Informing Users About Fingerprinting

By: Salomon Höglund

Supervisor: Helge Hüttenrauch
Södertörn University | School of Natural Sciences, Technology and Environmental Studies
Master’s dissertation 30 credits
Media technology | Spring semester 2019
Interactive Media Design Programme
Informing Users About Fingerprinting

Salomon Höglund
Södertörns högskola
Stockholm, Sweden
hoglund@protonmail.com

ABSTRACT
In peoples hyperconnected lives, a price to pay is their internet privacy and the different risks it faces the second their browser connects to the web. One such risk comes from how web tracking collect and analyze users information. This paper explores an approach to how web browsers can inform its users about the web tracking technique Fingerprinting, and through the concept presentation of this approach see: what key key aspects of visual aesthetics that affects the users experience when being informed; and to what extent differences in technological interest and knowledge affect users perception of Fingerprinting information, and the implementation implications the differences leads to. For this purpose a high fidelity prototype was created to: represent the concept of web browsers having integrated educational pages meant to inform its users on topics such as Fingerprinting, and to; be used in a user test. The results showed: a lack of knowledge on the existence of Fingerprinting; that differences in technological interest and knowledge among users affected what aspects of visual aesthetics they valued; and that those with less technological interest and knowledge to a higher degree had their attitudes towards Internet Privacy affected by the prototype’s information. It also showed that the differences affects users approach and interactions with software, and that the design implications this brings are to be considered for future browser functionality implementations.

Author Keywords
Fingerprinting; Human-Computer Interaction; Interaction Design; Internet Privacy; User Experience; User Interface; Visual Aesthetics; Web Tracking

1. INTRODUCTION
With the World Wide Web and its first web browser, WorldWideWeb [34], Tim-Berners Lee offered people a window to a world of information in its connection to the internet. Since then, a lot in society have transitioned to the digital world of the web, leading people to live hyperconnected lives, being “available for communication anywhere and anytime.” [28] This constant connection also enables the tracking of people's lives online through different web tracking techniques. One such technique is called Fingerprinting, which this paper will take a look at and explore an approach for how people can be informed about its existence and workings. Through this exploration, the paper also contributes knowledge on how differences in technological interest and knowledge among users can affect; what aspects of visual aesthetics they value; and their approach and interactions with software, such as browsers.

1.1 Internet Privacy
When more of our daily activities are moved to the internet, so are people's personal information, one way or another. A way for this to happen is through those who willingly give out their personal information, which can for example happen when signing up for services or buying things. This willingness have been found to be connected to people’s internet usage, in that those “who spend more time on Internet per week are more willing to give their personal information” [10], as well that more time lead to an increase in trust. This trust Joinson et al. [18] described as something that “operate in a symbiotic relationship” with privacy, which could lead to that “people may be willing to forgo privacy concerns when faced with a trusted requestor”. This relationship between willingness, time spent, and trust is bound to affect and spill over to the area where people spend most of their time on the internet, Social Media [14]. Its rise in use and popularity have, besides connecting people, contributed to that privacy should be considered “as a collective concept” [30]. That it is not only the personal information people willingly give out themselves that warrants policies and concern, but also the information that’s involuntary given out by other people, for example through the upload of pictures or their device’s contact lists to social media services. Besides information that is willingly or involuntary given, there is also that which is taken through the means of web tracking.

1.1.1 Web Tracking
The concern for people’s privacy expresses itself in part through the actions they take to protect it. Unfortunately, it is not as easy as it might seem to take action to avoid such things as web trackers, that collect information regardless whether people like it or not. Especially with the billions of dollars on the line in the internet advertisement business [4] Ad blocking browser extensions would have to be installed separately for every browser on every device in a person's possession, and these would still not cover and offer protection for software used outside of web browsers, as apps on a phone for example. This problem echoes in Acar et al.’s work which “suggests that even sophisticated users face great difficulties in evading tracking techniques” [1]. Sometimes there is also the case of misconceptions over the actions people take, in the belief that it would help protect them from web tracking, such as that 41 percent believed browsing in the Private Mode would protect them from being tracked [11].

1.1.2 Fingerprinting
One web tracking technique that is particularly difficult to deal with is called Fingerprinting [35]. It works on the basis that web browsers automatically reveal a lot of information about itself to websites you visit, as a kind of browser leakage. Such information is among other things tied to the web browser itself and the device on which it is being used, as for example the IP location, operating system, and browser and renderer version. With this web tracking technique, this information may be analyzed through the combination of every piece of revealing information and used in the creation of a digital fingerprint, a string of information that could be unique to you. This digital fingerprint can in turn be used to identify you and your web browser, and allow you to be tracked on the internet. But unlike a Browser Cookie, this is also not a file that can be deleted. An aspect of what makes Fingerprinting particularly difficult to deal with is that the information is revealed and acquired passively and actively [35]. Passive fingerprinting is based on information that is included in a web request the web browser
send to a server to access and download its content when visiting a website. This information is thus acquired by the server even before the content and its web page is returned in a response to the web browser. Active fingerprinting includes when for example the programming language JavaScript is used to get access to information. Although the act of disabling JavaScript is considered a “powerful defense against browser fingerprinting” [27], it come at a cost, in that JavaScript is commonly used on the websites of the internet and such an act would risk to break a lot of functionality, examples of such is that Facebook can not be accessed or that YouTube can not load any content. With other forms of defenses and privacy enhancing technologies there also lies a paradox, as Eckersley [12] called it. In his paper he states that measures meant to be a protection and concealment from Fingerprinting can rather make people stand out in the crowd “unless a lot of other people also take them”. As an example he mentions an privacy-enhancing browser that because of its rarity made its’ users in the data set unique.

1.1.3 Privacy Awareness

Based on the content that is included in the server response to a user’s web browser when visiting a website, the response can be used by ad blocking browser extensions. Because of this, such browser extensions have the ability to display for its users the web trackers it blocks, most commonly through their icons, main panels, or alert bubbles. What this display influence in users is looked at in a study by Schaub et al. [31], where they wanted to see its “impact on user privacy awareness and concern” in one hour test sessions. Although they found that the browser extensions affected users awareness, the users also “remained confused about many aspects of data tracking”, such as what data web trackers collect. To further help improve upon the user’s awareness, Malandrino et al. [22] created a privacy-enhancing tool, NoTrace, that could build a bridge over the gap between who and what, providing both protection and information [32]. While its functionality and content was contained to inside the tool itself, there are other thought of approaches. One such is Ackerman’s and Crano’s work on Privacy Critics [2], which they describe as “semi-autonomous agents that help people protect their online privacy by offering suggestions and warnings”. The idea would be that they pop up as an alert bubble [31] but provide a more comprehensible kind of information and an offer for interaction, depending on the content of the information.

1.1.4 Privacy Informing

To provide users with more of a context on tracking, more precisely behavioral tracking, Willis and Zeljkovic [36] created the website WhatTheyKnow, which was meant to show and educate users on how behavioral advertising is used to track them through their behavior on the internet. The website presented tailored information for its users based on the user’s browsing history, which was accessed with JavaScript, and combined this with “demographic information these sites may be inferring from these visited sites and the user’s geographic location”. Among the visiting users who partook in the survey, there was a bigger concern about the the “monitoring of activities” than it was over their IP-based location information. However, those concerned were “only slightly more likely to take preventive actions”, which show the long and winding road of getting people to take such actions on their own. This mirrors Spinelli [32] findings in his work where he put internet privacy up against users skills and its mutual influence. There, it was shown that the less skillful “exhibit a little willingness to adopt privacy preserving technologies” while also being more concerned about the risks of internet privacy than their counterpart [32]. This concern comes despite the two groups of less and more skillfulness put the same value on their privacy otherwise. Akhawe and Porter Felt [3] suggested that a “greater degree of technical skill [...] corresponds to reduced risk aversion”, and thus resulting in those users being more confident in their use of computers. Spinelli’s [32] work also showed little knowledge among the less skillful group of users in regards to behavioral advertising and the risks it poses. It should be noted though that the skillful group in the study, recruited from a computer science department, represents a comparatively expertise in the field.

1.2 Study Design

The study itself was built around the idea of what it could have looked like if the web browsers themselves took more responsibility and a different approach in informing users about Fingerprinting. That approach would be in the concept of web browsers having integrated pages meant to inform its users on browser and internet related topics such as Fingerprinting. Based on this, a high fidelity prototype was created to reflect this concept and to be used as part a user test.

Through this procedure, I will in my study seek answers to:
1. What key aspects of visual aesthetics from the prototype affect the users experience when being informed about Fingerprinting?
2. To what extent do differences in technological interest and knowledge affect users reception of Fingerprinting information, and what implementation implications does it lead to?

The paper is from here structured as follows. First there is an introduction to the creation of a high fidelity prototype and its content. This is then followed by the conducted user test with nine participants, and leading into a review of the gathered data from said user test. Finally, there is an discussion surrounding the findings on how the prototype was received and any discovered implementation implications.

2. PROTOTYPE CREATION

For the presentation of the prototype for the user test, I wished to include the feeling of using a web browser, which is why it was made as a high fidelity prototype and created as a web page through HTML and styled with CSS, and not as a put together image file. As an actual web page, the prototype could easily be accessed through an web browser and stay close to how it would be experienced in a live situation.

With the idea and concept of the prototype being an actual integrated part of a web browser, the choice fell on Google Chrome to be the model, since this web browser had a large majority of the web browser market share [33] and thus the most likely choice of web browser among the user test participants. The prototype was built upon Material Design Lite [13], a web design front-end template. Material Design Lite is created by Google, and made to follow Google’s own design language, Material Design [15]. This design language is used across Google’s products and services, including their web browser Google Chrome. The area where the already existing integrated pages and functions are located is chrome:// followed by the section’s name, for example chrome://settings. The look of this area is what the prototype striving for, in terms of for example colors, typography, and placement.

The data information used as examples in the prototype covered the topics, areas, of Location data (Figure 2), Device data (Figure 3), Browser Data (Figure 4), and System Fonts data
(Figure 5). All of which are part of the data which is accessible to the websites that users visit through their web browsers, which was explained at the top of the prototype under the topic of “About Browser Leakage” (Figure 1). To acquire these examples I tested one of my own devices, a PC, on Panopticlick [27] and BrowserLeaks [7], and used the data in the prototype. Panopticlick is a research project by the Electronic Frontier Foundation where you can test your browser against online tracking techniques, and BrowserLeaks gives an even more detailed and technical look into the data that is made accessible to websites by the web browser, covering sources such as IP Addresses and JavaScript.

For the topic of “Your Location”, the data displayed was based on information bound to the IP address. This included an IP number, country, city, language, timezone, and latitude/longitude of the IP address. The following three topics, “Your Device”, “Your Browser”, and “System Fonts”, included data accessible through JavaScript. “Your Device” included the data of the operating system, system time, CPU, display, device language, touch support, and battery. “Your Browser” included which web browser that was being used, browser version, browser plugins, and browser language. Lastly, “System Fonts” listed the fonts installed on the system.

The order of the topics, with information about the location placed first, followed by the device, web browser, and lastly system fonts, were chosen to start from a pulled back view, at one end of a hierarchy. So when the user ventured down through the prototype, with each topic it would be is at you could use the map from “Your Location” to zoom in for a more detailed view that would show the device in use, and taking it further would show the web browser belonging to said device.

The data examples used in the prototype, 17 in total, were just a small part of the data that was listed and available through Panopticlick and BrowserLeaks. The criteria I decided while choosing which data examples to include was to keep it to phrases and terms most likely to be understood by less than expert users, aimed towards the average user in other words, and avoid technical jargons [9, 24]. The ones included was data examples with common terms, such as information about the battery status, its percentage and if it was charging, or terms likely to have been encoutered by users while using their devices and web browsers, such as Operating System and Browser Plugins. Another criteria was to keep the number of examples limited as to not present an overwhelming amount of information for the test user and instead opt for page with a clean and clear overview [9, 19]. Because of this, I decided to exclude data examples such as Hash of canvas fingerprint, Hash of WebGL fingerprint, and HTTP_ACCEPT Headers, to name a few. While such data examples do play an important role in Fingerprinting tracking, they are not easily comprehensible and thus difficult for the layperson to understand.

Figure 1. Screenshot from the prototype. The top of the prototype, with a text about the topic of the information that web browsers make available to visited websites.

Figure 2. Screenshot from the prototype. The first topic that is introduced, showing data examples related to the user’s device location.

Figure 3. Screenshot from the prototype. The second topic, showing data examples related to the user’s device.
3. USER TEST

An qualitative approach was taken in the study, where a user test was conducted with 9 participants on separate occasions. The user test included an interview and a test of a high-fidelity prototype presenting Fingerprinting information, which each test lasting around 45 minutes.

3.1 Set-up

The reasoning for the qualitative approach to do interviews, instead of conducting a survey, was because they are more personal in its nature than surveys, and for the ability to ask follow up questions to answers participants gave. The user test itself was structured in three parts. First (1) the participants were interviewed on different subjects, covering topics such as: their relation to technology and the internet; and their approach and use web browsers and other softwares. This was then followed with (2) the participants being presented, and introduced, to the prototype. The prototype was described to them in which context it is thought to be used in, for this test as an integrated part of the desktop version of the Google Chrome web browser. After the user had gone through the prototype, (3) they were yet again interviewed on different subjects. This time on topics such as: how they received the prototype and the Fingerprinting information it presented; their relation to internet privacy and web tracking; their thoughts on the concept the prototype presented; and their thoughts on the prototype’s design format.

3.2 Participants

The participants were recruited from my social network of acquaintances, where I reached out to people in conjunction with the timeframe I had set for the user test. Through this, there were 9 people who responded and accepted, and were available within the timeframe, to be part of the study. These 9 participants all uses the internet and web browsers every day, for an average of 3 hours, using at least two devices per person, with a Personal Computer being the main device for six of them. The participants had varied backgrounds and knowledge, with none of whom possessing any professional expertise in IT.

3.3 Data Gathering and Analysis Method

During the user tests with every participant, their answers and comments were documented and written down next to each question. When the user tests were all over with, the answers were summarized and thematically analyzed [6], in a way to find patterns across the questions, and the answers to see what connections could be made between participants and their answers.

3.4 Limitations

To reduce the risk of something going wrong with the prototype and its introduction to the user test participants, the prototype’s functionality were limited. That is, the examples of information put on display in the prototype were all hard coded text examples written directly into the prototype’s html file. This mean that the information was static, non-changeable. For example, the information next to “System Time” or “Location” would not change depending on when and where it was used. Thus, it might have affected how they received the prototype, since the information it presented would not correlate to the actual testing situation. The benefit, though, were that every participant were presented with exactly the same information. The alternative, however, had been to implement actual JavaScript code to present the information live and correct, as well as to connect the prototype to Google Maps API. But with added functionality and code come greater risk of something not working properly for the participants during the user tests, and a severely prolonged development time of the prototype since code had to be found and/or written for every example presented.

Another possible limitation was the decision to use the design language of Google, as a way to make the prototype look like a part of the desktop version of the Google Chrome web browser, based on its market share [33]. However, if a participant was not used to the look and feel of Google Chrome, it may have affected how they received the prototype. A solution to this would have been the creation of multiple prototypes, to also cover the design language of Apple Safari and Mozilla Firefox. This was decided against, since it also would have severely prolonged the development time.

With the participants being acquaintances of mine, it may have affected their contributions. However, with the questions they answered did not cover any personal or private matters, I deem it unlikely. Although, this may also have resulted in a stronger willingness among the participants to answer the questions and do so sincerely when the interviewer was not a complete stranger in their eyes. The decision to include and use acquaintances came to be because of the circumstances of the time, where this was the most realistic group to acquire participants from that could put aside the required time for the user test.

4. RESULTS

Here follows the result of the user test that was carried out with nine participants on separate occasions. The participants themselves were also analyzed, to compare them based on if they were more or less technologically interested and knowledgeable. This was measured from their self-stated: interest in technology; knowledge about technology; and knowledge on the workings of web browsers. Through this,
4.1.2 Software Approach

Examples of documentation, from commented and everyone (9/9) said they were self taught about web browsers and the internet. “Trial and error” as one participant commented. Other sources of knowledge was school classes, internet forums, tech websites, related videos on YouTube, and from people in their surroundings. Although no one (0/9) had actively chosen to use the web browser manual or help documentation, participants in G1 had still learned something from the web browsers themselves (Q115 in Table 2). The examples given were a functionality demo, the description text for Private mode, and two who mentioned the text in web browser settings that describe how certain settings and functions work.

4.1.3 Internet Privacy and Web Tracking

On the topic of Internet Privacy and Security, 2/5 from G1 stated they were more knowledgeable regarding this than the average user, saying “most probably don’t know anything on the subject”, and “most people I know would not know about IP or DNS”. Comments from other participants were also on how they can feel the presence of something that watches over them, “like Big Brother” as one participant mentioned, and how they are targeted with ads. Further, three participants mentioned that privacy is not guaranteed and it is difficult for it to be with their assumption that a lot of service providers, Google and Facebook were mentioned as examples, already knew a lot or everything about them, and that “you can’t really protect your information” and that “this race is lost”.

Precautions participants had taken for their privacy included one from G2 who used a VPN as well as having restricted application access to the device location. From G1, one had started using the Apple Safari web browser instead of Google Chrome as well as not always being logged into Google while browsing, and sometimes used the Private mode on websites the participant knew had cookies for targeted ads. This participant and two others from G1 also mentioned the use of ad blocking browser extensions. However, on a question about browser extensions (Q135 in Table 4), another three also mentioned the use of ad blockers. Precautions G1 participants had thought of taking was two who said VPN, one of whom also mentioned a browser extension to turn off JavaScript, s/he added however “but then some fun functionality might stop working”. Of those who had not thought about taking any such precautions, from G2 one participant thought that “companies will get the information anyway”, and another one that the subject felt too big and unfathomable, and felt that it is difficult to know what you can or should do.
One of the participants (2/9) who did not know what a Browser Cookie was (Q137 in Table 5) had heard the term though, and added the example of when websites ask the visitors to accept browser cookies with the claim “for a better user experience”.

### 4.2 Prototype Experience

#### 4.2.1 Prototype Reception

<table>
<thead>
<tr>
<th>ID</th>
<th>Question</th>
<th>G1</th>
<th>G2</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q211</td>
<td>Have the prototype helped them to understand Fingerprinting</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Q213</td>
<td>If the prototype affected their attitude towards Internet Privacy</td>
<td>Yes</td>
<td>20%</td>
<td>80%</td>
</tr>
<tr>
<td>Q214</td>
<td>If the prototype made them think about acquiring privacy enhancing software</td>
<td>Yes</td>
<td>20%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Table 6. Questions regarding the prototype’s reception.

Upon having been introduced to and used the prototype, everyone (9/9) stated that the prototype had helped them to understand Fingerprinting. Among the participants in G1, one participant who had not heard the term Fingerprinting before said that s/he “pretty much” knew about this concept of web tracking already. Among those in G2, one mentioned confusion over how the leakage of information work in relation to the web browser, if it is its developers who made this information available. No one (0/9), however, said the prototype had helped them to understand more about how web browsers work. Everyone (9/9) also said that the prototype had introduced or taught them something new. Things mentioned in particular were the access to information about the language in use, battery status for relevant devices, and the installed system fonts and web browser extensions. Some were surprised over the amount of information in general that were made available. That multiple pieces of information could be pieced together was also mentioned, and that its uniqueness mattered. Lastly, one G2 participant mentioned that the difference between Fingerprinting and Browser Cookies was news to her/him.

About the impact the prototype made and if it had affected their attitude towards internet privacy (Q213 in Table 6), one of those from G1 who said no also stated that “things work as I already thought”, and another that although the attitude had “not really changed” s/he would pay more attention to this in the future. Among the ones affected in G2, one said s/he had not realized that all this information could be used, and did not think of the information as important before, and another one did not know the extent the web tracking, and had not thought that so much information is made available for others. The participant from G1 (1/5) who was affected said the prototype had made her/him think about think about acquiring a privacy enhancing software (Q214 in Table 6), and mentioned wanting to stop the real IP address from showing and revealing the location. Another participant from G1 added that s/he did not feel the leaked information was important enough to warrant an adoption of such a privacy software. Lastly, two from G2 said that they lacked knowledge on how to acquire such software, although on of whom “realize it’s a problem” with this kind of web tracking.

#### 4.2.2 Format

<table>
<thead>
<tr>
<th>ID</th>
<th>Question</th>
<th>G1</th>
<th>G2</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q221</td>
<td>Thought the prototype’s design format was good</td>
<td>80%</td>
<td>100%</td>
<td>89%</td>
</tr>
<tr>
<td>Q223</td>
<td>Their attitude towards the level of the prototype’s technical information</td>
<td>Good level</td>
<td>100%</td>
<td>0%</td>
</tr>
<tr>
<td>Q224</td>
<td>If they thought they would understand more technically detailed information</td>
<td>Yes</td>
<td>20%</td>
<td>0%</td>
</tr>
<tr>
<td>Q225</td>
<td>If they found the prototype easy to use</td>
<td>Yes</td>
<td>20%</td>
<td>0%</td>
</tr>
<tr>
<td>Q226</td>
<td>If they found the prototype complex</td>
<td>Yes</td>
<td>20%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Table 7. Questions regarding the prototype’s format.

The prototype’s design format in regards to educating in general and informing about the subject of Fingerprinting in particular was praised by the participants and deemed a good format (Q221 in Table 7). Two participants thought that it also could be used for any subject with concrete examples, with one saying it “Feels like a good ‘About page about any topic’ with its “uncomplicated and clean” appearance. Another suggested it could be used to teach young students, or people new to computers, about computers and the internet.

Aspects highlighted from the prototype were its simplicity with a clear and simple design and a small amount of text, the structure and grouping of the topics, and the variety of easy-to-understand examples, among others. In general, the preference was to keep things short, simple and easy, and with as little amount of text as possible, especially among the participants in G2. Such areas were also brought up by the participants when they mentioned things they thought could improve upon the format. Among their examples was make it more simple and basic, but to also include more examples, and make the prototype more easily understood. There was also mentions of less text, especially for the prototype’s introduction text, which one (G2) also thought “because people usually don’t have the patience for it”. In relation to this, 2/5 from G1 and 3/4 from G2 thought that images and/or illustrations could help the prototype in general and the introduction text in particular to “turther explain Fingerprinting.” A participant (G1) had the example of an illustration that could show what makes a user unique and stand out, “With this unique IP, this unique Language, and this unique combination of System Fonts it equals You”. Another (G2) added that images and making things more colorful could “make it more interesting”. Other things was 3/9 who thought that the inclusion of an informing video could be a good addition to the format.

Regarding the technical details of the information presented in the prototype, it was generally seen to be on a good level (Q223 in Table 7). One (G1) participant though thought that it would have been easier to understand the connections between the data examples had they been more detailed and in depth and...
4.2.3 The Concept

ID | Question | G1 | G2 | All
---|----------|----|----|----
Q231 | What they thought of the concept of having integrated educational pages, like the prototype, built into web browsers | Good idea | Not interested | 100% | 75% | 89% |
Q232 | If they would have used it themselves and/or recommended others | Use | Recommend | Neither | 80% | 50% | 67% |

Table 8. Questions regarding the prototype’s concept.

The participants thought it was a good idea with the concept of having integrated educational pages like the prototype built into web browsers, as a way to inform users about web browsers and the internet, on topics such as Fingerprinting (Q231 in Table 8). From G1, one participant thought it would have helped because it is “not that much knowledge about this out in our society”, and another adding s/he was given a clear understanding of Fingerprinting and on what is used to track a person online through the prototype. From G2, a participant who although liked the idea, said that it had to be easily comprehensible and easy to understand all the terms and phrases presented, if it had been real, and one who said s/he was not interested in how things work, but gets crazy when it does not work. That s/he would probably think “Oh, so it worked like this” but then not use it again. The concept would only be good “if it was very easy to understand and very basic”.

They were also asked if, had the prototype’s concept been real, they would have used it themselves, or recommended it to others (Q232 in Table 8). A participant responded that s/he “Like the concept. Would definitely have checked it out and tested it.”, and that depending on the information s/he would also have made privacy enhancing changes to her/his own device. Related to this, another (G2) would have also wanted more information on how one can protect one’s Fingerprinting information. In regards to recommending it to others, one (G1) especially mentioned the elderly generation as s/he thought would benefit from it, and another (G2) mentioned its inclusion in school education, because of the thought that everyone have devices but few really understand how things work. One (G2) of those not interested in neither using nor recommending it (2/9), stated to prefer to search through an external search engine if there was a specific subject s/he wanted to know more about, and that s/he is “not that interested in reading about [her-himself]”.

Two participants also expressed their concern for the implementation of the concept, that if it is accessed through the menu or settings system of a web browser, it could end up being “put far away, deep in the [menus/settings] as one (G1) put it, and that “Power users usually check settings and menus, but not the average user.” The other (G2) said “Everything is already put into menus and settings, but it is very difficult to find things there.”, and added “maybe that the user should be reminded about [the concept] somehow.” These two participants also expressed a wish of having this information available to them when they were browse around the internet as normal, to for example see what information a website saw from them. Another implementation suggestion from a participant (G2) was for it to be “a complement to a walkthrough when you install [the browser] and open it the first time”, or “part of an intro video to the web browser”, where if the browsers for example had differently themed videos “this one could be part of one on the theme of user privacy.”

If there was something about the internet and/or web browsers they wish they knew more about, 6/9 could not think of anything, with two of them adding that they just wanted thing to work. Of the other 3/9, they all said they wanted to know more about how Fingerprinting and web tracking works, in general and in relation to how it is used to target ads. One also added VPN to the list of things s/he wanted to know more about.

5. DISCUSSION

This section will, based on the results from the user test, go through the reception of the prototype, aspects which users valued, and implicating factors to consider for future implementation.

5.1 Informing on Fingerprinting with the Prototype

The results suggest that the created and tested prototype was successful in the task of presenting and informing users on the tracking technique of Fingerprinting. Regardless of previous awareness or technological interest and knowledge, every user test participant did feel that the prototype had helped them to understand Fingerprinting and learnt something new from it. A lack of previous knowledge on Fingerprinting was also shown, where a few had only heard the term.

However, in regards to how impactful the prototype was on users attitudes towards internet privacy, users with a higher technological interest and knowledge were less likely to be affected. This may be because of their better understanding of the limitation web browsers possess and awareness of the extent at which web tracking work and operate. None of those who felt affected though had come to think of acquiring any privacy related software, coming from this experience, nor was any intent expressed before they experienced the prototype. This goes in hand with previous work about the gap between concern and action [36], and the correlation between technical skills and the adoption of such privacy enhancing technologies [32].

A part of the prototypes success in how it was able to help users understand Fingerprinting lies in, and is credited to, its format. Aspects of visual aesthetics [21, 23], on which the format was built upon, of worth was among others the perceived simplicity [19] rather than complexity. They put value on keeping things short and simple, and importantly as easy to understand as possible. In relation to the simplicity was also its structure, in how the different topics were grouped and divided, as was the diversity of examples.

The less technologically interested and knowledgeable were more inclined though to wanting to simplify the content even more. Areas of such improvements was the text. They wanted further, better, explanations of the workings of Fingerprinting, but in other mediums rather than text, in part to replace the text already in place. In research by Nielsen [26] it showed that of the tested users “only 16 percent read word-by-word” on a “new page they came across”, and as a result he opted for scannable text. This lies in line with my test participants preferences, one of which who also at first had misunderstood the meaning of Fingerprinting after having read the text in a
scanning fashion instead of word-by-word. As a complement to the text, or replacement of, was the request of more images and illustrations, or even video, to assist with the explanation of the content and to make it more interesting, which further highlight Nielsen's findings [26]. This could also be the result of the times we live in, were people are always connected to the internet and spend hours browsing every day, as the participants in this user test also reported. A study showed that the patience for waiting on a video to start up was 2 seconds after which people started abandon it at an increasing rate for every second past [20]. The lack of patience was also mentioned by one of the participants when talking about the prototype's introduction text. In a study on “millenials [...] hyperconnected lives”, the authors summarized it as “Negative effects include a need for instant gratification, loss of patience” [5]. This could be interpreted as, beside to help with the explanations, a mean through which images and/or video would provide the participants with a quicker way to process the information, in a more passive and less processing demanding fashion. Still, as long as it had further helped users it would have been a recipe for success. The difficulties though, to accomplish such a thing as to better people's understanding of a subject, is shown in a study on Private Browsing [11], that 75.8% of the function's users “incorrectly identify the protection” and 66.5% “overestimate its benefits”, despite that the Private Mode explain its function and limitations at every startup.

The desire to simplify to further the ease of use connects to findings from Castañeda et al. [8], in how a “perceived ease of use” played a big role in the decision to revisit a website among those with less experience from the website in question, in contrast to “perceived usefulness” for those with more experience. The less familiar you are with something, the more value is put on how easy it is. This usefulness also expressed itself in my test, where the more technologically interested and knowledgeable were more inclined to want the prototype to offer even more information, or to be directed to more information, as well as an implied expression to use it as a tool.

5.2 Concept Implementation Implications

The concept of web browsers having integrated pages meant to inform users on browser and internet related topics such as Fingerprinting, as was the case with the prototype, was met with positive reactions. Had it been real, most would also have liked to use it themselves and to have recommended it to others. A problem, however, would be the implementation. There is a famous quote by Steve Jobs that highlight this problem, that “People don't know what they want until you show it to them.” [17] It rings true even for this study. If people knew about internet privacy, for most it was still just a feeling of the presence of something that watches and tracks, where there both was an expressed hopelessness over the situation in regards to the information big internet companies already, or lack of awareness over how they could better their privacy. Even on the nose in regards to the quote, that no participant could think of some other internet or browser related subject they wished they knew more about. Still, upon being introduced to the prototype, and to Fingerprinting, they found it helpful and useful. But to introduce prototypes during user tests is comparatively easy. Just as easy would it be to realize the concept and throw a link to the page into the web browser menu somewhere. The real challenge would be to actually show it to people, if it had been real. To make them aware [9] of, and to get them to use, it.

Where most browser content and functionality end up and reached from are in the menus and settings. An example of one such thing is their manuals or help documentations. But, even though their function is to provide users with browser related help and information it is something often overlooked [16], with no participant in this study having ever used them. Less technologically interested and knowledgeable participants were also less prone to even using the menus and settings [32] for their web browsers and in other software, with some who had never done so in their browsers. The opposite was true for more technologically interested and knowledgeable users, who also showed more curiosity towards new software in general, with some at times also checking the patch notes. Although no one of this group had gone for the manual or help documentation, all but one reported to have used external search engines to search for help and information about to their web browsers. This would likely lead to that mostly the already technologically interested, knowledgeable and aware would even discover [9] this integrated page and have the ability to test and use it, while the less technologically interested and knowledgeable had a better chance of finding it by the recommendation of others than through their own discovery. A question one then could ask is if and how the web browsers themselves could take an active and visible role at this part of an implementation.

The concern, regarding if it had already been implemented as an actual integrated page, was also expressed by participants, with a suggestion being that users would have to be reminded by their browsers. One such proposed solution was to include it in a walkthrough for the browser. But even there it was shown that less technologically interested and knowledgeable users did not use walkthroughs, and rather opted to go straight to using the software without any exploration. An alternative functionality solution, that also came as requests from participants, could be in the form of an active user interface elements, that could inform the user in real time while s/he was using the web browser as normal, similar to Ackerman’s and Cranor’s Privacy Critics [2]. In today’s web browsers, this functionality can express itself through browser extensions, where they can be interacted with or used to notify users with pop-up bubbles. A study, in relation to this, showed that most of its participants did not notice the alert bubbles from the two evaluated browser extensions, and “Those that did, found them either useful or particularly annoying.” [31] Combined with the report of “warning fatigue” from security warnings [3], this show the difficult balancing act such a solution would have to be able to execute, in terms of whether the limit goes between being too active and visible in front of the users or too passive and concealed to even be noticed.

5.3 Future Work

Even though a realization and implementation of the concept would have obstacles to overcome, it is something that would be interesting to test in a live setting with a functionally working prototype, how it could affect the reception. Both as it was presented in this study, but with the added improvements mentioned in part 5.1 of the discussion, and also in the form of a browser extension in an active and visible role. For the latter format, a longer test period could see if Fingerprinting awareness affected users behavior over time. Such a study could also see if novelty played a part in affecting users momentary and episodic experience [29], since the workings of Fingerprinting was new to almost all participants of this study.

It would also be interesting to see how the subject chosen affects the reception and how users learn, and if another topic than Fingerprinting would be as effective in informing. Privacy, and internet privacy, is in itself a very personal matter. And as with the prototype, the presentation or reporting of web tracking
and Fingerprinting is not as much about how Someone can be tracked but rather how You are tracked. This is in the prototype present in the data examples it includes, like a user’s location pinpointed on a map, or their device’s battery status. The information and examples become more concrete, something closer and personal, which is probably easier to relate to and feel that it matters to me, than if the subject and its examples had been more abstract and impersonal.

It should be noted that the web browsers Apple Safari and Mozilla Firefox have taken action in regards to web tracking and Fingerprinting as of late during the work on this paper. Both took steps to protect their users, and making Fingerprinting a bit less effective, by enabling Fingerprinting protection by default. Mozilla described their effort as having “compiled lists of domains that serve fingerprinting [...] scripts” which the browser then will block [25]. Google Chrome, that remains the global market leader [33], have however not announced any such plans. This could make it interesting if, with a fully functioning prototype and a larger amount of participants, it would have showed any differences among user groups with different web browsers.

6. CONCLUSION

This study have investigated (1) what key aspects of visual aesthetics affected users when being informed about the web tracking technique Fingerprinting, and (2) to what extent differences in technological interest and knowledge affected users reception of Fingerprinting information, and what implementation implications it leads to. To accomplish this, a high fidelity prototype meant to present Fingerprinting information was created and used as part of an user test. The result of which showed that those less technologically interested and knowledgeable experienced more of an impact from the prototype’s information, where their attitudes towards Internet Privacy to a higher degree were affected. Further, it also showed a way for how web browsers can inform its users on topics such as Fingerprinting, and the aspects users valued from it. Additionally it gave insights on how technological interest and knowledge affects users approach and interactions with software, and the implications this brings that could be taken in consideration by designers and developers for future browser related functionality implementations.

REFERENCES


