User Privacy Protection Issues of Safari

Is Safari a good privacy browser as it claims to be?

Junjie Yue
University of Illinois at Urbana-Champaign

1 Introduction

As we become more and more like digital entities in the virtual world, our concerns over digital privacy get much stronger, which directly drives the formation of a new battleground about user privacy among different browsers. Many of them have launched their methods to protect user privacy. Being one of the leading companies in the field of information technology, Apple has announced some new features of Safari in Apple's Worldwide Developers Conference in 2018. The current version of Safari we are using can protect us explicitly while a website is trying to grasp our cookies or other kinds of data. It can also block the "fingerprinting" approach, in which others may use publicly accessible information about devices we use.

Apple and its products are always being compared with other companies and their products. I am curious about whether Safari is a good privacy browser as it claims to be? And when it comes to an ethical problem, how well it is good at dealing with it.

To answer this question, I would like to divide this question into several small questions. First, what is Internet privacy and what kinds of threats we are facing. Second, according to users or in eyes of users, what kind of privacy protection is expected from a browser, and what are their certain criterions about it? Furthermore, users of browsers are very diverse, with different needs, abilities, cultural preferences etc. They use browsers for diverse purposes. These differences between can affect whether the user is concerned about privacy, how they understand privacy, whether they are able to take measures to protect themselves. Some people are more vulnerable than others to privacy violations. Third, recent years have seen so many cases on how browsers breach our personal information, and the social impacts they have on the whole society. Among them, what are the ethical problems that people care about the most? After knowing the expectation and the most concerned ethical

issue people have, we can estimate whether Safari is a good privacy browser or not by comparing it with other browsers and analyzing whether the function it offered has met users' satisfaction.

2 Literature review

2.1 Users' Concerns About Internet Privacy

Understanding and enhancing personal privacy protection on the Internet has been a critical issue with the widespread use of information systems and the Internet. Many researchers have focused on what are the issues people concern most about their Internet privacy. In a survey conducted in 2002, it revealed that Internet users basically cared about information transfer, notice/awareness, and information storage. However, online privacy policies focused more on data integrity/security, information collection and user choice/content. Therefore, they found out that the top three privacy concerns of Internet users didn't align with the most emphasized items in online privacy policies.

Six years later, they created and validated another survey which suggested that the top three privacy concerns among Internet users haven't changed since 2002, but there are some certain topics about which people's level of concern has been influenced. For example, according to the result of the survey, individual's level of concerns about data collection has increased specifically. The disclosures of purchasing patterns and trading personal identifiable information to third parties are the issues about which people cared the most. Web sites tend to use such kind of collected data to better place personalized advertisements for targeted marketing [1].

Internet browsers are more like windows that by looking through which there is a broad world awaiting us to explore, while others can look at us at the same time and abuse the personal identifiable information they gained from us. The techniques they use are various, but the major two of them are extensions and fingerprinting methods.

2.2 Internet Browsers

It is safe to say that the Internet gained its popularity due to the introduction of Internet browsers. They provide us with a platform that we can easily surf the Internet and interact with others. The first browsing tool is Netscape which was created in 1995 and later that year Internet Explorer was bundled up with the operating system of Microsoft. Firefox and Safari was introduced in 2003, and Chrome in 2008. Although Chrome is the browser that has been introduced the most recently, it is now the most popular desktop browser worldwide with a 64% market share in Oct. 2019 [2].

2.3 Browser Extensions

As the internet is becoming more complex and the scale of data being stored is getting larger, browser extensions provide us the conveniences and accessibilities we need to help us better our experience while surfing the Internet.

However, this is only true when the extension is written by trusted developers and is censored by the third party like the company that introduced the browser to guarantee that it can safeguard users' privacy. Otherwise, the extension can be written to extract privacy information and use it for purposes that users would not agree to. According to the work of Steven Ursell and Thaier Hayajneh, there are basically three concerns about extension privacy. First, the agreement statements of extensions are not always understandable for all users. Second, the header that indicates the webpage the user is browsing can be collected by HTTP Referer header information. Third, warnings from the programs while being used are usually ignored by users and are not easily understandable as well. After examining the extensions used by Chrome and Firefox, they made a conclusion that users are not aware of the powerfulness of extensions and the damage they can cause if written by some untrusted developers. A decision tool is needed to narrow the gap between the expected functions of the extension from users and the work that it actually does [3].

2.4 Fingerprinting

Besides extensions, fingerprinting techniques deserve our attention when it comes to Internet privacy issues. It is more likely for big companies to store the user information due to the advantages of big data. Thus, they fail to self-regulate and enhance a formation of a dysfunctional information market which put more users in danger [4]. When discussing Internet privacy and users' resistance against malicious websites, we have to consider fingerprints alongside cookies. More and more people are becoming aware that storing HTTP cookies has a potential risk of information bleach ,and some of them will block the storage function of cookies data in their browser setting or delete local cookies completely. In the experiment conducted by Soltani et. al., more than half of the websites in their sample will use Flash cookies, some of which can even be used to recover HTTP cookies that had been deleted by the user [5]. It is basically impossible for a user to tackle the attack from a well-developed fingerprinting malware, since certain kinds of debuggability weight more than the protection against fingerprintability in current browsers [5]. What's more, it is unlikely that normal users will notice the deeply-hidden fingerprinting techniques which are usually not mentioned neither in the statement of browsers nor in the websites we visit.

While surfing the internet, it is easy to leave traceable marks both locally and remotely, such as the history of visited webpages, terms searched, cookies, password we typed, personal information we used by using some online application, etc.. Many web browser companies attach great importance to user privacy, which renders the introduction of private mode which is supported by the most of widely used browsers. Some previous researches are conducted to examine the privacy protection abilities of these browsers while using private mode.

2.5 Private Mode

In 2010, Aggarwal et. al. created a specific criteria for the goals of private mode and set up a threat mode to test several browsers whether they have meet the

expectation. There are basically two kinds of attackers: local attackers who can control the computer after the user has triggered the malware unconsciously while visiting some malicious web pages and web attackers who can control the website the user visits. During one of the experiments, the local attacker totally disabled the safeguard functions of the private mode [6].

The similar kind of situation occurred when Said et. al. did another investigation on the effectiveness of the privacy mode supported by three web browsers which are Internet Explorer, Chrome and Firefox. The method they used to identify traces after private mode browsing has three phases. First, examine history and cache records. Second, use forensic tools to examine other places on local machine. Finally, look for the traces in RAM. They made a conclusion that although history and cache records are deleted, it is still likely for attackers to extract information from RAM as long as the computer is running [7].

Based on the work of researches mentioned above, Satvat et. al. refined the threat method used in [4] and investigated more angle than [7], which means they also scrutinized in network and network traffic. In terms of Safari, one of the major method it uses to eliminate traces of visiting history is erasing the records which is written in the SQLite database when the private mode is closed normally. Otherwise, if we terminate the Safari window manually, the records will not be deleted. These private browsers disclosures complex vulnerabilities due to mainly three reasons: a lack of comprehension of threat model, a lack of control of running extensions, and a lack of systemic tests [8].

There is another experiment which is conducted specifically to test whether traces will be discarded after using the privacy mode in some web browsers. The method they used are forensics tools as well. In the result part of their work, we can see that Safari didn't pass the text since they still found the browsing data in a file named "WebpageIcons.db". It seems that Safari didn't completely discard the traceable information of users while using privacy mode as it claims to do [9]. Notably, among eight browsers that had been texted, only Chrome and Firefox had passed their test. However, using the tools mentioned in [8], they are not the most perfect privacy protection browsers at all.

2.6 Privacy by Design

We have reviewed some work that focuses on the perspective of users and illustrates how different malicious programs will invade users' privacy and how browser vendors seek to handle such kind of problems. However, as an Internet of things (IoT), it is vital to know how do we consider privacy protection issues in the first place and regulate developers to pay more attention to related values in the process of developing the browsers.

Explicitly emphasizing the privacy-by-design(PoD) guidelines can help generate a more privacy- aware IoT, and these guidelines will help both novice and expert software engineers work more efficiently on the privacy designing of IoT [10]. As for how to launch socio-technical design approaches which privacy is considered as a key value, Degeling et. al. proposed that all stakeholders should participate in the processing models which makes

the basis of PoD . It is an adaption that can support a collective work when it comes to issues that relate to personally identifiable information [11]. In addition, the work of Pattakou et. al. evaluated to what degree the existing usability criteria can be used to measure the methodologies used in the PoD development [12].

3 Description & Analysis

3.1 Apple's Attitude Towards Privacy Protection

"Privacy is a fundamental human right. At Apple, it's also one of our core values." This is the first sentence we will see on the web page of Apple Privacy. Actually, Apple's attitude towards privacy has always been fairly aggressive and it touted itself for being more privacy-conscious than its competitors like Google.

Although it is never clear, as somebody said online, whether it is a hypocrite that uses privacy protection as a business strategy, Apple has done a lot of work to protect users' privacy as they claim to do. For example, Apple is the first company that lunched the privacy mode on its browser. Besides that, whenever there is an app on iPhone wants to access the location of the user, the permission from users is always required since 2010, because Apple doesn't trust the app developers thus force the app to get users' consent. The funder and the former CEO of Apple Steve Jobs said that privacy protection is taken "extremely seriously" by Apple.

As it is mentioned above, targeted advertising is one of the most important way for advisers to make money. Facebook and Google make a fortune without coasting a penny just by allowing advertising on their platforms. It is ubiquitous and inevitable that our information such as search history, personal identifiable information, automatically filled-in passwords, sometimes even credit card numbers and SSN will be captured by many websites. However, Apple said no to such kind of information invasion.

Many advertisers accused Apple for destroying the basic economic structure of Internet business, and requested Apple to reconsider the feature of its advertisement-blocking method attached to Safari. However, Apple decided not to disable this function on Safari. "Apple believes that people have a right to privacy" said by an Apple representative [13].

Not only Apple didn't back down, it took this method even further after advertisers picking up a fight over this "intelligent tracking prevention " feature. At Apple's Worldwide Developers Conference in 2018, Apple announced a set of new constraints on Safari that helped to prevent not only online ads, but also some cookies extracting and fingerprinting techniques used by certain websites [14]. As it is mentioned in the literature review that by capturing cookies and fingerprinting information about the users' devices, we can gain much private information of a user. Here are more specific scenarios. In terms of cookies, advertisers can use them to serve multiplatform ads. For example, when you searched a certain item on Amazon, the ad of that item will show up on your Facebook, this is because cookies.

As for fingerprinting, it is a technique that can identify you by analyzing

the information your browsers send back to the websites while you are visiting them. For example, by recognizing the fonts your browser is using, the extensions you have installed, and the current version of your browser etc. , the website can easily identify your machine very well. Apple chooses to say no to all of this. Not only by controlling the information get by the websites, but also by controlling what kind of information can be sent out by your browser [15].

However, some people say that Apple is a hypocrite that it doesn't attach much importance to user privacy as it claims to do.

As it has been reported by TechCrunch, Facebook pays teens to install VPN that spies on them [13], which Facebook didn't deny that they were using the data collected to analyze the usage habits in a research program, and the outcome of which will be used to better its data used for advertising and painting a portrait of competitor behavior. After the news was broken, Apple took a seemingly immediate action by shutting down the iOS version of the program, which is more like a moral cover than doing something that the company claims to oppose.

Facebook and Google seem to be the biggest winner of the online targeted advertising by using data collecting methods that are regarded as privacy invasions by Apple. However, Apple itself has benefitted a lot just by making a cooperation with these so called privacy offenders and saying it takes user privacy "extremely seriously " at the same time. For example, just simply by prioritizing Google as the default search engine, Apple can get paid 12 million [16] from Google this year. Google has always been accused by using questionable data. Apple is also an indirect part of the problem since it has such an acquiescent attitude and gives this privilege to Google [17].

3.2 Privacy Protection Features of Safari

According to the white paper of Safari (Safari Privacy Overview) which was released Nov. 2019 [18], there are several aspects mentioned how Safari will protect users' privacy. Among which there are two of them I want to discuss.

3.2.1 Privacy by design

Safari has been designed from the ground up to protect user privacy. Key privacy features like Intelligent Tracking Prevention (ITP) and fingerprinting defense are turned on by default. Safari minimizes the amount of data collected by Apple and shared with third parties. Where possible, Safari's privacy protections are designed to process data on device. Safari also limits the amount of information passed to search engines when a user searches using the Smart Search field. Safari is designed to provide users with transparency and control around data that is shared. Safari implements security best practices to protect user data. (Apple Inc. 2019)

As it is mentioned above, there are two primary features of Safari that can protect users from the malicious invasion of privacy information: ITP and fingerprinting defense. Safari got an "intelligent tracking prevention" feature in Safari 11 which was launched in 2017. This feature sufficiently blocked a large amount of online advertisements, and in many other browsers such kind of features are not even an option. This privacy protection setting is set

by default which meets the transparent criterion that is mentioned in [12]. Transparency means users don't have to understand how some functions of the system work in the human- computer interaction while they are using it. Google and Facebook have so many data-bleaching sandals in recent years, and they still collecting data from users as a way to make profit. In the case of Apple, Safari collects information from users as well. The personal information being collected includes mailing address, phone number, email address, contact preferences, device identifiers, IP address, location information, credit card information and profile information. [19] Instead of giving the information collected to third party companies, Apple will use it to advertise other products made by Apple, such as the update of software, upcoming events etc. . In addition, some non- personal information will be collected as well to analyze the purchase pattern of certain groups of people.

3.2.2 Protection from cross-site tracking

In the years since the web was created, technology has been developed to track user behavior across websites for advertising purposes. Users experience this tracking in action when they look at a product online and then ads for that product seem to follow them around the web. Tracking is pervasive; some websites include 100 or more trackers from different companies on a single page. (Apple Inc. 2019)

This is one of the most strict anti-ads features of Safari, which is the least liked by online advertisers. This function allows Safari to block the tracking of some web sites intelligently. However, some supporting functions of the web page is also blocked by the ITP, when it comes to such kind of situations, Safari will ask for users consent.

In order to know whether this function works, I did a small experiment. It is very common to see related ads on Facebook when we used Facebook account to login some other websites. As it is stated above, if I use Safari private mode to surf such kind of websites and the protection from cross-site tracking works, there would be no relevant ads appear on my Facebook. So I opened a new private window and searched "car rental" , there are multiple results and I just clicked the first link (https://www.kayak.com). I searched for a rental car at that site after logging in with my Facebook account. When I had chosen a car to see whether it was still available , the web page popped up to another page (https://www.expedia.com). After that I closed all the windows. Then I logged into my Facebook on the phone and I was surprised to find that I saw the advertisement of Expedia after a few refresh of the front page.

4 Discussion & Conclusion

Apple, as one of the biggest companies should have a sense of social responsibility. Its attitude towards privacy is quite robust and aggressive. Safari is one of the most popular browsers among Internet users and the privacy protection methods has drew attention from not only users, but also competitors, relevant researchers and social media.

In conclusion, there are several features asserted in Safari to prevent the invasion of users' privacy. First, private mode of Safari can realize the most basic functions of private browsing. The function that can automatically fill-in passwords is still available but the newly created passwords will not be stored. In addition, after the user closes the private window normally, all the local cookies and browsing history will be eliminated in the SQLite database of Safari. However, if terminated by the Activity Monitor, some cookies will still remain in the database. Second, the functions are usually invisible to normal users, which are Intelligent Tracking Prevention (ITP) and fingerprinting defense, are set as default settings to protect users. These are the most important and unique features of Safari. In summary, the goal of these features is to protect users from cross-site advertising and personally identifiable information by blocking the tracking functions that can extract browsing cookies and detailed information about devices that can be used to individually identify users.

These malicious functions are used excessively by companies that serve personalized online ads. What surprised me the most is the small experiment I did to test the privacy protection ability of Safari. It turned out that Safari didn't protect me from cross-site advertising as it claimed to do. As for the reasons, I think Facebook is to blame, since I logged in the website using a Facebook account. Even if I was using a private window of Safari, it couldn't prevent Facebook from getting the purchasing information and post targeted ads on the front page of my Facebook. This paper provides a perspective of a normal user tin understanding the Internet privacy and an actual experience of using the private mode of Safari.

There are several limitations in this paper. First, some detailed technologic methods are not used in this paper, for example, some forensic tools used by researchers mentioned in the literature review since I focused more on the ethical analysis of whether Safari can protect users' privacy very well. Second, it would be better to make a comparison between Safari and other browsers to demonstrate the problem.

References

1. A.I. Antón, J.B. Earp, and J.D. Young. How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy*, 8(1):21–27, 2010.

2. Statcounter: Desktop browser market share worldwide. statcounter, 19 nov 2019.

3. *Desktop Browser Extension Security and Privacy Issues*, Cham, 2019. Springer.

4. S.E. Peacock. How web tracking changes user agency in the age of big data: The used user. *Big Data & Society*, 1(2), 2014.

5. A. Soltani, S. Canty, Q. Mayo, L. Thomas, and C.J. Hoofnagle. Flash cookies and privacy, 2009.

6. *An Analysis of Private Browsing Modes in Modern Browsers*, Vancouver, 2010.

7. *Forensic analysis of private browsing artifacts*, 2011.

8. *On the privacy of private browsing–a forensic approach*, Berlin, Heidelberg, 2013. Springer.

9. E.S. Noorulla. Web browser private mode forensics analysis, 2014.

10. C. Perera, M. Barhamgi, A.K. Bandara, M. Ajmal, B. Price, and B. Nuseibeh. Designing privacy-aware internet of things applications. *Information Sciences*, pages 238–257, 2020.

11. *Privacy by socio-technical design: A collaborative approach for privacy friendly system design*. IEEE, 2016.

12. *Towards the design of usable privacy by design methodologies*. IEEE, 2018.

13. Shankland S. Web browser private mode forensics analysis, 2017.

14. N Lily Hay. Apple just made safari the good privacy browser, 2018.

15. Shankland S. New safari privacy features on macos mojave and ios 12 crack down on nosy websites, 2018.

16. M. Sullivan. At $ 12.85 per iphone, google's default search payment is probably a steal, 2018.

17. I. Bogost. Apple's empty grandstanding about privacy, 2019.

18. Apple Inc. Safari privacy overview, 2019.

19. Apple Inc, 2019.