Privacy-aware Snippets: Enhancing Assessment of Balance between Privacy Risks and Benefits in Web Search

Yusuke Shimizu
Tetsushi Ohki
Yusuke Yamamoto
shimizu@design.inf.shizuoka.ac.jp
ohki@inf.shizuoka.ac.jp
yusuke_yamamoto@acm.org
Shizuoka University
Hamamatsu, Shizuoka, Japan

ABSTRACT

This paper proposes two search user interfaces (UI) to provide web search users with comprehensive information about to whom web browsing histories could be shared and how much. The two UIs aim to encourage web searchers to consider the trade-off between the risks of online tracking and the benefits of information access. In an online user study, we examined how the proposed search UIs influence the users' privacy awareness and behaviors in web searches. The results of the user study indicated that the participants felt that the proposed UIs were more effective in terms of learning the extent of browsing history sharing than a search result UI that simply identifies the presence or absence of embedded trackers. In addition, search behavior analysis revealed that the participants tended to click websites embedded with trackers more actively to look for useful information if the search engines present a summary of categories and the number of share destination websites in browsing histories.

CCS CONCEPTS

• **Information systems** → **Search interfaces**; • **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → **User studies**.

KEYWORDS

web search, privacy, search interface, human factor, behavior change

ACM Reference Format:
Yusuke Shimizu, Tetsushi Ohki, and Yusuke Yamamoto. 2022. Privacy-aware Snippets: Enhancing Assessment of Balance between Privacy Risks and Benefits in Web Search. In *Conference on Information Technology for Social Good (GoodIT'22), September 7–9, 2022, Limassol, Cyprus.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3524458.3547231

1 INTRODUCTION

Personalized information delivery on the web has become increasingly popular; however, with the increase in personalized information delivery, data privacy issues have become an important social issue. Digital marketing agencies can deliver personalized ads by tracking user behavior logs, e.g., web search and browsing histories depending on user behavior and preferences. However, an increasing number of people distrust personalized web advertising [16] and have serious concerns about how their data will be used [3]. Excessive tracking can display web ads that reflect information that is too private, e.g., health concerns and ideological beliefs. As a result, people are concerned about embarrassment that may occur if their private information is shared with others.

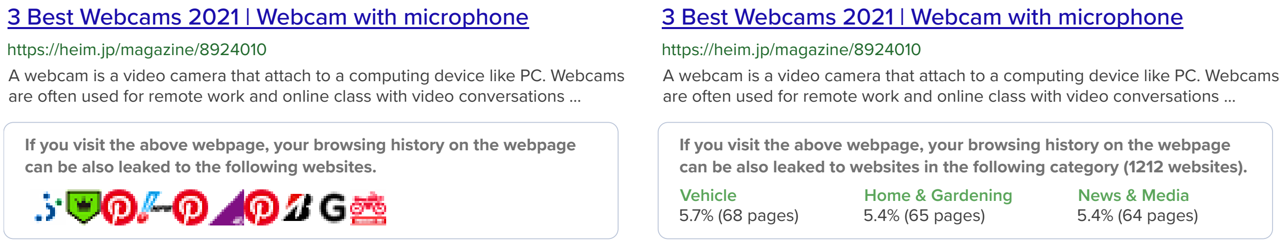
Due to these concerns, momentum to protect personal data has grown. For example, the General Data Protection Regulation[1] and the California Consumer Privacy Act[2] have been established in Europe and California, USA, respectively. In addition, researchers have developed and improved tracking blockers for web browsers. Currently, many people use such blockers to prevent their browsing histories from being shared with others; however, technologies have been developed to avoid tracking blockers. It is difficult for purely technology-oriented approaches to provide complete protection against online tracking risks [9]. To protect data privacy on the web, users must also adopt effective behaviors to protect their privacy in web search and browsing.

Although web search engines are widely used as the main tools to retrieve information on the web, there are several data privacy-related problems to consider when performing web searches. First, web search engines generally only provide relevant information with respect to information needs in their search engine results

[1] https://gdpr-info.eu/
[2] https://oag.ca.gov/privacy/ccpa

GoodIT'22, September 7–9, 2022, Limassol, Cyprus

ACM ISBN 978-1-4503-9284-6/22/09…$15.00
https://doi.org/10.1145/3524458.3547231



3 Best Webcams 2021 | Webcam with microphone

https://heim.jp/magazine/8924010

A webcam is a video camera that attach to a computing device like PC. Webcams are often used for remote work and online class with video conversations ...

If you visit the above webpage, your browsing history on the webpage can be also leaked to the following websites.

3 Best Webcams 2021 | Webcam with microphone

https://heim.jp/magazine/8924010

A webcam is a video camera that attach to a computing device like PC. Webcams are often used for remote work and online class with video conversations ...

If you visit the above webpage, your browsing history on the webpage can be also leaked to websites in the following category (1212 websites).

Vehicle	Home & Gardening	News & Media
5.7% (68 pages)	5.4% (65 pages)	5.4% (64 pages)

(a) Icon UI

(b) Ratio UI

Figure 1: Proposed web search result representations on SERPs.

pages (SERP), e.g., titles, URLs, and snippets. As a result, it is difficult to examine and assess privacy risks, e.g., tracking risks, on webpages listed in SERPs. Several researchers have proposed approaches to present simple privacy-related information on SERPs to notify whether webpages have privacy risks or not [15]. However, such simple information is not enough for web searchers to fully understand complicated privacy risks. Some web searchers may overestimate the risks and lose the opportunities to obtain information. The second problem involves the trade-off between aversion of privacy risks and the benefits of visiting webpages. When simply visiting a web page to review privacy policy information, web searchers have privacy risks of tracking their behavior data. One way to protect the data privacy of web searchers is to exclude webpages where there can be privacy risks from SERPs or not visit such pages. However, depending on the purpose and subjects of the tracking, web searchers may accept such tracking risks if they want to access a given website [9]. A simple approach to ignore webpages with privacy risks would deprive web searchers of the opportunity to browse such webpages even if they are willing to accept some degree of risk.

Information about privacy risks on webpages should be readily accessible to web searchers so they can consider the trade-offs between the risks and benefits of browsing webpages *prior to visiting them*. Thus, this paper focuses on a specific privacy risk in web search, i.e., the risk that browsing history could be collected and shared by a third party. We attempt to provide web searchers with comprehensive information about to whom web browsing histories could be shared and how much. To this end, we propose the two types of search result representations on SERPs and reveal how the representation user interfaces (UI) influence privacy awareness and user search behavior.

The main contributions of this paper are summarized as follows.

- We proposed the Icon and Ratio search result representation UIs to clearly convey the extent of sharing of browsing history on a webpage (see Fig. 1).
- The results of the user study indicate that the participants felt that the Icon and Ratio UIs were more effective in terms of learning the extent of browsing history sharing than a search result UI that simply identifies the presence or absence of embedded trackers.
- An analysis of search behavior revealed that participants using the Ratio UI tended to browse search results embedded with trackers more actively to look for useful information than the simple SERP UI. In contrast, we did not observe this tendency with the Icon UI.

2 RELATED WORKS

2.1 Tracking in web search and browsing

Online behavioral tracking (OBT) plays a key role in optimizing information delivery, e.g., targeting ads and web search personalization, depending on user preferences and behaviors. Various approached have been developed to track online behaviors across websites [2]. One popular approach uses third-party cookies. For example, Englehardt et al. found that OBT using third-party cookies can reveal users' browsing transitions on the web more efficiently than using IP addresses [4]. Due to concerns about third-party cookies, Apple and Google have introduced intelligent tracking prevention[3] and a privacy sandbox[4] to block online tracking, respectively. However, adversaries have started to develop new methods to identify and track users on the web that do not rely on third-party cookies, e.g., link decoration[5], CNAME cloaking[6], and browser fingerprints [1, 17]. Levia et al. reported that even mouse movement information can be used to infer user demographics with reasonable accuracy [7].

This study explores which privacy risk indicators can provide web searchers with comprehensive information about web browsing histories are shared to and the extent of the sharing. This study focuses on third-party cookies as a way to detect tracking activity on websites before moving from search engine sites to the websites.

2.2 Awareness of online privacy

An increasing number of people have serious concerns about how their online behaviors are tracked, and distrust in targeted online advertisements is increasing [16]. Today, a lot of people use tracking blockers such as uBlock Origin[7] and Ghostery[8] to prevent their behavioral data from being shared. In addition, people have expressed concerns about how web search personalization modifies search results to reflect their interests, which can cause filter bubbles, particularly for political topics [19]. Even though people generally worry about online behavior privacy, they do not care

[3] https://www.apple.com/privacy/features/
[4] https://www.chromium.org/Home/chromium-privacy/privacy-sandbox
[5] https://webkit.org/blog/8828/intelligent-tracking-prevention-2-2/
[6] https://webkit.org/blog/11338/cname-cloaking-and-bounce-tracking-defense/
[7] https://ublockorigin.com/
[8] https://www.ghostery.com/

about their behavioral data while browsing the web. This inconsistency of privacy attitudes is often referred to as the "privacy paradox" [6]. Matic et al. revealed that even if people worry about their online privacy, some favored highly personalized web ads and were willing to provide personal data to view such ads [10]. Leon et al. surveyed how the privacy policy of advertisement agencies affected web users' willingness to share their data with such agencies [8]. Their survey results suggested that web users would be more willing to provide personal data to third parties if they could control who collects the data and why kinds of data are collected. Similarly, Mathur's survey reported that people would accept behavior tracking on familiar websites or those that serve valued content [9].

Following the above results, we propose the `Icon` and `Ratio` UIs to encourage web searchers to consider the trade-off between the risks of online tracking and the benefits of information access.

2.3 Enhancing privacy awareness

Generally, it is difficult to make people concretely understand privacy risks and take actions to protect their online privacy, even though they may wish to protect their online privacy [12]. Privacy policies are important information for webpage visitors to learn what kinds of their data will be treated and how. However, several researchers have reported that many privacy policies do not provide case examples to explain the usage of the collected behavior data. Reidenberg et al. demonstrate the discrepancies in the interpretation of privacy policies between experts and non-experts [13]. Obar et al. investigated how many people skip reading the privacy policy [11]. They reveal that 74% of their participants did not read the privacy policy, and the average reading time was 73 seconds even if reading the policy. Thus, privacy policies do not work well enough to make web users aware of their privacy risks.

Some researchers have explored methods to encourage people to perform more privacy-aware actions online. Harbach et al. proposed a nudge approach to increase awareness of privacy risks in smartphone users when installing mobile applications [5]. Their approach shows examples of personal data that third-party applications can access on smartphones to make users consider the privacy risks of applications. In addition, Wang et al. proposed a privacy nudge that shows Facebook profile pictures of target audience when users post content on Facebook to make users more aware of potential risks when posting on social networking service [18].

Tools have been proposed to enhance privacy awareness in web search and browsing. Zimmerman et al. proposed a privacy nudge in web search to indicate the level of privacy risk of each web search result for a given query [20]. DuckDuckGo Inc. has released the *Privacy Essentials*[9], which is a browser extension that shows privacy risk levels for browsed websites. In addition, *Privacy Badger*[10] is a tool that is similar to Privacy Essentials. Based on privacy risk level indicators like Zimmerman's work, we propose the `Icon` and `Ratio` UIs, which provide web searchers with comprehensive information about which third parties web browsing histories could be shared with and how much.

3 PRIVACY-AWARE SEARCH SNIPPETS

Here, we explore the snippet representations on SERPs so that web searchers can consider the trade-off between privacy risks and the benefits of information access when performing web searches. The proposed search snippets help web searchers intuitively learn which third parties would monitor their behavior data prior to visiting webpages on SERPs, i.e., clicking web search results. Here, we define websites to which browsing histories on a webpage can be shared as *sharing destinations*. First, the proposed method detects which webpages on SERPs track users' behaviors and the potential sharing destinations. Then, the method generates privacy-aware snippets by extending common web search results. In this study, we investigated three snippet representations to explain the sharing extent of browsing behavior. The concepts and purposes of these three snippet representations are described in the following.

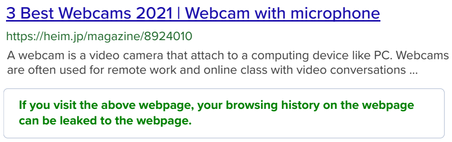
3.1 Snippet design

As shown in Figure 1(a), `Icon` UI presents a list of favicons for sharing destinations for a web search result. This UI enables users to learn several examples of websites to which their browsing histories on a webpage can be shared as well as tracking possibilities on each search result on SERPs. Note that the `Icon` UI is inspired by Wang's studies [18]. Wang et al. proposed to identify friends who can view photos shared on SNS as personalized examples to help SNS users understand the possibility that unexpected friends can view their photos. In a user study, Wang et al. revealed that their method helps users intuitively understand privacy risks when sharing photos on SNS. Unlike Wang's studies, the proposed `Icon` UI does not show personalized examples to web searchers. Instead, the `Icon` UI informs web searchers about which famous websites their browsing histories can be shared to, as sharing destination examples.

As shown in Figure 1(b), the `Ratio` UI shows the top three categories of sharing destination websites and their size. The `Ratio` UI informs users about the kinds of category websites to which their browsing histories on a web search result (i.e., a webpage) can be shared when they click the corresponding web search result. In addition, the `Ratio` UI identifies how many websites the histories can be shared to according to the website category. Unlike the `Icon` UI, the `Ratio` UI displays the number of sharing destinations and the percentage of shared website categories rather than examples of sharing destination websites. Note that one potential disadvantage of the `Icon` UI is that some users may be unfamiliar with websites represented by favicons. Showing the number of sharing destination websites with their category can be more comprehensible to some users than examples of sharing destinations. Thus, we expect that the `Ratio` UI will enable web searchers to understand the extent and types of sharing destinations better than Icon UI even if they are unfamiliar with the details of each sharing destination website.

As shown in Figure 2, similar to *DuckDuckGo Privacy Essentials* and *Privacy Badger*, the baseline representation UI, which we refer to as the `Control` UI, attempts to alarm only tracking possibility for a webpage to users. The `Control` UI does not suggest information about sharing destinations unlike the `Icon` and `Ratio` UIs. Here, assume that webpages linked from search results include embedded trackers. In this case, the baseline UI displays indicators with the

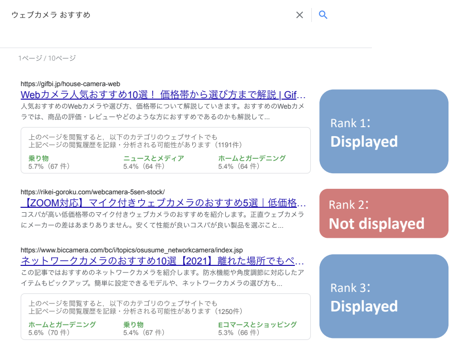
[9] https://duckduckgo.com/app
[10] https://privacybadger.org/



3 Best Webcams 2021 | Webcam with microphone
https://heim.jp/magazine/8924010
A webcam is a video camera that attach to a computing device like PC. Webcams are often used for remote work and online class with video conversations ...

If you visit the above webpage, your browsing history on the webpage can be leaked to the webpage.

Figure 2: Overview of web search result representation with simple tracking indicator (i.e., `Control` UI).



ウェブカメラ おすすめ

1ページ / 10ページ

https://gifbi.jp/house-camera-web
Webカメラ人気おすすめ10選！ 価格帯から選び方まで解説 | Gif...
人気おすすめのWebカメラや選び方、価格帯について解説していきます。おすすめのWebカメラでは、商品の評価・レビューやどのような方におすすめであるのかも解説して...

上のページを閲覧すると，以下のカテゴリのウェブサイトでも
上記ページの閲覧履歴を記録・分析される可能性があります（1191件）

乗り物	ニュースとメディア	ホームとガーデニング
5.7%（67 件）	5.4%（64 件）	5.4%（64 件）

https://rikei-goroku.com/webcamera-5sen-stock/
【ZOOM対応】マイク付きウェブカメラのおすすめ5選｜低価格...
コスパが高い低価格帯のマイク付きウェブカメラのおすすめを紹介します。正直ウェブカメラにメーカーの差はあまりありません。安くて性能が良いコスパが良い製品を選ぶこと...

https://www.biccamera.com/bc/i/topics/osusume_networkcamera/index.jsp
ネットワークカメラのおすすめ10選【2021】離れた場所でもペ...
この記事ではおすすめのネットワークカメラを紹介します。防水機能や角度調節に対応したアイテムもピックアップ。簡単に設定できるモデルや、ネットワークカメラの選び方も...

上のページを閲覧すると，以下のカテゴリのウェブサイトでも
上記ページの閲覧履歴を記録・分析される可能性があります（1250件）

ホームとガーデニング	乗り物	Eコマースとショッピング
5.6%（70 件）	5.4%（67 件）	5.3%（66 件）

Figure 3: Manipulation of search result list on SERPs. Search results labeled as "Displayed" show privacy risks indicators, and search results labeled as "Not displayed" do not show privacy risks indicators.

search results to only show that once users visit the webpages, their browsing logs on the pages can be stored and analyzed. This baseline UI enables users to identify which webpages on SERPs could involve tracking risks in a simple manner.

3.2 Hypotheses

In this study, we investigated the impact of the proposed privacy-aware snippet UIs on users' understanding of privacy risks and their search behaviors during web searches. Specifically, we focused on testing the following hypotheses.

- **H1** By displaying informative indicators about which third parties can monitor web searchers' browsing histories for a web search result in advance, the searchers will become more aware of privacy risks in web searches than simply displaying the presence of tracking.
- **H2** The informative indicators encourage web searchers to spend more time on SERP and check lower (deeper)-rank web search results in order to carefully check privacy risks and their data privacy in web searches.
- **H3** The indicators enable web searchers to consider the trade-off between privacy risks and the benefit of viewing webpages, as well identify more webpages that they are willing to view even if they accept some risks.

4 USER STUDY

In an online user study, we evaluated the effectiveness of the proposed snippet representations in terms of their ability to explain the risks related to behavioral data sharing in web searches. The user study was conducted in Japanese on August 14 and 15, 2021. We recruited 424 participants via CrowdWorks.jp [11], which is a Japanese crowdsourcing service. Prior to conducting the user study, we explained the data collection policy, and the participants proceeded only if they agreed that we could use the data collected during the search tasks. Note that we excluded 19 participants from the analysis as outliers because they did not complete the tasks or spent an unusually long time performing the tasks[12]. Thus, we analyzed a total of 405 participant responses (male = 56.5%, female = 42.7%, NA = 0.7%). Most participants were 30 to 50 years of age (20s = 17.5%, 30s = 30.6%, 40s = 28.9%, 50s = 15.3%, others = 7.7%). All participants who completed the tasks received 150 JPY (approximately 1 USD). On average, the participants finished all tasks within 429.8 s.

For this user study, we prepared four search tasks in two topic categories, i.e., shopping and health. For the shopping category, we prepared two search tasks, where participants searched for the best manufacturer of web cameras (or earphones) they would want to buy. For the health topic category, we asked participants to search for typical symptoms of diabetes or Meniere's disease to determine whether a symptom is relevant to the target disease. In each search task, the participants searched a prepared list of web search results to report their answers.

4.1 Search system

We developed a web-based search system to conduct the search tasks and monitor participant behaviors during the user study. The system generates privacy risk indicators for each web search result on SERPs as follows.

1. Web search results are fetched using the API of a conventional web search engine (e.g., Google or Bing).
2. Each search result (webpage) on the SERPs is assessed to determine whether it contains third-party cookies.
3. If a target search result contains third-party cookies, the system checks whether the issuing domains of the cookies (i.e., third-party domains) appear in a list of third-party domains detected for popular websites.
4. If search result X shares the same third-party domains with popular website Y, the system determines that the browsing histories on X can be shared to Y (i.e., website Y is a sharing destination).

For step 1, we issued the queries "web camera recommend," "earphone recommend," "diabetes symptom," and "Meniere symptom" into the Bing Web Search API[13] and obtained 100 search results for each query prior to conducting the user study. Each result on the SERPs comprised three components that are common to web search, i.e., the title, URL, and content description (i.e., snippet), as

[11] https://crowdworks.jp

[12] We calculated the interquartile range (IQR) of the log-transformed session times in the task. As outliers, we then excluded participants whose log-transformed session time was above Q3 + 1.5 IQR or below Q1 − 1.5 IQR.

[13] https://docs.microsoft.com/en-us/azure/cognitive-services/bing-web-search/overview

Table 1: Participant allocation.

	Search UI		
Search topic	Control	Icon	Ratio
Shopping	68	76	71
Health	62	67	61
Total	130	143	132

well as the privacy risk indicator. A SERP presented a list of 10 webpages (i.e., search results) matching the given query. The system paginated 10 SERPs for each query. Thus, each participant viewed at most 100 webpages for the given query. Although our SERPs imitated the SERPs of common web search engines, we configured the search system such that the participants could not modify the search queries on SERPs for each search task. There corresponding webpage was displayed when the participants clicked each search result.

For step 3, we prepared a list of websites using SimilarWeb.com[14], which is a web service that analyzes website traffic exhaustively. Using SimilarWeb.com, we created a list of the top 100 most frequently accessed Japanese websites for 24 main categories. Here, we refer to the listed 2400 websites as *famous websites*. Then, we analyzed the third-party cookies of the collected web search results to examine the presence of trackers. In steps 2 and 3, the prototype system analyzes third-party cookies in webpages using the open source **webXray** tool[15], which analyzes webpage traffic and content to identify companies that collect user data. Unfortunately, the **webXray** tool spends a long time scanning a webpage to detect third-party cookies. Therefore, we performed this analysis before conducting the user study.

4.2 Design and procedure

We adopted a between-subjects factorial design to examine the effects of the Icon, Ratio, and Control UIs. After the participants agreed to a consent form on a recruiting website, they were directed to the website for the user study. Then, we randomly allocated a search UI condition and a search topic category to each participant. Table 1 shows the allocation of UI conditions and topic categories.

First, the participants read a description of the task flow. In addition, the data collection policy was explained. Note that the participants proceeded with the user study only if they agreed that we could use the data collected during the search tasks. The participants filled out a pre-task questionnaire before performing each search task. In the pre-task questionnaire, the participants were asked about their awareness of privacy risks in web searches.

Then, each participant performed two search tasks for either the shopping or health topic category. Note that the task order was randomized for each participant. The participants browsed the list to formulate their answers. For all search UIs, we controlled whether the privacy risk indicators would be displayed on the web search results depending on search result ranks. As shown in Figure 3, the search system displayed the risk indicators only for web search results in odd-ranked positions. This manipulation was implemented to display web search results with and without the risk indicators as equally as possible. One purpose of this study was to examine how privacy risk indicators affect participant behaviors in web searches. We expected that this manipulation would enable us to compare the click counts of web search results with and without risk indicators. Once the participants reached a decision, they reported their choice on our study website. We then asked the participants to explain the reason for their decision.

Table 2: Statistical significance values reported from the pairwise comparison (Significant level at *: 0.05; **: 0.01; *; 0.001).**

Question	**Pair**		
	Control-Icon	Control-Ratio	Icon-Ratio
Q1	0.092	**	0.108
Q2	0.224	**	*
Q3	*	*	0.403
Q4	0.177	**	0.058
Q5	NA	NA	NA
Q6	NA	NA	NA
Q7	0.093	***	0.058
Q8	*	**	0.338
Q0	NA	NA	NA

After the participants completed all search tasks, they were asked to fill out an exit questionnaire. The exit questionnaire was designed to examine the change in the participants' privacy awareness in web searches and provide a subjective evaluation of the search UIs (see the questionnaire contents on the following URL [16]).

5 RESULTS

We analyzed 405 participant responses to examine the effects of the three privacy risk indicators on web search results. Here, we employed a nonparametric Kruskal–Wallis one-way analysis of variance (ANOVA) test for the three UIs because the collected data did not follow a normal distribution. We also used the Benjamini–Hochaberg FDR test [14] for multiple comparison tests in a posthoc analysis.

5.1 Questionnaire analysis

Table 3 shows the mean responses for the nine questions and the statistical significance of the ANOVA results. For Q0, we calculated the score difference between the responses to the questions about awareness of privacy risks before and after the search tasks. Higher mean values indicate more positive results to the UIs. Table 2 shows the pairwise comparison between the three UIs in posthoc analysis.

As can be seen, the mean values for Q1–Q8 were greater than three, which suggests that the participants generally felt positively about all three UIs. For several questions, the ANOVA and posthoc analysis results demonstrated a statistical difference between the UIs, especially between the Ratio and Control UIs.

[14] https://www.similarweb.com
[15] https://webxray.org/
[16] https://github.com/ymmt3-lab/GoodIT2022-shimizu/blob/main/GoodIT2022_questionnaire.pdf

Table 3: Mean, standard deviation, and statistical significance in ANOVA for questions in exit questionnaire (significance level at *: 0.05; **: 0.01; *; 0.001). Q1–Q8 were answered on a five-point Likert scale (1: Strongly negative; 3: Neutral; 5: Strongly positive).**

Question	UI			*p*-value
	`Control`	`Icon`	`Ratio`	
Q1. Search without concerns on privacy risks	3.88 (0.95)	3.66 (1.00)	3.45 (1.06)	**
Q2. Findability of search results with trackers	3.99 (0.93)	3.87 (0.93)	3.60 (1.01)	**
Q3. Usefulness to understand the extent of data leakage	3.32 (1.16)	3.75 (1.02)	3.64 (0.99)	*
Q4. Usefulness to avoid privacy-risky search results	4.02 (0.94)	3.87 (0.97)	3.58 (1.11)	**
Q5. Usefulness to find risky but valuable search results	3.75 (1.04)	3.59 (1.08)	3.54 (1.07)	0.25
Q6. Easy to search	3.93 (0.82)	3.82 (0.79)	3.86 (0.89)	0.52
Q7. Comprehensibility of representation	4.02 (0.80)	3.80 (0.99)	3.55 (1.03)	***
Q8. Willingness to use	3.82 (0.84)	3.57 (0.94)	3.47 (0.99)	**
Q0. Improvement of awareness on privacy risks	0.12 (0.69)	0.20 (0.61)	0.11 (0.63)	0.71

For Q1, Q2, and Q4 about privacy matters, the ANOVA results revealed significant differences between the three UIs (Q1: $p < 0.01$, Q2: $p < 0.01$, and Q4: $p < 0.01$). In addition, the posthoc analysis revealed that the mean responses for the `Ratio` UI were less than those of the `Control` UI for Q1, Q2, and Q4. With the `Ratio` UI, we found that the participants often felt more concerns about privacy risks during web searches than those using the `Control` UI (Q1 mean: 3.45 vs 3.88; $p < 0.01$). In addition, when using the `Ratio` UI, we found that the participants encountered more difficulty in terms of finding search results with trackers than the `Control` UI (Q2 mean: 3.60 vs. 3.99; $p < 0.01$) and `Icon` UI (Q2 mean: 3.60 vs 3.87; $p < 0.05$). Similarly, the participants generally found that the `Ratio` UI was less useful in terms of avoiding privacy-risky search results than the `Control` UI although the mean responses of the `Ratio` UI were greater than the neutral score (Q4 mean: 3.58 vs. 4.02; $p < 0.01$).

Note that we observed a different trend for Q3. The ANOVA results revealed significant differences between the three UIs ($p < 0.05$); however, the participants rated the `Ratio` UI (mean: 3.64) and `Icon` UI (mean: 3.75) more highly than the `Control` UI (mean: 3.32) compared to Q1, Q2, and Q4 (Q3; Control-Ratio: $p < 0.05$; Control-Icon: $p < 0.05$). In other words, the participants tended to judge the `Ratio` and `Icon` UIs as more useful in terms of supporting their understanding of which websites their browsing behaviors would be shared to once they clicked a search result.

For Q5, we did not observe statistical differences between the three UIs ($p = 0.25$). In addition, from a usability perspective, we observed significant differences for Q7 and Q8 between the three UIs (Q7: $p < 0.001$, Q8: $p < 0.01$). We found that the information provided by the `Ratio` UI (mean: 3.55) was more difficult to understand than that of the `Control` UI (mean: 4.02) even though the `Ratio` UI did not obtain negative scores so much (Q7; Control-Ratio: $p < 0.001$). We also found that the participants were more willing to use the `Control` UI (mean: 3.82) than the `Ratio` UI (mean: 3.47) and `Icon` UI (mean: 3.57) (Q8; Control-Ratio: $p < 0.01$; Control-Icon: $p < 0.05$). For Q6 (ease of search), we did not observe statistical differences between the three UIs ($p = 0.52$).

For Q0, all three UIs slightly improved the participants' awareness of privacy risks in web searches on average (Q0: `Icon`= 0.20, `Ratio`= 0.11, `Control`= 0.12). However, no significant differences were observed in terms of improving privacy risk awareness between the three UIs ($p = 0.71$).

5.2 Behavior analysis

We analyzed the dwell times on SERPs to investigate how much time the participants spent examining the list of web search results. The ANOVA analysis did not identify significant differences between the three UIs ($p = 0.49$).

Then, to investigate how carefully the participants scanned a list of web search results, we analyzed the time required to click a search result on the SERPs for the first time during the search tasks, (i.e., *time to first click*). As shown in Table 4, we did not observe significant differences between the three UIs ($p = 0.66$).

To investigate how much effort was required by the participants to scan a list of web search results, we examined the ranks of the search results that the participants clicked to analyze the maximum search result rank, which we refer to as *maximum click depth*. Here, we interpret a greater maximum click depth to mean that the participants viewed results that were deeper in the search result list. As shown in Table 4, the ANOVA results indicated no significant differences between the three UIs ($p = 0.98$).

To investigate whether each UI made the participants willing / unwilling to click webpages in the search result list, we analyzed how many webpages the participants viewed during the search tasks (i.e., *pageviews*). As shown in Table 4, we observed no significant differences between the three UIs for the total pageview count ($p = 0.23$).

As described in Section 4, the experimental search system displayed search results with and without privacy risk indicators alternately. If each search UI could enhance participants' awareness of privacy risks in the search results, the participants would attempt to avoid clicking search results with privacy risks. In addition, even if the search results display privacy risk information, if the participants determine that some search results have no privacy risks to view, they would click the results to obtain information. Therefore,

Table 4: Search behavior statistics. The mean, standard deviation, and statistical significance are shown (significance at *: 0.05).

Metric	UI condition			p-value
	Control	Icon	Ratio	
Dwell time on SERPs (s)	343.9 (259.9)	376.0 (299.1)	416.6 (333.7)	0.49
Time to first click (s)	32.5 (48.7)	32.9 (90.3)	27.6 (26.6)	0.66
Maximum click depth	6.87 (6.01)	7.76 (8.15)	7.77 (8.15)	0.98
Total page views	2.88 (2.10)	3.16 (2.25)	3.25 (2.19)	0.23
View count of extended search results	1.21 (1.26)	1.28 (1.29)	1.54 (1.26)	*
View count of non-extended search results	1.66 (1.34)	1.88 (1.59)	1.70 (1.48)	0.50

we also examined how many search results displaying privacy risk indicators the participants clicked during the search tasks (i.e., *view count of extended search results*).

As shown in Table 4, the ANOVA analysis indicated significant differences in terms of the view count of extended search results between the three UIs ($p < 0.05$). The posthoc analysis revealed that the Ratio UI had a larger mean view count of extended search results (1.54) than the Control UI (1.21) ($p < 0.05$). It is possible that the Ratio UI encouraged the participants to click more search results regardless of the presence or absence of privacy indicators. Thus, we also examined how many search results without privacy risk indicators the participants clicked during the search tasks (i.e., *view count of non-extended search results*). Here, we observed no significant differences between the three UIs in terms of view count of non-extended search results, as opposed to the view count of extended search results ($p = 0.50$). These results indicate that the Ratio UI could encourage the participants to click more search results with the indicator than the Control and Icon UIs even though such results could monitor the participants' browsing behavior logs.

6 DISCUSSION

In terms of improving privacy risk awareness, the questionnaire analysis revealed no significant difference between the three UIs, and we found that the UIs did not improve the awareness of privacy risks so much (Q0 on Table 3). On the other hand, the results of the statistical analysis indicated that the participants felt that the Ratio UI was less useful in terms of searching the web without concerns about privacy risks than the Control UI (Q1). In other words, this result implies that the Ratio UI better enhances the awareness of privacy risks in web searches compared to Control UI. Therefore, we conclude that **H1** is weakly supported.

We expected that the Icon and Ratio UIs would encourage the participants to scan a list of web search results more cautiously than the Control UI. However, the behavior analysis revealed no significant differences between the three UIs relative to the participants' behaviors toward the web search (i.e., dwell time on SERP, time to first click, maximum click depth, and the total number of page views). Therefore, we conclude that **H2** is not supported.

On the other hand, the behavior analysis revealed that participants using the Ratio UI tended to browse search results embedded with trackers more actively than the Control UI (refer to the view count of extended search results shown in Table 4). On the other hand, no significant differences were observed between the three UIs for the pageview count of the search results without trackers (i.e., the view count of non-extended search results in Table 4). These results suggest that the participants using Ratio UI could intentionally browse more webpages with tracking risks. In other words, compared to the Control UI, the Ratio UI could encourage the participants to identify webpages that they are willing to view even if they accept some degree of risk. From these results, we conclude that **H3** is supported.

One limitation of this study is related to the detection of trackers and browsing history sharing destinations. The prototype system used third-party cookies to determine whether the web search results include trackers and to find which popular websites browsing histories could be shared to. The use of third-party cookies on web browsers is ending; thus, other methods to track online user behaviors are becoming increasingly popular, e.g., browser fingerprints. This study focused on privacy risk representations, and the proposed UIs are independent of sharing detection methods; however, in future, we plan to explore other effective methods to detect browsing history sharing using the latest tracking technologies. Furthermore, prototype system assumed that websites with trackers can share browsing histories with advertising agencies; however, some websites may use trackers only for access analysis (rather than targeted advertising). Different websites employ tracking for different reasons; thus, the proposed privacy risk indicators should identify the tracking purposes with the privacy risk levels to web searchers.

Another limitation is related to the conditions of the user study. Through an online user study via a crowdsourcing service, we roughly examined how the proposed privacy risk indicators affected web searchers' privacy awareness and behaviors. However, we did not investigate in detail what the participants were thinking while using the proposed systems during the search tasks. It is difficult to convey and examine privacy issues only via online studies; Thus, laboratory studies should be conducted in future for more effective analysis. In addition, we have to examine the difference of the UI effects depending on search topics. Furthermore, further studies on cultural differences are also required because our user study only examined the effect of the proposed UIs in a Japanese context.

7 CONCLUSION

In summary, the Ratio UI was useful in terms of understanding the sharing destinations of browsing histories in web searches. In addition, it encouraged participants to identify webpages that they are willing to view even if they accept some risks. Thus, if web searchers can learn the number of browsing history sharing with the destination category on SERPs, they can effectively consider the trade-off between tracking risks and the benefits of information access.

ACKNOWLEDGMENTS

The work was supported in part by the Grants-in-Aid for Scientific Research (18H03244, 18H03554, 18H03775, 22H03905) from the MEXT of Japan.

REFERENCES

[1] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz. 2014. The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. In *Proceedings of the 2014 ACM Conference on Computer and Communications Security (CCS 2014)*. 674–689.

[2] Tomasz Bujlow, Valentín Carela-Español, Josep Solé-Pareta, and Pere Barlet-Ros. 2017. A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proc. IEEE* 105, 8 (2017), 1476–1510.

[3] Farah Chanchary and Sonia Chiasson. 2015. User Perceptions of Sharing, Advertising, and Tracking. In *Proceedings of the 11th USENIX Symposium On Usable Privacy and Security (SOUPS 2015)*. 53–67.

[4] Steven Englehardt, Dillon Reisman, Christian Eubank, Peter Zimmerman, Jonathan Mayer, Arvind Narayanan, and Edward W. Felten. 2015. Cookies That Give You Away: The Surveillance Implications of Web Tracking. In *Proceedings of the 24th International Conference on World Wide Web (WWW 2015)*. 289–299.

[5] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using Personal Examples to Improve Risk Communication for Security & Privacy Decisions. In *Proceedings of the 2014 ACM Conference on Human Factors in Computing Systems (CHI 2014)*. 2647–2656.

[6] Spyros Kokolakis. 2017. Privacy Attitudes and Privacy Behaviour. *Comput. Secur.* 64, C (jan 2017), 122–134.

[7] Luis A. Leiva, Ioannis Arapakis, and Costas Iordanou. 2021. My Mouse, My Rules: Privacy Issues of Behavioral User Profiling via Mouse Tracking. In *Proceedings of the 2021 ACM Conference on Human Information Interaction and Retrieval (CHIIR 2021)*. 51–61.

[8] Pedro Giovanni Leon, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. 2013. What Matters to Users? Factors That Affect Users' Willingness to Share Information with Online Advertisers. In *Proceedings of the 9th USENIX Symposium on Usable Privacy and Security (SOUP 2013)*. 1–13.

[9] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. 2018. Characterizing the Use of Browser-Based Blocking Extensions to Prevent Online Tracking. In *Proceedings of the 14th USENIX Symposium on Usable Privacy and Security (SOUPS 2018)*. 103–116.

[10] Aleksandar Matic, Martin Pielot, and Nuria Oliver. 2017. OMG! How Did It Know That?: Reactions to Highly-Personalized Ads. In *Proceedings of the 25th ACM Conference on User Modeling, Adaptation and Personalization (UMAP 2017)*. 41–46.

[11] Jonathan Obar and Anne Oeldorf-Hirsch. 2018. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23 (07 2018), 1–20.

[12] Joseph Phelps, Glen Nowak, and Elizabeth Ferrell. 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing* 19, 1 (2000), 27–41.

[13] Joel Reidenberg, Travis Breaux, Lorrie Cranor, Brian French, Amanda Grannis, James Graves, Fei Liu, Aleecia McDonald, Thomas Norton, Rohan Ramanath, N. Russell, Norman Sadeh, and Florian Schaub. 2014. Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. *SSRN Electronic Journal* (01 2014).

[14] David Thissen, Lynne Steinberg, and Daniel Kuang. 2002. Quick and easy implementation of the Benjamini-Hochberg procedure for controlling the false positive rate in multiple comparisons. *Journal of educational and behavioral statistics* 27, 1 (2002), 77–83.

[15] Janice Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research* 22 (01 2011), 254–268.

[16] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proceedings of the 8th USENIX Symposium on Usable Privacy and Security (SOUPS 2012)*. 1–15.

[17] Antoine Vastel, Pierre Laperdrix, Walter Rudametkin, and Romain Rouvoy. 2018. FP-STALKER: Tracking Browser Fingerprint Evolutions. In *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP 2018)*. 728–741.

[18] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A Field Trial of Privacy Nudges for Facebook. In *Proceedings of the 2014 ACM Conference on Human Factors in Computing Systems (CHI 2014)*. 2367–2376.

[19] Yusuke Yamamoto and Takehiro Yamamoto. 2020. Personalization Finder: A Search Interface for Identifying and Self-Controlling Web Search Personalization. In *Proceedings of the ACM/IEEE Joint Conference on Digital Libraries in 2020 (JCDL 2020)*. 37–46.

[20] Steven Zimmerman, Alistair Thorpe, Chris Fox, and Udo Kruschwitz. 2019. Privacy Nudging in Search: Investigating Potential Impacts. In *Proceedings of the 2019 ACM Conference on Human Information Interaction and Retrieval (CHIIR 2019)*. 283–287.