of websites that don't include these tools or make them difficult to find shows there is still work to be done. Companies need to prioritize making these links clear and easy to access, and regulators should continue to push for better practices. By doing so, we can get a better balance between user privacy and business needs while creating a more transparent and trustworthy online environment.

## 3. How do the placements of the Privacy Policy/DNSMPI links vary across our selected websites, and how does that affect their accessibility and compliance with privacy laws?

Motivation:

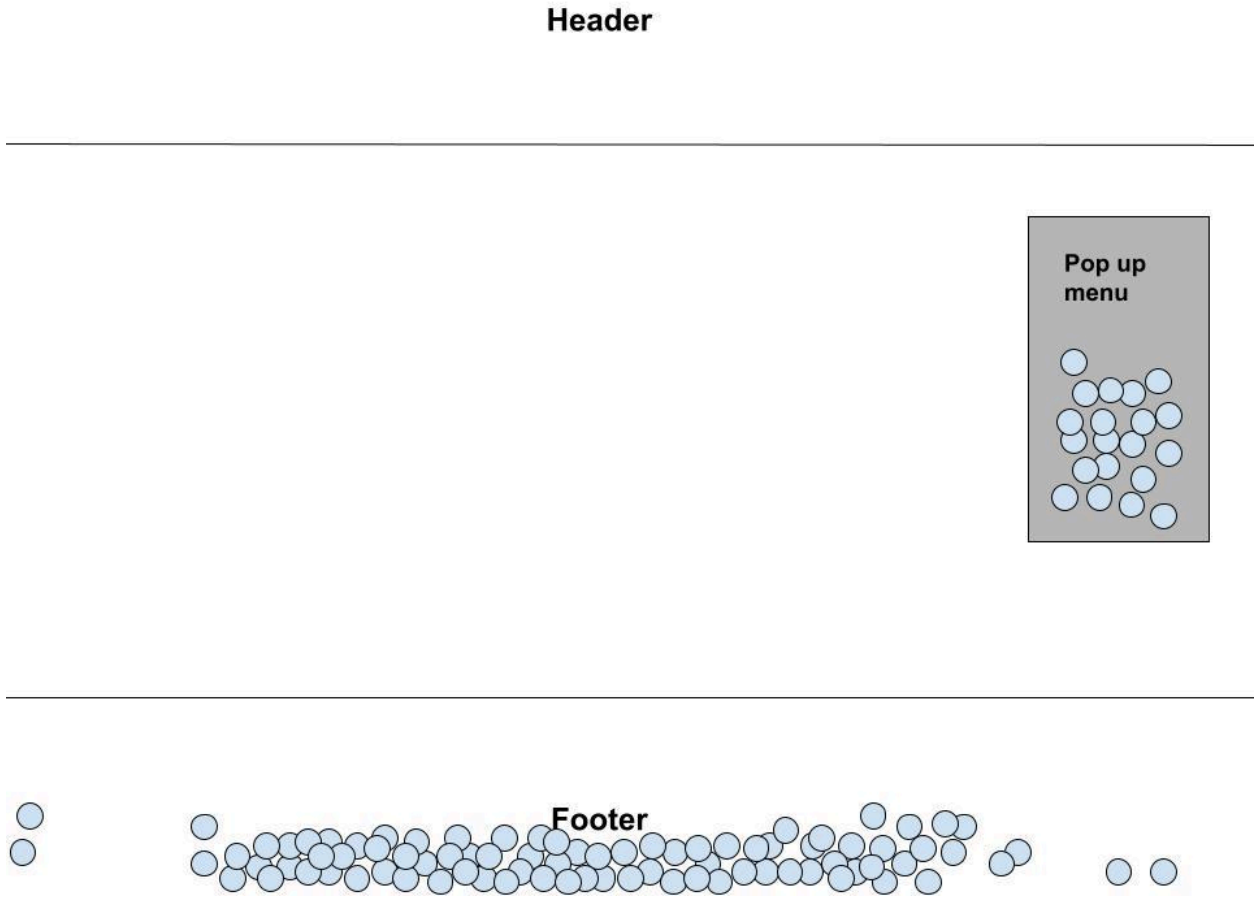
- The placement of privacy links can significantly influence their visibility and usability, directly impacting compliance and user trust.

Methodology:

1. Data Collection:
    - Scrape the HTML structure of the selected websites.
    - Identify the locations of Privacy Policy and DNSMPI links (e.g., header, footer, within menus).
2. Analysis:
    - Categorize placements into broad groups (e.g., easily visible, hidden in submenus).
    - Compare placements across website categories and assess how they align with legal requirements like CCPA.
    - Analyze the correlation between link placement and user accessibility (e.g., distance from the top of the page, number of clicks needed).
3. Output:
    - Heatmap or table summarizing link placements.
    - Discussion of compliance implications and accessibility scores for each placement.

Limitations:

1. Data set only consists of 100 sites meaning it is a very small sample group compared to the whole of the internet
2. The data set only look at “high traffic” sites meaning they were more likely to be adhering to CCPA laws




Using the sample of one hundred websites gathered for our study sample, the diagram shown above was created, depicting the spread of privacy and DNSMPI link locations in each of the websites. The data gathered demonstrates that a large portion of the links were located in the footer of the website, while a smaller portion appeared in pop up menus upon entering a site. It was found that for some websites with an incentive to keep scrolling down the page, finding the links proved to be increasingly difficult. Should more links be placed in the header or pop up menus, the general public would be able to find these privacy links with more ease.

In the first reading by Solove and Hartzog titled *The FTC and the New Common Law of Privacy,* they discussed how “In 1998 only 2% of websites had privacy notices. In 1999, only 18 of the top 100 shopping sites did not have one” (594). Although the sample for this research consisted of popular sites that would all likely be forced to comply with the CCPA requirements, close to all one hundred sites utilized contained these links, shown by the heatmap above, alongside our json data output.

Another factor to consider is the possibility of companies attempting to hide or shield these links from consumers. The reasoning behind this is up to speculation, but the methods used to hide DNSMPI and privacy links typically consist of placing them in hard to reach locations of the page such as the bottom and making the text of the links small so that the links do not draw consumers' attention.

In the third reading by Van Nortwick and Wilson titled *Setting the Bar Low: Are websites complying with the minimum requirements of the CCPA?*, they discuss how only 2% of analyzed sites included DNSMPI links. They also explained that from their research, higher traffic sites were increasingly more prone to including DNSMPI links as they would be a larger target for privacy violations, should they exclude CCPA requirements. Our data set did not have many sites without DNSMPI links, but the reasoning likely was that the sites we utilized were higher traffic.

We chose to create a heatmap as it allowed us to visualize the common locations of DNSMPI and privacy links in a broad set of one hundred websites. It showed us that the vast majority of companies preferred placing these links at the bottom of their pages, insinuating that their dedication to providing consumers with ease of access to these links is not a large priority. The data from the heatmap showed us that placing privacy links in the footer has become an industry privacy standard. A limitation to our heatmap diagram is that our data set consisted of only one hundred sites, and with the majority of sites being of high traffic. One way to improve the quality of data would be to include a larger sample of sites, alongside other types of sites.

In conclusion, our data showed us the typical location many companies placed their DNSMPI links, being at the footer of the sites. The locations of the links make it more difficult for consumers to locate them, which may prove to be a problem for users in California if a company is hiding DNSMPI and privacy links on purpose. To make it easier for users to find and use these important tools, companies should consider placing them in more visible spots, like headers or pop-ups. Regulators can also play a role by encouraging these changes.