University of Windsor

COMP8677-3-R-2022S Networking and Data Security

Project Report:
How Can and Would People Protect From Online Tracking?

Guided by:

Dr. Shaoquan Jiang

Submitted by:

Bhavya Bhimani - 110066194
Deep Shah - 110072582
Madhavkumar Sheladiya - 110071277
Nupur Badiani – 110069785
Rutvik Lathiya - 110071704

Abstract

Users find it difficult to defend themselves from online tracking because it is complicated. According to researchers, choosing to reject previously accepted privacy settings makes it much harder to opt-out of privacy settings than it is to choose to accept new ones. Although systems and users for monitoring activities have been thoroughly examined by the academic community, it is unclear how data protection laws, how websites provide privacy-enhancing technologies (PETs), and how users become aware of and utilize PETs relate to one another. This research uses a multifaceted strategy to identify such a relationship. During the evaluation of the top 100 EU websites, it was discovered that information regarding PETs is presented in a way that goes well beyond the cookie notice. Many users discover PETs for tracking protection either on their own or with the assistance of family and friends. Additionally, an online survey with 614 participants from the UK, France, and Germany to get a more comprehensive insight of consumers' tracking protection habits was conducted and it was discovered that there is a disconnect between what websites advertise as tracking protection and how users report to do so. This difference makes it clear why present procedures and rules are unsuccessful at encouraging users to use PETs.

Introduction

Having a lot of data on a website result in targeted advertising, digital discrimination, and privacy fuzziness. Online behavioral advertising refers to the process through which ad networks profile a person based on their online behaviors and then utilize that profile to portray that user as more likely to be interested in specific advertisements. A web page's content may come from a first- or third-party when people access it. While there are other methods for tracking user activity, the most basic one involves an advertiser placing a cookie with a special identifier on the user's computer.

Most EU websites display cookie consent notices, which are supposed to inform visitors of the site's cookie use and tracking policies. Regarding cookie notice's ability to prevent tracking, there is some skepticism. Consent management solutions frequently use implied consent and dark patterns. The GDPR minimum criteria are only met by 11.8% of the top 10,000 websites in the UK.

By refusing the cookie notification, employing browser blocking extensions, or by using other tracking protection and privacy-enhancing technologies, users can protect themselves from tracking in several ways.

It has been suggested that peer-to-peer tracking methods and mechanisms have usability problems. It has been established that cookie notifications and PETs in general do not provide fair practices. In websites' cookie notices, such as those pertaining to location, many suspicious trends have been identified. Beyond the cookie notice, there is little study on alternative privacy-enhancing information options, and those that are available, to our knowledge, mostly target US customers.

Scope of the paper

Despite prior studies have looked at systems and users for monitoring activities, it is evident that there is no obvious connection between data protection laws, website practices for presenting PETs in the real world, and how users learn about and utilize PETs. Consequently, the purpose of this research is to examine the connections between these three factors.

The paper is divided into three main parts. The first one is background study, followed by case study1 and then at last case study2. What are the legal criteria for tracking protection? How are PETs for tracking protection communicated to users on websites, and how useful are these methods? What types of PETs do users employ and how do they learn about PETs for tracking protection? These are the main questions answered in first part of the paper.

Study 1 conducts a thorough investigation of cookie notices, user options outside of the cookie notice, and the challenges associated with opting-out. To locate all the PETs and gauge their popularity, the privacy-related content of 100 top EU websites was examined. Results showed that opting-in via cookie consent is considerably easier than opting-out. Many websites rely on users' browser settings to block tracking since they do not present a fair cookie notification. According to our understanding, these findings represent non-compliant practices that have never been researched.

The purpose of Study 2 was to better understand how Internet users discover PETs for tracking protection and the methods they employ to do so. PETs for tracking protection were the subject of a survey that included 614 Internet users from the UK, Germany, and France. This study provides information on user awareness and tracking protection strategies. Additionally, the effectiveness of cross-national and gender differences is discussed.

Background

The following components made up the background investigation:

1. Online Tracking

Online service providers have steadily developed a variety of methods for gathering user data for targeted advertising. Every device that is a part of a network can leak data about its environment and users. Online tracking techniques have advanced to a new level with the rise of linked smart devices (such as smartphones, tablets, and the Internet of Things).

When a website is visited, little amounts of text-based data called cookies are downloaded on device. Browsers transmit cookies to the client's machine. There are two groups made up of them: cookies from both first- and third-parties. The website the user is visiting sets first-party cookies, and only that website can view them (due to the restrictions set by SOP mechanism). Various websites may use their own cookies to set content on some web pages. A page (like Facebook) that you share a link to may leave a cookie on your browser. Third-party cookies are not under the website's control. A website can identify a user's browser by fingerprinting it in addition to using cookies, thanks to data gathered by JavaScript. Web beacons, clear GIFs, page tags, and web bugs are examples of other tracking technologies. Users generally have some control over how to stop online tracking.

2. Regulations

General Data Protection Regulation (GDPR), which was adopted by the European Union (EU), becomes effective in 2018. Online service providers are required to inform users about cookies, explain what they perform, and obtain their consent. In-depth guidance on legal compliance is provided by the Information Commissioner's Office (ICO).

Online service providers must inform users about cookies (or any other comparable tracking technology) they are using, explain what they do and why, and obtain consent before using cookies to comply with the GDPR's data protection principles, rights, and obligations. Because of this, it is necessary according to the legislation to give the user a simple, fair, and independent way to stop monitoring or alter their preferences at any moment.

Related Work

It comprises of 2 main points which are discussed as below:

1. **Human Aspects**

In user studies, blocking and transparency are the tactics that have been most thoroughly studied. The positioning and options of cookie notices, for example, have a significant impact on how well users interact with them. Only about 10% of websites adhere to the GDPR's strict minimum standards. Popular cookie designs do not provide users many options for control. The effectiveness of browser extensions varies, and they can be divided into ad blocking extensions and tracker blocking extensions. Ads and trackers may still be blocked ineffectively by default settings, necessitating further adjustment. Despite the fact that certain extensions' readability has improved, jargon was sometimes found to be used in their descriptions.

2. **Gap in the research**

Studies done in the past have looked at the human aspects of PETs, including tracking activities and tracking on smartphones and other smart devices. The difficulty of choosing not to use previously established privacy settings has not received much attention. Closing some of the gaps between vendors and end users would be made easier by having knowledge of the statistics on PETs being offered by websites in the real world.

It may be possible to evaluate the approaches to tracking protection via PETs by understanding how users acquire knowledge of tracking protection techniques. Previous studies have examined the general sources of information in the security and privacy context. Through user research in Study 2, we examine both elements in this study.

Study 1: System Studies of Tracking Protection Models

Aim

User studies have been conducted to examine the usability of cookie notices and other types of PETs (such as data deletion) in. If a person changes their mind and decides to reject privacy settings, we don't know what the challenges are with opting out. To the best of our knowledge, no one has investigated the many kinds of PETs that websites provide their visitors. To contribute to the awareness of such modifications, it was also examined that the cookie notices of well-known websites.

The GDPR framework was the focus, which mandates that service providers disclose information about tracking technology (cookies) in a way that users will notice it on their first visit to a website. They do not include cookie notices in terms and conditions or privacy notices, nor do they emphasize acceptance over rejection. Cookies that don't need the user's explicit agreement can be modified at any time with the same ease that they were allowed to use them, and such cookie rules avoid depending on the user's browser settings (or other processes) to set preferences.

Under RQ1 and RQ2, top EU websites were visited and examined for their privacy consent, opt-out options, and other PETs. RQ1: What effects would opting out of the privacy consent have, as well as if the user later changes their mind? and RQ2: What other PETs are available to users to enhance their privacy on these websites, in addition to a variety of user control options?

Process Followed

To find the best websites in the EU, the region 'Europe' on Alexa was selected to carry out the study. The construction of a data collection with 100 webpages excluded redundant and non-English websites. The functions and services offered by these websites vary, ranging from news and search engines to gaming, social media, and commerce.

The procedural website was examined, with a focus on the listed points

I. Whether a cookie notice is present or absent? Where is the notice's location?
II. How many clicks are required to refuse (opt-out)? How many clicks do you need to make to withdraw your permission to cookies
III. Aside from the cookie consent, what additional PETs are there on the website's privacy-related pages?

Each website was launched to make these observations, and each one was made to attempt to disable cookies and keep track of the number of clicks. The browsing history was then deleted, and on the subsequent visit, we agreed to the cookies. This time, the browser's cookie settings were left in place. The experiment was conducted using the privacy-focused browsers Brave, Firefox Private, and Google Chrome Incognito to ensure that erasing the browsing history was sufficient for our purposes.

The needed number of clicks for each objective was counted to assess the difficulties associated with opting-out. After viewing the first several websites for the evaluation, certain patterns were more obvious and were learned, which minimized errors. Various investigations have used more sophisticated measurement techniques (e.g., all user action such as scrolling, reading, clicking).

The browsing history was then once more cleared, and each website was opened, and the relevant privacy links were followed. This complex manual technique is error prone. By using keywords to search the privacy-related pages, every item was double checked. The Appendix contains a more thorough template that was used for our website analysis.

Limitations

Additional elements like the time spent, other user actions (such scrolling, filling text, etc.), the difficulty of discovering the opt-out pathways, and so forth, were not taken into account. Many privacy settings are often accessible through the small-font links at the bottom of a webpage that are dedicated to privacy. Opting-out is far more difficult than using the default settings, even under a simplified test scenario. It was acknowledged that by streamlining studies, more data about usability metrics like text size, colors, etc. was lost. Dark patterns can be seen, nevertheless, and our method doesn't refute our findings.

Since the study was examining these websites from the perspective of their users, it was carried out manually. Large-scale research are not suitable for this method. The experiments only looked at the differences between PC browsers and other platforms, like mobile browsers and mobile apps. Previous studies have demonstrated that privacy policies do vary amongst platforms. This remains as future work to study the same difficulties in accordance with other data protection rules such as the CCPA, even though there may be some applicability to other legal frameworks.

Results

The study's findings were divided into three key categories: cookie notice, opting out, and available PETs.

1. Cookie Notice

The user was only given a cookie notification on 15 websites without any other control options. 22 websites only offered the option of accepting their cookie notification (agree, ok, yes, I understand, etc.). The Accept option was highlighted over other options on 44 websites, which also included other options (further information, settings, tailor my selections, etc.). There were only 14 websites that displayed cookie notices with more than just the Accept choice, and only Accept was underlined. Only three of them were permitted to reject as easily as accept, though. Except for the last group, all other actions are illegal and fall short of the GDPR's minimal standards. This rate falls within the same range as that discovered in earlier research.

The formats (in-page vs. overlay), sizes, colors, and typefaces used to show cookie notices varied. These websites displayed their cookie notices in a variety of locations: 15 websites displayed the notice at the top of the page, 48 websites displayed it in the lower portion of the page, and 31 websites displayed it in the center of the page. In the middle of the page, cookie alerts were displayed on about one-third of our websites. Although it hasn't been used, this approach might greatly engage users.

2. Opting Out

Of the 100 websites, 5 had no cookie notice at all, 34 did not permit opting out through the cookie notice (as indicated by not possible in the left plot), and 46 did not offer an opt-out option in case a user changed their mind. In order to reject the cookie notification on the remaining websites, the user would often need to make 3 clicks. Even when only two or three clicks were required to opt-out, we saw that users still had to deal with additional difficulties. They must, for instance, scroll down to discover the refuse option or visit a different website to obtain the desired privacy settings. These findings demonstrate that opting-out (under any conditions) is more difficult than opting-in, which often only necessitates one click from the consumer.

Most websites required users to click on the privacy links at the bottom of the page in order to try to opt-out of previously agreed privacy settings. After clicking the privacy link, the cookie notice might occasionally appear in some situations. Only in three of these instances did a privacy icon appear at the bottom of the page as an overlay design that was always visible to the user while on the website (and it was still modest). The same shadowy patterns of the cookie notices, such as emphasizing Accept over Reject, were also present in other parts of numerous websites, which we also discovered.

3. Available PETs

It is crucial to look into any additional privacy-enhancing features offered by internet providers. The majority of websites offer two distinct pages, including one for privacy and another for cookies. The study demonstrates these PETs and their appeal to the websites it surveyed.

Nearly every website had information on how to get in touch with them via some sort of electronic communication, such as email addresses, online forms, or links specific to privacy concerns. For privacy, some companies provided other communication channels including SMS and an opt-out option for receiving advertisements on their website.

Most of these websites advised users to change their browser settings, including turning on Do Not Track (DNT), manually removing cookies, and offering links to instructions on how to do so in specific browsers such Internet Explorer, Firefox, Chrome, and Safari on PCs and mobile devices, in order to prevent tracking. It should be noted that relying on the user to change their browser's settings to prevent tracking is illegal under the GDPR. Many websites directed visitors to related projects including the European Interactive Digital Advertising Alliance (EDAA), Network Advertising Initiative (NAI, network advertising. org), Allaboutcookies.org, privacyshield.org, and cookielaw.org in order to protect their privacy.

More than half of websites allowed users to opt out while also providing information and links regarding their partners. This contained details on the user's privacy settings as well as information about and/or links to major corporations like Google (and YouTube), Facebook (and Instagram), and Twitter. Unless there is a feature like "Reject all," this usually involves a lengthy list of third parties and is not a useful solution.

The Information Commissioner's Office (ico.org.uk) has information on where users can go to learn more about internet privacy. This also necessitates the user leaving the page and going to another site in order to improve their privacy, similar to the categories mentioned above. Websites advising users to modify privacy choices through user accounts and website privacy dashboard settings make up one-third of all websites. While some just suggested this as a possibility, others supplied links. To safeguard their privacy, some websites recommended consumers to quit using their services by deactivating or deleting their user accounts.

One-fourth of websites offered information about and links to privacy-enhancing add-ons. Most of this link directed to the Google Analytics Opt-out Add-on. During an examination by the BBC News website, Ghostery was cited on one website. The privacy settings on mobile devices can be changed to better protect privacy, according to certain websites that gave information and links regarding this subject. By choosing "Privacy" and "Advertising" in the Settings on your Apple iPhone or iPad, for instance, you can choose not to receive interest-based advertising.

To find options, users must browse through a number of text-heavy privacy-related pages. There are some broken links, and it's debatable whether the content is readable by non-expert users. This study also investigates the top 100 EU websites. These well-known websites are probably well-equipped and may even have more resources to concentrate on law-complaint practices. Websites that may be less well-known and have fewer financial and human resources would use less suitable techniques, resulting in worse tracking activities and fewer alternatives for user control.

Study 2: User Inquiry of Tracking Protection Models

Aim

The use and deployment of personal electronic devices (PETs) for tracking protection is influenced by a number of additional factors, such as awareness of PETs and knowledge of their potential benefits. With little discussion of other issues, prior study mostly focused on the usefulness of notification, choice, and browser extensions. Therefore, in Study 2, following factors are considered to better understand how specific PETs are used for tracking protection.

I. How people learn about tracking protection via PETs, and
II. An online poll asking about the PETs they use

RQ1's "How do people learn about PETs for tracking protection?" and "What PETs do people employ for TPT protection?" questions examined PET awareness. The main emphasis was on third-party tracking, which was emphasized as being a more intrusive tracking technique than first-party tracking.

Method

N = 614 people participated in an online poll. In the UK, Germany, and France, we sampled N = 202, N = 202, and N = 203, respectively. Participants received compensation at a rate of £7.5 per hour even though the study only took 20 minutes. These three nations were picked because they have the most internet users in Europe, which means more people could be vulnerable to online surveillance.

The study was balanced by the number of participants in each country and gender, as well as their use of personal electronic devices (PETs). The survey was written in English and includes a section on demographics, a comment on privacy technology, and information on how individuals learn about PETs. On the Prolific platform, the survey was piloted in three different nations, and the participants were asked to remark on it. The use of positron emission tomography (PET) to examine people with learning difficulties was the major goal of this investigation. In order to prevent tracking, people were asked to write on how they understood third-party tracking (TPT). Privacy technology, tools, or features may be one way to do this. The participants were given the option of indicating how they discovered privacy technology, tools, and features that can aid in preventing such online tracking.

The participants were presented with a selection of 57 options to gauge how often PETs were used. These choices came from three different places, including extensions and browsers that prioritize privacy. It was mentioned that not all of the components in, or the 26 generic PETs, may protect from tracking. However, some technologies may be used by participants under the presumption that they offer useful tracking protection. Participants selected from a similar sample pool likewise called these PETs. The participants in this study might withdraw at any time and participation was entirely voluntary and anonymous. The study's details, including the fact that participation was optional and anonymous, were provided on the first page of the survey.

Limitations

Although self-reports were the primary method used in this study, they are frequently used to elicit user responses in user studies on privacy and security. Because only UK participants could access that function at the time the study was being conducted, we did not select a sample from Prolific's sample pool. In all three nations, there was no discernible age difference between men and women. The study was restricted to exploring how PETs are used and how people become aware of them. A representative sample or a different sample population may be the goals of future investigations.

The survey was conducted in the UK, Germany, and France and was written in English. Although laypeople might not be familiar with every item on the list, we anticipated them to mention the ones they use. It is possible to conduct more research on the pathways to awareness and how awareness affects PETs. A solid command of English may be associated with greater experience in IT and security, which was not assess or elicit, despite the fact that the survey was piloted in the relevant countries to encourage participant comments (on structure and comprehension).

Results

The study's conclusions were broken down into two primary categories: knowledge about PETs and use of PETs.

1. Awareness of PETs

Given the disparities in gender and nationality, RQ1 asks "Are people aware of PETs and how do they learn about PETs for tracking protection?" It was found that participants commonly included PETs in their responses to the "other" choice under the "friend/social interaction" category. The "Don't know" theme relates to participants who are not aware of PETs for tracking protection. Other replies pointed to individuals' own research to look for PETs via internet searches or finding information on webpages (as set in the questionnaire). A few people mentioned how they discovered PETs using browser options or technological details like P336.

In all three nations, a higher proportion of women than males claimed to be ignorant of PETs. The most common method used by males in all nations to learn about PETs was doing one's own study. The next step was learning with the help of friends and family, which is also how women prefer to learn. Three binary logistic regressions were used to assess the statistical effects of gender and national differences on learning about PETs. As numerous comparison corrections would be required for more (X2) tests, regression models were employed instead of X2 tests.

Those from Germany and France were twice as likely as participants from the UK to do their own study. The model's precision is 78%. The model with "friend/family" as the target variable is not significant, but the model with "don't know" as the target variable and country and gender as predictors is significant with 2(3) = 70.135, p .001, and R2 is between 11% (Cox & Snell) and 15% (Nagelkerke). Women are about 2.7 times more likely than men to not be aware of or remember PETs, and both German and French participants are about 66% less likely than The accuracy of the model is 64%.

2. Use of PETs

How do people employ PETs to guard against TPT? is RQ2, which were studied. calculated how often each of the 57 PETs is mentioned. The 45 most popular PETs are included along with the PETs utilized by at least 10 participants. Adblock, AdblockPlus, and UBlock are a few of the most widely used browser addons for tracking protection. The prevalence of browser extensions is consistent with earlier studies; extensions are widely utilized and frequently employed for user experience (UX) rather than privacy.

Eight categories were created using PETs, which show how popular each category is. The categories describe the kind of tracking protection and the layout of the PET, such as whether they are privacy tools, browser extensions, built-in settings, or blocking software. The two most popular PETs categories for tracking protection were discovered to be extensions and manual opt-out, with the "others" category coming in third. This group includes technologies that are obviously ineffective for tracking, such Paypal.

Ads and trackers may still be displayed in some browser addons. A severe hazard is posed by malicious extension behavior in browser extensions. Some browser extensions acquired from the official repositories are prone to harmful behavior despite passing through thorough vetting processes. For their own tracking purposes, certain tracker-blocking extensions might use backdoors. When the browser is closed, this setting causes cookies and browsing history to be automatically erased. However, if a determined attacker looks into side-channel data like deletion traces, private browsing would reveal user information.

Using a VPN, the user's identity (i.e., IP address) is concealed from the website server using a private server to which the user is already connected, which is very useful for blocking applications. This configuration's main concern is a lack of confidence between the user and the private server. The private server can nevertheless monitor user activity and browsing habits. This tracking information may be saved on a private server, sold to third parties, or taken over by hostile actors. The user and the private server must therefore have at least a minimal level of confidence.

The features that come with most browsers allow you to stop user tracking without installing any additional software or plugins from third parties. The browser's request for a webpage triggers the beginning of the track blockage. For instance, the browser does not at all send a request to load a tracking JavaScript script. Users will gain from faster webpage loading, bandwidth savings, and tracker blocking as a result of this. A track blocker feature is integrated into mainstream browsers. The disadvantages of these technologies have not yet been thoroughly studied. Additionally, it is against the law to use browser settings as the primary means of blocking tracking. The usefulness of alternative strategies, particularly those offered on websites through different projects, hasn't been thoroughly investigated either.

Discussions

This section of the report included recommendations for different stakeholders, including as service providers, PETs designers, end users, and regulators.

1. **Recommendations**

In order to determine which interventions (and their qualities) are most suited for improving access, researchers may also involve users in participatory studies. Some of the irregularities and dark patterns that were discovered in Study 1's display of the cookie notices and user opt-out paths have also been demonstrated by others. For instance, a website might refuse to deliver services to a user until the user's device's track-blocking software is disabled. It was advised that websites carefully review their privacy policies and strive for legal, ethical, and moral procedures. According to Study 2, a number of techniques exist that, secretly to users, may differ in how well they block tracking. However, this may not be true for all nations and genders. Users' own research may be the most reported method of learning about protective techniques overall. A close second favored way for learning through social ties is social media.

In a language that corresponds to consumers' limited awareness of tracking and cookies, designers should be clear about the level of protection provided by specific PETs. Additionally, designers must consider how people learn about PETs differently depending on their country of origin and gender. More study is required to determine the most effective ways to inform users of PETs. Creating PETs repositories and improving the accessibility of validated recommendations for non-expert users may also be beneficial.

The methods available to end users to limit and/or prevent internet tracking activities are numerous. Based on Chromium, the open-source variant of Google Chrome, Brave Browser was created. While waiting for the website to load, the user will be safeguarded against tracking by a built-in track blocker. Education (using free online courses and reputable sources like the ICO [37]) is another way to enhance user privacy experiences. Users can also manage privacy settings across all of their user accounts and exercise their data privacy rights by contacting service providers and other relevant organizations. Additionally, users might be urged to speak candidly about their online privacy protection experiences. Also made easier by this would be the growth of online groups that value privacy more.

2. Online Privacy Regulations

In order to create more efficient and occasionally unique regulations, regulators must first assess the demands. Evidently, the tracking business was able to influence election outcomes by using efficient micro-targeting advertisements. To address the specific abuses of gathered monitoring data, the regulators should think about modifying the law. Laws regarding political advertising, for instance, must to be crystal clear. Multiple factors should be considered for more effective legislation rather than general rules. Tracking across demographics, nationalities, and purposes is one of these dimensions. The ICO has already begun to establish detailed rules for certain important data protection subjects involving children, ageing, and AI. More settings should be included in such initiatives.

There are gaps between the PETs that are advertised on websites, those that consumers use, and the methods via which they learn about them. Furthermore, relatively few websites adhere to legal standards. When such a wide variety of infractions exist, one would wonder how effective enforcement of data protection legislation is even conceivable. In addition to the other services that these data protection authorities can provide (such as reporting a breach, filing a complaint, and paying fees), they also offer a set of technical recommendations that translate legal requirements into technical terms (such as the criteria for cookie notice.

The App Tracking Transparency (ATT) policy from Apple is an illustration of self-regulation in the industry. For its Play Store and apps, Google is also developing a privacy feature akin to this. According to some recent statistics, 96% of US users have chosen not to employ app tracking since iOS 14.5 was released. As an illustration, it implies that iPhone users are now encountering many more privacy notices when using their usual apps. Each of these messages requests users' consent to "track their activities across other firms' apps and websites," and provides users with the choice to "Ask App not to Track" or "Allow" in addition to the app name being displayed in the Tracking menu inside the user's broader iOS Privacy settings, which may be used to make additional manual adjustments. The iOS 14.5 privacy statement from Apple makes it simpler to reject app tracking. For its Play Store and apps, Google is also developing a privacy feature akin to this. Although some studies claim that 96% of US consumers opt-in, this number may not be exact. For its Google Play Store and apps, Google is also developing a comparable privacy feature, but the specifics of this project are still unknown.

Future research should focus on data about "marginalized user groups" across various platforms, including PC, mobile, and IoT. A proactive approach might be taken into consideration in order to preserve user privacy more effectively through strong collaboration between regulators and researchers.

Conclusion

From all angles, including monitoring techniques, protection technologies, legal requirements, and user considerations, online tracking is chaotic and complex. Internet users can better protect themselves with the aid of privacy-enhancing products and techniques. It is challenging for them to properly embrace such instruments, nevertheless, due to the intricacy of the regulations and how they are implemented and enforced.

In Study 1, we first looked at cookie notice presentation and control options in 100 prominent EU websites, and then we assessed the challenges of opting out in two scenarios: 1) when a user visits the websites for the first time, and 2) when a user changes their mind and wants to opt out of previously accepted privacy settings. In Study 2, 614 users in the UK, Germany, and France were polled on whether or not they use online tracking protection, as well as about how they do so. How do they learn about these defence strategies was another question posed to them (e.g. via research, friends and family, Facebook, etc.).

The protection strategies used by users were found to not always correspond with the PETs provided by online service providers, and some of the strategies employed by users do not at all prevent tracking. There is a startling disconnect between privacy laws, how websites present PETs in the real world, and how users learn about and use PETs. Researchers, politicians, service providers, and designers of PETs must all work urgently to close the gaps in this field.