Empirical Studies on the Usability of Web Privacy Controls

Yuemeng Yin, School of Computer Science and Engineering
Supervisor: Dr Rahat Masood

Introduction

With the increasing awareness and concerns around privacy, many service providers are offering various privacy controls to their users. However, these controls may be buried deep within menus or settings, making them difficult for a user to access [1]. Additionally, the terminology used to describe privacy controls can sometimes be confusing or technical, further complicating the user's ability to understand and use them effectively [2,3]. While many privacy controls have been proposed to protect user data on these sites, existing research tends to focus on individual controls rather than providing a comprehensive overview of the privacy landscape.

Objective

This project aims to fill the gaps in existing literature by providing an analysis of four privacy controls, namely privacy nudge, privacy notice, privacy policy, and privacy setting, and evaluating their usability on websites. Through the manual investigation and automated data crawlers, we intend to collect usability data (awareness, efficiency, comprehension, functionality, and choice) in three website visit scenarios.

Key Findings

- Privacy policies are most common across all visit scenarios, with privacy nudges and notices being prevalent in sign-up situations.
- The unstructured display style of privacy notices and nudges, the absence of clear instructions under privacy settings, and the limited language options provided for privacy policies are few of the issues we have identified.

Summary

The usability exploration of top 100 most visited health websites has been conducted using our analysis template. Our future research involves gathering usability data from a larger sample of websites using automated data crawlers and designing user surveys to delve into human factors linked to privacy risk quantification and assessment.

References

[1] Habib et al. (2019). An empirical analysis of data deletion and Opt-Out choices on 150 Websites.
[2] Ermakova et al. (2015). Readability of privacy policies of healthcare websites.
[3] Ali et al. (2020). Readability of websites security privacy policies: A survey on text content and readers.

Methods & Results

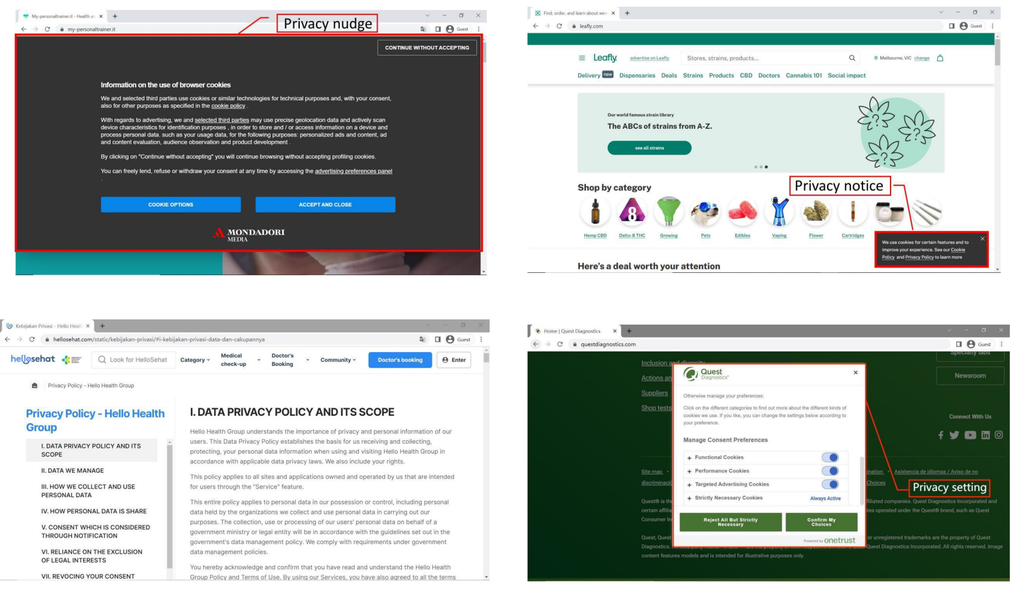

Figure 1. Example of Four Privacy Control Types

Usability Attributes		Guest Visit				Sign-up User Visit				Registered User Visit
		nudge	notice	policy	setting	nudge	notice	policy	setting	account setting
Awareness	Location	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Display type	✓	✓			✓	✓		✓	
Efficiency	Number of clicks			✓	✓					✓
Comprehension	Language			✓	✓				✓	✓
	Table of content			✓						
Functionality	Type of privacy content	✓	✓		✓	✓	✓		✓	✓
Choice	Types of options	✓		✓		✓				
	Explicit choice guidance	✓		✓		✓				

Table 1. Usability Attributes for Four Privacy Controls in Three Visit Scenarios

1. Classification of Privacy Controls

We classify privacy controls into four distinct categories: privacy nudges, privacy notices, privacy policies, and privacy settings. This categorization allows for a systematic approach in evaluating usability.

1.1 Privacy Nudge

A privacy nudge provides user privacy-related information and the opportunity for user to make privacy choices.

1.2 Privacy Notice

The privacy notice provides the user only with privacy information. This means there is no option for the user to take an action on the displayed notice except for removing it from their display.

1.3 Privacy Policy

The privacy policy is a statement that explains what information is collected and how a website collects and processes the user's personal information.

1.4 Privacy Setting

The privacy setting is the selection of options that allows users to control their data privacy according to their service demands and personal willingness.

2. Usability Evaluation Metrics

We introduce the Privacy Controls Evaluation Framework, summarized in Table 1, which provides a set of criteria that can be used in usability evaluations of privacy controls. We structure the framework according to the 5 usability attributes, which are *awareness, efficiency, comprehension, functionality, and choice*. For each metric included in the framework, we highlight the study approaches and describe measures or example prompts that can be incorporated into a usability study.

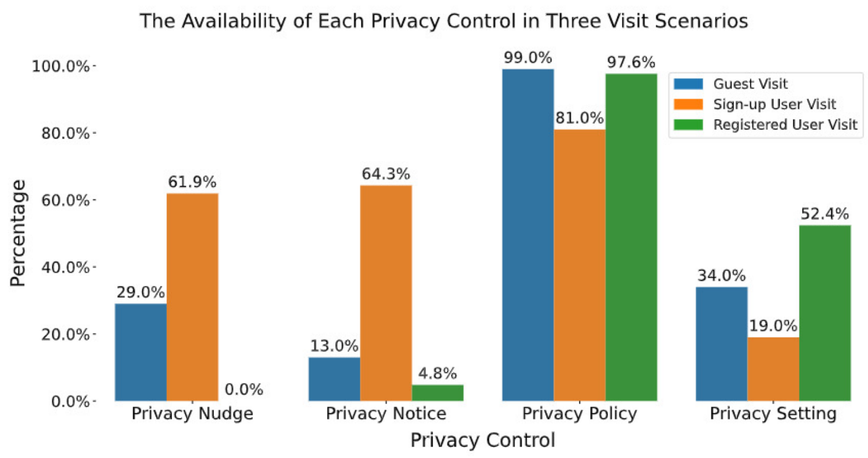

Figure 2. The Availability of Each Privacy Control in the Top 100 Health Websites

3. Data Collection

Two methods to investigate the usability of sampled websites are explored.

3.1 Heuristic Evaluation

We have developed a data collection template for assessing the usability of websites based on the five usability metrics mentioned earlier. Our primary focus is on three different scenarios when users visit a website: *guest visit, sign-up user visit, and registered user visit*. A team of three researchers was involved to independently conduct data collection and fill out the template.

3.2 Web crawling

Through the automated data crawlers, we collect usability data/attributes in three website visit scenarios.

We use Pyppeteer with the headless chrome browser to open the webpage and scrape the information relating to privacy nudges, privacy notices, privacy policy, and privacy settings. Selenium Webdriver is used for navigating from website main page to the privacy policy/setting page. For non-English websites, google translate API is applied to detect/translate texts. The results obtained from the script are exported to survey excel template through xlwings.

User account is pre-registered. Navigate to login/sign-in page by Selenium Webdriver, and input username, password to log into the website. Once logged in, navigate to the user account page, analyze information regarding privacy nudges, notices, and especially privacy setting.

4. Discussion

4.1 Analysis of Existing Privacy Controls

We thoroughly explore and present strategies to improve usability, emphasizing the importance of adhering to best practices and user-centric approaches. Based on our findings, we provide suggestions to improve the display location, functionality, comprehension, and access efficiency of privacy controls.

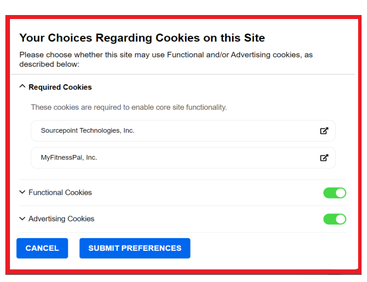

Figure 3. Example of By Default Cookie Options and Opt-In Behavior

4.2 Dark Patterns

Dark patterns are increasingly being used to coerce unsuspecting users to accept less privacy protective options. During our data gathering process, we came across several such practices followed by different websites.

Acknowledgments

I would like to thank my supervisor Dr Rahat Masood for her continuous support and invaluable inspiration throughout the project. This work was created as part of the Taste of Research Program 2023 at the University of New South Wales, Australia.