A Cross-Platform Evaluation of Privacy Notices and Tracking Practices

Maryam Mehrnezhad
School of Computing, Newcastle University, UK
maryam.mehrnezhad@ncl.ac.uk

***Abstract*—As online services diversify, protecting user privacy becomes more complicated since user tracking as well as presented privacy options vary across platforms. We conduct a cross-platform evaluation on three different platforms: PC browser, mobile browser, and mobile apps, which is the first study of its kind. We study the tracking behaviours, privacy notice presentation, user control options, and further privacy enhancing technologies. Our study considers the top 116 EU websites and their corresponding Android apps (available for 101 out of 116 services). The results show that the privacy consent banner is presented to the user in various and inconsistent ways across websites, browsers, and mobile apps, where the majority of these consent notices do not comply with the GDPR. In addition, most of these services start tracking the user right after the website is loaded and the app starts running, without waiting for the user to interact with the privacy consent. This behaviour can be considered not respectful to the user and is, indeed, not-compliant to current regulations.**

***Index Terms*—Online Platforms, Privacy Enhancing Technologies, Data Privacy Right, Cookie Consent, Online User Tracking, GDPR**

1. Introduction

Online services are diversifying at a high speed. From websites on PCs, tablets, and mobile browsers, to mobile apps, smart wearables (e.g. fitness and medical), smart home services, and other Internet of Things (IoT) platforms, companies are offering a vast range of online services using heterogeneous technologies. The types of available operating systems, browser applications, and system resources generating personal data (e.g. GPS, pictures and files, sensor data) vary on these platforms.

By moving online services from conventional platforms to smarter technologies, the generated (and potentially personal) data diversifies intensely. The sensors available on smart devices and infrastructures enable them to generate all sorts of data about people and their activities and environments. Although the sensitivity of certain smart systems such as medical wearables is more intuitively visible, the risk of sharing data in other systems might not be immediately perceived. As an example, the sensor data coming from a smart building office (light, CO2 level, etc.) can easily compromise the occupant's privacy (e.g. their presence, number of meetings and people in the room). Ambient and motion sensor data is not typically protected in such systems and is freely available to developers [13]. Is has been previously reported that sensor APIs are accessed in 3695 of Alexa's top 100K websites, 63% of whom also engage in browser fingerprinting [1].

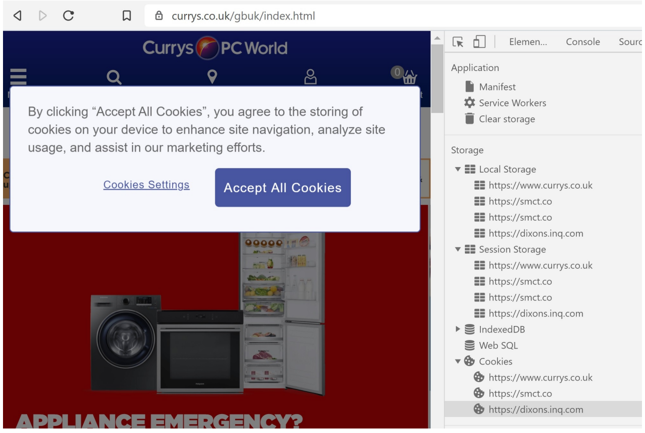
The research community has intensively studied user online privacy specially on PC browsers and after the enforcement of the General Data Protection Regulation (GDPR). These studies cover a wide range of topics including consent notice [2], [12], [15], [20], [25], tracking activities [2], [9], [12], [20], [24], user studies [6], [25], and legal aspects [12], [21]. User online privacy on mobile devices has been mainly studied on apps (as opposed to mobile browsers); e.g. [1], [7], [14], [17], [19]. Some levels of inconsistency have been previously shown, e.g. authors of [17], [27] found new trackers in the mobile ecosystem, which had been unknown to the web-based blacklists. Limited research of this kind is available on IoT platforms (e.g. smart TV apps [26]).

Measuring the tracking behaviour of online services across platforms has been limitedly done prior to the enforcement of the GDPR e.g. [11]. In a recent work [27], tracking behaviour of websites on desktop and mobile environments has been studied through browsers only. To the best of our knowledge, there is no previous work studying the privacy notices and tracking practices of online services across three platforms (PC browsers, mobile browsers, and mobile apps) after the enforcement of the GDPR. In this paper, for the first time, we conduct such a study. We examine Alexa's top 116 EU websites and their corresponding Android apps (101 apps) for their tracking behaviours, user privacy consent presentation and control options, and further Privacy Enhancing Technologies (PETs). Our contributions fall into four categories:

Privacy notice: We study the privacy banner of these websites in three browsers (Firefox, Chrome, and Brave) on PC and mobile as well as their corresponding Android apps. We visit each website in three browsers on Windows and Android and observe if there is any privacy notice and how is it presented to the user. We also install the corresponding Android app of each of these websites and analyse their privacy notice too. We categorise these designs and compare them across platforms and browsers as well as against the best practices.

Control options: We repeat the above experiment for the available user control options. For each privacy consent, we observe what control options (accept, reject, settings, links, none) are offered to the user and whether any of these options are emphasised over others. We categorise the available practices across platforms and evaluate their compliance with the law.

Tracking activities: We study the tracking practices of these services in browsers and apps. We use Brave (a privacy-oriented browser) [22] for websites on Windows and Android and Lumen Privacy Monitor app [18] for



By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

Figure 1. An example of tracking cookies being placed in the browser before any user interaction with the privacy notice in Brave (Shields down). When Brave’s Shields are up, this privacy notice gets blocked.

Android apps. Brave and Lumen report the number of tracking activities of websites and apps, respectively. In this paper, we only observe the tracking activities of each web service on its first page and before any user interaction with the privacy notice.

Available PETs: Finally, by following the contents and links provided in the privacy notice, we visit multiple pages in each website and categorise all the available privacy enhancing technologies (browser, mobile, and website settings, cookie opt-out, add-on, etc.) presented to the user.

Our results demonstrate that:

- The privacy notices on websites and apps are displayed in various locations (top, bottom, middle, full-page) and ways (in-line, overlay, new-page) across services, browsers, and platforms. The most popular designs found on these websites and apps are not necessarily the most effective ones in terms of the likelihood of user engagement.
- The user control options in these cookie consents are inconsistent across services, browsers, and platforms where the majority of these services nudge the user to accept the notice; a practice which is not-compliant with the law.
- The majority of these online services start tracking the user before any interaction with the privacy consent (Figs. 1 and 2); another non-compliant behaviour which was observed in all platforms.
- The offered PETs vary across websites and most of them require the user to go much further than the first page to find and use them.

In Section 2, we describe the details of our experiments and in Sections 3, 4 and 5, we present the results at length. We discuss the results, limitations, and future work in Sections 6 and 7, and conclude the paper in Section 8.

2. Methodology

In this section, we explain the methods, tools and experiments of this paper.

2.1. Cross-platform evaluation

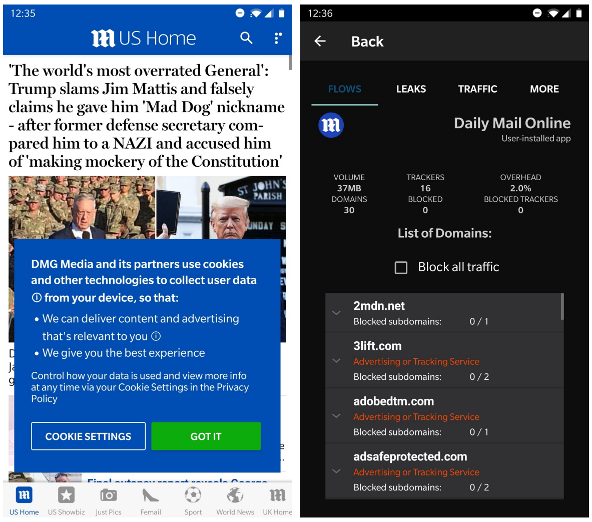
We run our experiments using three different browsers (Chrome, Firefox, and Brave) on PC (Windows 10) and mobile (Android 9), and where available the latest version of the corresponding Android apps of the websites. Chrome and Firefox are the most popular browsers both on Windows and Android. We also use Brave which is a free, open-source and cross-platform browser developed based on the Chromium web browser. Brave uses a block-by-design mechanism that blocks and reports ads and website trackers while the webpage is getting parsed (more details in Section 2.5).

We use Google Chrome (ver 81.0.4044.122 on Windows and 81.0.4044.117 on Android), Mozilla Firefox (ver 75.0 on Windows and 68.7.0 on Android), and Brave (ver 1.7.98 on Windows and 1.5.131 on Android). For each browser on both PC and mobile, we use the default settings and make sure that all the cookies and site data are removed before opening each website. All the experiments were conducted in April and May 2020 and on one laptop PC (screen size: 13 inches, resolution: 3200 x 1800 pixels) and one Android phone (screen size: 5.5 inches, resolution: 1920 x 1080 pixels). The browsers were full screen on PC and they were in the portrait mode on the phone.

2.2. Case study

As a case study, we use Alexa’s top 150 EU websites in April 2020 where we exclude 34 of them since they are either non-English, down, or redirect to another website already in the list. These websites vary in their purposes and services, ranging from search engines and news to gaming, social media, shopping, etc. When the website (and later its app) require us to choose a location and language to continue with its service, we pick UK and English. Note that based on the EU and UK agreement for securing a smooth transition due to Brexit, the UK will remain subject to all EU laws until 31 December 2020 (unless extended). Furthermore, the organisations will likely be subject to regulatory responsibilities under both the EU and UK versions of the GDPR [3].

We also search for the corresponding Android app of each website in Google Play app store to conduct our studies on mobile apps too. Some of these services offer more than one app. Due to the nature of this research, the experiments are conducted through a manual process, therefore, we choose to test one app as the representative of each service. We install the most popular one (in terms of the number of downloads) which, in most cases, is the main product of the company. This is a tedious process and many similar apps are available in the market which are not provided by the intended service. One way of finding the right app is to check whether the app’s developer details on the app store –including the provided website-matches the intended service or not (which might be the parent company). Another way is to visit the website and search for a link to its Android app in the related pages (e.g. about or contact). We use a combination of these approaches to make an accurate list of Android apps of top EU websites resulting in 101 Android apps out of 116



12:35

US Home

'The world's most overrated General': Trump slams Jim Mattis and falsely claims he gave him 'Mad Dog' nickname - after former defense secretary compared him to a NAZI and accused him of 'making mockery of the Constitution'

DMG Media and its partners use cookies and other technologies to collect user data ⓘ from your device, so that:

- We can deliver content and advertising that's relevant to you ⓘ
- We give you the best experience

Control how your data is used and view more info at any time via your Cookie Settings in the Privacy Policy

12:36

Daily Mail Online
User-installed app

VOLUME 37MB
DOMAINS 30
TRACKERS 16
BLOCKED 0
OVERHEAD 2.0%
BLOCKED TRACKERS 0

List of Domains:

□ Block all traffic

2mdn.net
Blocked subdomains: 0 / 1

3lift.com
Advertising or Tracking Service
Blocked subdomains: 0 / 2

adobedtm.com
Advertising or Tracking Service
Blocked subdomains: 0 / 1

adsafeprotected.com
Advertising or Tracking Service
Blocked subdomains: 0 / 2

Figure 2. An example of an Android app's cookie consent (left) and the identified trackers by Lumen (right) before any user interaction with the privacy notice.

websites. Please see Appendix 1 for the list of websites and apps (and the number of installs).

2.3. Privacy notice and control options analysis

In order to analyse the privacy notice of the case study websites, we open them in Chrome, Firefox and Brave on our PC and mobile. Note that some browsers provide a developer tools option on PC and a desktop view on mobile to allow changing the website view from desktop to mobile and vice versa. However, in this paper, we perform our experiments directly on the PC and mobile device for real-world results.

We don't interact with any notification in these websites (e.g. location permission, update notification). In each website, we observe whether there is a privacy notice and how it is presented to the user in each browser. We copy the content of the privacy notice to our database and log the location of it in the page (e.g. top, bottom, middle).

In the next set of our experiments, we install the corresponding Android apps (apart from Google which is a pre-installed system app) and observe how the privacy notice (if any) is presented to the user when opened for the first time. In some apps, users can familiarise themselves with the app via a few introduction pages leading the user to the actual first page (this was not seen in any of our websites). We either skip this or, where not possible, click next. Some apps ask for particular permissions (e.g. location, photos, notification) or settings (e.g. make lists, choose service preferences), we reject them all. Note that some websites and apps need the user to log-in. If we cannot continue as a guest, we don't log-in, and therefore, we don't observe whether there exists any privacy notice behind the log-in page.

In each website (on PC and mobile and in three browsers) and its corresponding Android app, we analyse the user consent notice to identify the user control options. After extracting the options and listing them, we categorise them based on the choices they give to the user (e.g. agree or reject, agree or further options, available links, no option). The results are reported in Section 3.

In addition, by following all the possible routes in the privacy notice of each website (clicking multiple buttons and links) and reading all the privacy policy related pages, we list the available PETs offered to the users and categorise them. The results are presented in Section 5.

2.4. Tracking behaviours

PC and mobile browsers: In order to study the tracking behaviours of these online services, we open each website in Brave [22] on PC and mobile and don't interact with them (i.e. no click, no log-in, no scroll, etc.). We specially don't interact with the privacy notice and just let the website be open in the browser for an hour while carrying on with the normal usage of the computer and mobile.

We do not change the default settings of Brave when conducting our experiments. In both Windows and Android versions of Brave, 'Brave's Shields' are 'UP' by default. When the Shields icon is clicked, a few items are listed: Cross-site trackers blocked (default setting: on), Connections upgraded to HTTPs (on), Scripts blocked (off), Cookies blocked (options available), and Fingerprinting blocked (options available). We log the number of the reported cases for each website.

In the mobile version, two sections are presented to the user when the Brave icon is touched. The first section (Blocking Monitor) is a report of the website's tracking activities and includes Ads & trackers, HTTPS upgrades, Scripts blocked, and Fingerprint methods. In the second section (Individual Controls), the user can change these settings: Block ads & tracking (default: on), HTTPS everywhere (on), Block 3rd party cookies (on), Block scripts (off), and fingerprinting protection (on). An example of trackers and cookies placed in the browser when Brave's Shields are down is shown in Fig. 1.

Mobile apps: In order to observe the tracking behaviour of apps, we use Lumen Privacy Monitor app (ver 2.2.2) [18] (a privacy enhancing free Android app) to analyse each app's traffic and communications. Lumen reveals how each app communicates with tracking services and list the level of the sensitivity of the shared data (device model, fingerprint, etc.). Lumen doesn't require root permissions and leverages the VPN API on Android.

We install Lumen on our Android device and allow all the permissions and the VPN request. Then we open the apps and leave them in the background for an hour while carrying on with the normal usage of the mobile device. We report the contacted domains and identified trackers by Lumen for each app. An example of the reported trackers and domains by Lumen for an Android app is shown in Fig. 2. The results are reported in Section 4.

2.5. Brave and Lumen overview

Brave adopts various privacy enhancing techniques which are not possible at the browser extension level (due to access restrictions and performance limitations) making it a powerful tool to observe tracking behaviours of websites [4], [5], [10], [16]. In addition, privacy-oriented extensions are limited on mobile browsers and are not suited for our experiments. Among other privacy-oriented browsers and search engines (e.g. Tor and DuckDuckGo),

Position		PC Browser	Mobile Browser
Bottom	Overall	43%	48%
	Right	5%	1%
	Left	2%	-
Middle	Overlay	22%	11%
	In-page	1%	1%
Top	Overlay	7%	2%
	In-page	11%	8%
Full-page		-	20%
No notice		9%	9%

TABLE 1. PRIVACY NOTICE PRESENTATION IN THE TOP 116 EU WEBSITES, PC VS. MOBILE

Position	Android App
Full-page	16%
Middle	8%
Bottom	7%
Top	1%
No notice	51%
Left behind log-in	17%

TABLE 2. PRIVACY NOTICE PRESENTATION IN 101 ANDROID APPS (OF 116 EU WEBSITES)

Brave is the only one which reports the tracking activities of the websites on PC and mobile, making it a suitable choice for our experiments. Instead of using URL-based approaches and behaviour-based blocking, which are prone to evasions, Brave uses ML-based classifiers at different levels (network, layout, JS) e.g. via JS code [10], browser's image rendering pipeline [23], and browser Reader Mode [5]. These ML-based approaches are not limited to lists and can adapt as trackers adapt [22].

Lumen runs directly on the mobile device itself and can comprehensively (system-wide) observe the app, device and network activities. In contrast to dynamic and static analysis, and network traffic analysis approaches which don't offer access to real-world data, Lumen monitors app behaviour and network traffic under regular usage and network conditions [18]. Lumen uses the Android VPN permission to capture and analyse the network traffic, including encrypted flows by inserting itself as a middleware between apps and the network interface. Lumen employs a transparent man-in-the-middle (MITM) proxy for TLS traffic with user consent. It adopts deep packet inspection techniques to analyse app payload and identify sensitive data exported by apps, not only within the regular flows but also within compressed flows in order to identify the obfuscated privacy leaks. Lumen uses a list of known tracking and advertising domain names and compiles it using anonymous tracking data received from its real users [17], [18].

3. Privacy Notice Results

In this section, we compare the privacy notice presentation and user control options in three browsers on Windows and Android, as well as Android apps.

3.1. Privacy notice presentation

Browsers on Windows: Table 1 demonstrates how the privacy notice is presented in inconsistent locations across these websites on PC in Firefox and Chrome (which were identical). We observed three locations for these privacy notices: bottom, middle and top. All the bottom and middle notices (except one) and around one third of the top notices were shown as an overlay. Note that the overlay presentation is another layer on top of the main page and will still be visible when scrolling. In contrast, an in-line presentation will go out of the user's sight when scrolling down since it is actually a part of the page.

In half of the cases, the privacy notice was shown to the user at the bottom of the page and in various ways, font sizes, colours, and locations (overall, right, left). In 23% of the websites, the banner was shown in the middle of the page and as an overlay (except one case). In 18% of the websites, the notice was shown at the top of the page where in 8 cases it was shown as an overlay banner and in 13 websites it was an in-page presentation.

Brave behaved differently in 21 cases. In 16 cases, it completely blocked the privacy notice when it's Shields were on and showed the exact privacy notice (to Mozilla and Chrome) when the Shields were off. In 4 cases, the privacy notice was shown at the bottom of the page as opposed to the centre (compared to Mozilla and Chrome). When the Shields were off, only two cases changed the location from bottom to centre. There was one case where the privacy notice was blocked, and after the Shields were off, it was shown at the bottom as opposed to the centre (as seen in Mozilla and Chrome). We will discuss potential reasons for Brave's behaviour in Section 6.

Browsers on Android: It is more challenging to classify the location of the privacy notice on mobile devices due to multiple screen sizes. We observed that in many cases the privacy notice would take a much larger area of the page –sometimes the whole screen. Therefore, in this section, we add a new category: full-page which means that the privacy notice occupies the whole screen (e.g. Fig. 3). Evidently, full-page notices also exist on desktop websites, however, our sample set did not happen to contain such websites. In all cases on PC, even if the privacy notice occupied a big part of the screen, some parts of the website were still visible to the user.

As it can be seen in Table 1, the notices located at the bottom were still the most popular ones (49%). However, many top and centre banners appeared as full-page privacy notices on our mobile device (20%). 12% of the websites presented the banner in the centre, and 10% at the top. These results were based on Firefox and were identical to Chrome's results.

In general, 15 websites presented the privacy notice in a different location compared to their PC versions. This excludes those websites on PC that their privacy notice at the top and in middle of the page occupied the whole screen in the mobile browser. Except one, all bottom-right and bottom-left banners (7 websites) moved to the bottom-overall category. The other inconsistencies included: bottom and top to centre (3 websites), top and centre to bottom (3 websites), and bottom to full-page (2 websites).

Except for one website, the inconsistencies found in Brave and other browsers on Windows, in addition to the above ones were observed here too. In Brave on Android, one of the websites did not show any privacy notice (as expected) even when the Shields were off.

Category	Default	PC Browser	Mobile Browser
Agree or Reject	No default Agree Reject	3% 2% 1%	3% 2% 1%
Agree or Settings	No default Agree In-page options	8% 36% 2%	8% 35% 2%
Only agree		28%	27%
Links		12%	14%
No notice		9%	9%

TABLE 3. Privacy notice user control options in top 116 EU websites, PC vs. Mobile

Category	Default	Android App
Agree or Reject	No default Agree Reject	5% 2% -
Agree or Settings	No default Agree In-page options	2% 13% -
Only agree		8%
Links		2%
No notice		51%
Left behind log-in		17%

TABLE 4. Privacy notice user control options in 101 corresponding Android apps (of 116 EU websites)

Android apps: Table 2 shows how the privacy notice is shown in mobile apps (101 available apps out of 116 web services) when opened for the first time.

Note that due to the platform and usage differences in browsers and apps, studying mobile apps is not as straightforward as websites in browsers. As we observed in some cases, the corresponding apps of certain websites (e.g. banking) would require the user to log-in once the app is open to be able to use the app. 17 apps fall into this category. In case of any requested permission, we deny (unless we had to accept to be able to open the app). We close all the other notifications (e.g. C-19 related ones) to be able to get to the first page. After we open each app, if presented with any form of consent (e.g. terms and conditions), we don't give the consent and leave the app open in that status.

As shown in Table 2, under the described test condition, 52 apps had no privacy notice, 16 apps showed a full-page notice (and sometimes had to scroll down since there was too much content), 7 apps had a bottom-page presentation, 8 apps showed the privacy notice in the middle and one at the top of the page.

As we observed, the privacy notice presentation in apps is significantly different from the mobile browser. Our further analysis shows that in many cases the privacy notice would disappear when replacing the website with the app. In those cases that both website and app presented a privacy notice to the user, the two notices were not necessarily identical at many levels (design, location, control options, etc.). An example is shown in Fig. 3.

3.2. User choices

We analysed the privacy notices of these websites and apps by parsing the content and options available to the user. Based on our observations, we categorised the control options in terms of the user choices as follow:

- **Agree or Reject**: This is when the two options –Agree (Agree, Accept, OK, Understand, etc.) or Reject (Reject, Decline, No, etc.)– are presented to the user with the same level of control (two buttons). These notices fall into three groups: (i) none of these options is emphasised (activated, coloured, etc.) over the other one, (ii) Agree is emphasised, and (iii) Reject is emphasised.
- **Agree or Settings**: This is when the two options –Agree or Settings (Options, Settings, Policy, Manage, Learn more, etc.)– are presented to the user with the same level of control (two buttons). These notices fall into three groups: (i) none of these options is emphasised, (ii) Agree is emphasised by default (we observed no cases where Settings were emphasised), and (iii) Agree is emphasised, but control choices are available in the privacy notice where the user can change the preferences and apply without going to a new page.
- **Only Agree**: When the banner has only one option for the user to click: Agree. Other options would be available as links (e.g. settings, and links to privacy policies, e.g. Fig. 3, left).
- **Links**: When the privacy notice is only notifying about the cookies without providing the user with any immediate options (no buttons). This notice would include links to privacy policy pages or/and options of the website.
- **No Notice**: When the website displays no privacy notice at all.

Browsers on Windows: As it can be seen in Table 3, 46% of the websites' control options were: Agree or Settings. The next popular group is Only Agree (28%). 12% of the websites only provided links to their privacy policies and 9% of the websites did not have any privacy notice. Only 6 websites provided an Agree or Reject form of control options, where 3 of them had neither of the options emphasised, in 2 websites the Agree button was emphasised, and interestingly, in one case (Belgium.be) the Reject button was emphasised.

Brave behaved similarly in terms of the control options presented to the user for those websites that it didn't block their privacy notice (Shields on), except in one case. In one website there was a privacy notice with only Links in Brave (vs. Agree or Settings in other browsers). When the Shields were off, all the other websites (including the above exception) showed the same control options.

Browsers on Android: As reported in Table 3, except for two cases, we observed the same privacy notice control options seen on Windows in Firefox and Chrome on mobile. In one website, the control options changed from Only Agree (on PC) to Links (on mobile), and in the other website, it changed from Agree or Settings to Links. Brave changed the privacy options in the first case above, but not the second one.

Brave also showed the same inconsistencies seen on Windows (vs. Firefox and Chrome) for the exception reported in the previous section when it Shields were on and off.

Android Apps: As it was explained before, only around one third of the 101 apps had a privacy notice. Similar to the presentation of the privacy notice, the user control options in mobile apps were also significantly inconsistent with the ones offered on the websites (Table 4). 15 apps presented an Agree or Settings design where in most cases Agree was emphasised. 7 apps offered an Agree or Reject design where in 5 cases none of the options was emphasised. 8 apps provided an Only Agree design and 2 only had Links. Our further analysis shows that these control options are not necessarily the same as the ones seen in the corresponding websites (e.g. Fig. 3).

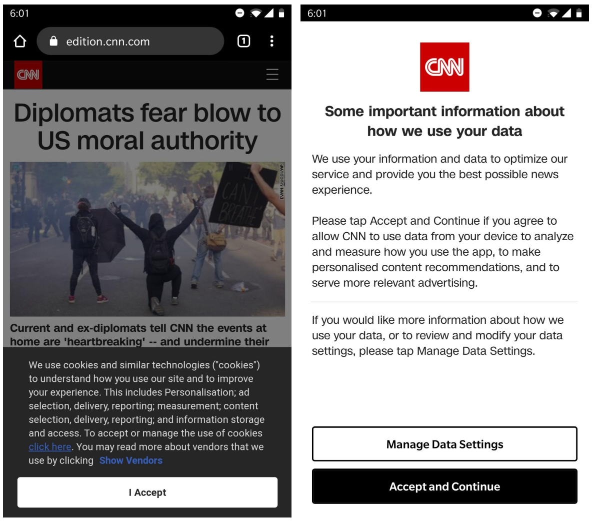
3.3. Further analysis

Privacy notice position: As reported in [25], users are more likely to engage with a notice positioned in the lower left side of the screen in PC and lower part of the screen on mobile; a practice which was not dominant in our websites on PC and Android apps. In [25], the most popular location of 1,000 privacy notices (drawn from 5,087 popular EU websites in 2018) in PC browsers was also bottom. However, the second popular position was top as opposed to the centre which was the case in this study. Note that, based on our results, the most popular location category in mobile apps and second most popular in mobile browsers was the full-page display which has not been studied in [25].

We also noticed that there is a substantial difference between the content of the privacy notice when presented in the browser vs. app. Our observations show that the privacy notice in the app does not include the word 'cookie' in many cases (Fig. 3). We also noticed that some websites and apps would change the way they display their privacy notice to the user on the further visits even if the user doesn't interact with the notice in the first visit. These sorts of inconsistencies need further investigation in the future.

User control options: According to Information Commissioner's Office (ICO)'s guidelines [8], cookie consents which only provide Agree buttons and/or links, or emphasise Agree over Reject or other options, are not complying with the law. In addition, such dark patterns substantially impact people's acceptance of cookies [15], [25]. According to our results, the majority of the consent notices shown in the browser (PC and mobile) and mobile apps suffer from such non-compliant designs. In [15], the authors study the consent management platforms (CMPs) on the top 10,000 UK websites in 2019 where only 11.8% of them meet the minimal requirements set based on the GDPR. These requirements include (i) no optional boxes pre-ticked, (ii) reject all as easy as accept all, and (iii) consent is explicit. We observed that 12% of the websites on the PC and mobile meet such requirements in our sample set. However, only 7% of our mobile apps satisfy those conditions.

Authors of [12] report that 47% of 1,426 EU websites with TCF[1]-related cookie banners (2019) offer preselected choices within their cookie notice, while 7% of these websites do not provide any means to refuse consent. While we observed similar behaviour for the pre-selected choices (around 40% in PC browser), the websites with no refuse option appeared much more frequent in our sample set in the PC browser (28% with only Agree button, and 12% with Links only).



Diplomats fear blow to US moral authority

Current and ex-diplomats tell CNN the events at home are 'heartbreaking' -- and undermine their

We use cookies and similar technologies ("cookies") to understand how you use our site and to improve your experience. This includes Personalisation; ad selection, delivery, reporting; measurement; content selection, delivery, reporting; and information storage and access. To accept or manage the use of cookies click here. You may read more about vendors that we use by clicking Show Vendors

Some important information about how we use your data

We use your information and data to optimize our service and provide you the best possible news experience.

Please tap Accept and Continue if you agree to allow CNN to use data from your device to analyze and measure how you use the app, to make personalised content recommendations, and to serve more relevant advertising.

If you would like more information about how we use your data, or to review and modify your data settings, please tap Manage Data Settings.

Figure 3. An example of inconsistencies in location, user options, and content of privacy notice of a website in mobile browser (left) vs. its mobile app (right).

The results of this paper, in addition to those found before, prove that the exiting non-compliant practices are spreading from websites on PC browsers, to mobile browsers and apps too; making it more challenging to protect user online privacy.

4. Tracking Activities Results

In this section, we present our observations of the tracking activities captured by Brave for websites on Windows and Android, and Lumen for Android apps.

4.1. PC and mobile browsers

Note that tracking is an un-deterministic activity, so are blocking reports. Tracking behaviours might be different for the same webpage on different devices and when visited at different times. Therefore, in order to achieve more comparable results, we opened each website on Windows and Android and observed their tracking behaviours about the same time.

We logged the reported tracking activities by Brave (Shields Up) on PC and Android at three different times: (i) in less than half an hour within the page first visit while engaging with the browser, (ii) around an hour after the page visit while the browser was open, but not necessarily engaged, and (iii) after one hour and when turning the Brave's Shields off and on. We chose these test conditions in order to examine the tracking practices of these websites under regular usage of the browsers and operating systems.

A scatter chart for the number of tracking activities reported by Brave on Android vs. Windows for these three test conditions is shown in Fig. 4. We observed the followings:

- The number of tracking activities on the two platforms are generally within the same range and very strongly correlated (Spearman's correlation

[1] IAB Europe's Transparency and Consent Framework (TCF)

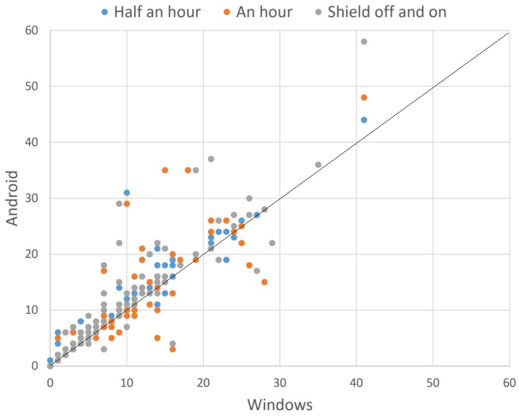


Figure 4. Scatter chart of tracking activities blocked by Brave in Windows vs. Android in three different test conditions for 116 websites.

coefficient = 0.92, test condition: an hour). The most significant mismatches were observed on both sides of the line in Fig. 4.

- In all the three conditions, the average tracking activities reported on Windows were less than Android (8.6 vs. 9.6, 8.7 vs. 9.5, and 8.5 vs. 10.1, respectively).
- Windows' results were more stable across the three test conditions i.e. the range of the reported numbers were closer in comparison to Android's results. This can be due to various factors e.g. the differences between the OSs, versions of Brave, websites designs, etc.

4.2. Mobile apps

In order to report the tracking activities of Android apps, we opened each app and did not interact with them at all (similar to the websites). However, in previous sections, sometimes we had to interact with the app (e.g. language and country selection and permission control) to find out if any privacy related content is available in further pages in the app. Hence, the desirable test condition was disrupted. In such cases, we uninstalled and installed the app again in order to report the results of this section.

We opened the 101 Android apps in three batches (of 33-34) and let them be open in the background. Then we turned on Lumen and engaged with the mobile device for an hour. Lumen monitors all the app connections by recording the data and then reassembling and processing it when the connections close. Therefore, its reports are not updated in real-time. Some apps keep their connections open for a long time, and accordingly causing a delay in Lumen's reports. For this reason, we didn't log the results after half an hour and only report the tracking activities after one hour. We also observed that turning Lumen on and off did not impact the results much, hence, we don't report that either.

Out of 101 apps, Lumen didn't report anything for 4 apps. Here we analyse Lumen's results (number of contacted domains and identified trackers) for 97 apps.

- The average tracking activities and domains detected by Lumen were 2.6 and 5.9, respectively. If we exclude those apps that we could not proceed beyond the log-in/registration page, these numbers increase to 2.9 and 6.4, respectively.
- The tracking behaviours of online services reported by Brave and Lumen are moderately related. Our analysis shows the Spearman's correlation coefficient of 0.36 and .049 for trackers and contacted domains in relation to the similar test condition in the mobile browser (website open for one hour). These coefficients are 0.39 and 0.51 when calculated in relation to PC browser.
- Lumen detected a number of privacy leaks for these apps including Network Hostname, Private IP, Time-zone, Board Information, Brand, Device Model, and Build Fingerprint. These items have been sent to trackers without the user's consent via several apps.

Note that the reported tracking activities of these websites and apps are for the first page of each service and before any user engagement with the privacy notice. In other words, our results show that these online services don't even wait for the user to interact with the privacy notice and start tracking right after the service (website, app) starts running. Our findings are consistent with those reported in [12], [21], confirming that user's privacy is potentially violated in online services across platforms depending on the use of these collected data.

4.3. Further analysis

As reported in [12], 10% of websites (out of 1,426 EU websites with TCF cookie banners) register a positive consent before any user interaction with the privacy policy and 5% of the websites store an all–accepting consent even if the user has explicitly opted out in the privacy notice. We found out the majority of the websites and apps start tracking the users regardless of the presence of the privacy notice and before any user interaction with it across platforms.

It has been previously shown that the mobile ecosystem has its unique characteristics especially due to mobile-specific trackers found both on the mobile browser [27] and mobile apps [17]. On a sample size of 23,310 websites studied in 2019, the authors of [27] report that (from the perspective of JavaScript APIs) 762 (13.1%) trackers are mobile-specific, 1,783 (30.6%) trackers are desktop-specific, and 3,290 (56.3%) trackers appear on both mobile and desktop websites. In an older study on 14,599 Android apps (2017) [17], it was reported that 233 out of the 2,121 identified tracking services were previously unknown to other popular advertising and tracking (and mainly desktop-based) lists.

The above findings confirm that tracking on mobile platforms is increasing at a high speed. Although we did not perform any analysis on the similarities of the identified trackers on our tested platforms, we observed that the reported tracking activities by Brave on mobile were indeed higher than those reported on PC. We believe that the risks of mobile web tracking are higher than that of PC tracking since users have a much more personal usage of their mobile devices. We anticipate that the problem becomes more severe as online services expand on other platforms such as IoT with different and constrained user interfaces limiting the users to have control over their privacy.

5. PETs Results

Available PETs: From the user's point of view, it is important to examine what further privacy enhancing tools and options are provided by online services. By following the related privacy links and options available in the privacy notice of each website, we identified the following privacy enhancing options, links and tools for the users:

- **Browser settings**: Changing the browser settings including activating DO Not Track (DNT), and deleting cookies manually, etc.
- **Browser add-on**: Using privacy enhancing extensions such as Google Analytics Opt-out Add-on to prevent data from being used by Google Analytics.
- **Initiatives**: Linking to the related initiatives for more information and tools including European Interactive Digital Advertising Alliance (EDAA) websites (e.g. edaa.eu or youronlinechoices.com/), Interactive Digital Advertising Alliance (DAA, optout.aboutads.info/), Canadian (youradchoices.ca) and Japanese (ddai.info), Interactive Advertising Bureau (IAB) and its European version, Network Advertising Initiative (NAI, networkadvertising.org), allaboutcookies.org, privacyshield.gov, and cookielaw.org.
- **Cookie opt-out**: Opting out of cookies through the privacy notice settings either by the cookie category or by third party name.
- **Website & account settings**: Changing privacy preferences via the website privacy dashboard settings, user account, or for major companies such as Google and Facebook.
- **Mobile & app settings**: Modifying mobile device and apps settings to change privacy preferences.
- **Privacy-aware browsers**: Using a browser that can report and block tracking activities.
- **Account deactivation**: Not using the service any more by deleting or deactivating the user account.
- **Contacting service provider**: Contacting the website via email addresses and/or online forms or links (e.g. privacytrust.com/drs/stackexchange) in case of any privacy concern.

As it can be seen, a wide range of options are offered to the user. Based on our observations, most of the above require the user to go much further than the first page to find and use them. The efficacy of some of these items has been studied in the previous work e.g. [6]. However, the inconsistencies across platforms and for all items, as well as other factors such as the adoption of further online privacy technologies (e.g. anti-spayware and anti-malware, firewall, password manager) by users remain unresearched topics and require more investigation in the future.

6. Discussion

Inconsistencies: In this paper, we observed several levels of inconsistencies concerning user online privacy across platforms. The differences between the presence, position, and control options of the privacy notice in Chrome and Firefox vs. Brave is mainly due to the nature of Brave as a privacy-oriented browser. Brave blocks some of the privacy notices due to its block-by-design approach which is discussed later in this Section.

Our results demonstrate substantial differences between the position of the privacy notice in PC vs. mobile browsers. This is mainly due to the different approaches adopted by website implementers when practising the responsive mode design. As we observed, some of these services change the presentation of the privacy notice when shown on the mobile browser causing inconsistencies between the platforms. Some other websites choose to keep the two designs (PC and mobile) identical resulting in unusable designs (i.e. showing the same privacy notice in a much smaller size on mobile). Some other websites keep the balance i.e. showing the privacy notice in a similar position but with proper settings e.g. the font size.

When moving from websites opened in mobile browsers to apps, the identified inconsistencies grow even larger. Not only the presence, position, and control options of the privacy notices are not consistent, but also there are major differences in the content of these notices (mobile browser vs. app). We reckon two main reasons for this. First, there are fundamental differences between a website opened in the browser and its corresponding app installed on the device (e.g. implementation languages, permission models, tracking technologies, etc.). Second, the website and the app might have been developed by two different teams (even within the same company) involving different legal team members leading to inconsistent practices.

In terms of the differences between the tracking practices across platforms, PC and mobile platforms have dissimilar sets of resources which can be exploited for online tracking. As previously discussed, the identified trackers on the two ecosystems (PC vs. mobile) are not identical [17], [27]. Yet, we observed very strong and moderate correlations between the tracking behaviours of PC browser vs. mobile browser, and browsers vs. apps, respectively.

Apart from the above, other factors such as website and app implementation errors and browser parsing bugs may also contribute to the inconsistencies identified in this paper.

Since the impact of these inconsistencies on user privacy has not been studied in the past, its is not straightforward to simply advise the service providers to avoid such differences between their products to improve the user experience. In many cases, these companies integrate a CMP developed by another company into their systems. Though, a more coordinated practice between the teams developing different products for the same company would improve the product design towards more consistency.

In addition, by following a law-compliant approach lots of these inconsistencies will be resolved automatically. We examined that only 12% of the websites and 7% of the mobile apps meet the requirements of such practice. Hence, we recommend the service providers to follow the available guidelines (e.g. [8]) in order to avoid inconsistencies in their products and improve user privacy.

Reporting to Brave: We communicated our results with Brave and reported the identified inconsistencies.

They acknowledged the issue confirming that in many webpages the privacy notice itself is a tracker; resulting in being blocked by Brave. They believe that the privacy notice is not effective as, in some cases, it is not even taken into consideration. In some cases, cookies are placed prior to the presentation of the privacy notice [12], [21]. In our studies, Brave blocked the privacy notices of 17 websites on PC and 18 websites on mobile; marking them as trackers. Out further analysis also confirms that in some of these websites, the cookies are indeed placed in the browser regardless of the privacy notice existence and/or user interaction with it (Fig. 1).

It was also explained that there have been numerous calls for Brave to simply block all of the privacy banners, but the team believes that if an honest website wants to show a privacy notice, it should be able to. However, even if the user gives their consent, Brave blocks all the tracking activities anyway when its Shields are up. We believe that this inconsistency in the presentation of the cookie notices impacts the user experience which we aim to study in the future.

Brave vs. Lumen: Since the set of techniques used in Brave and Lumen for identification of tracking activities are not identical, the results are not comparable. Brave, as a privacy-oriented browser, is a more powerful tool in comparison to Lumen as a VPN-based privacy monitor app. Though since they both report the tracking behaviours of websites and apps in real-world settings, they give us valuable insights into the tracking activities of online services across platforms. We have reported the Spearman's rank-order correlation in order to observe if online services with higher website trackers also include more trackers in their apps. We found a moderate correlation in this relative comparison. In addition, our most important finding is the fact that both websites and apps do start tracking the user right after the service starts and before any user interaction with the privacy notice.

COVID-19 pandemic: The experiments of this paper have been conducted in April and May 2020 were many EU countries have been under lockdown due to the pandemic coronavirus disease 2019. This may have impacted the Internet usage (top websites, new online services, etc.). When conducting our studies, we noticed that some of the websites and apps present a COVID-19 notice in different ways (similar to the privacy notice). It is not clear how this notice would impact the user experience of dealing with the privacy notice, and whether or not it contains trackers too. This remains to be explored in the future.

7. Limitations and Future Work

Datasets: Our dataset includes 116 EU websites and 101 corresponding apps. We acknowledge that this dataset can be more comprehensive. First, we excluded 34 websites since they were either redundant in the list (7 websites), or did not offer an English version (24 websites), or were down at the time of the experiments (3 websites). Not including the non-English websites has probably skewed our sample set toward UK and Irish websites. We plan to address this in the future by using translation tools and including all the EU websites in the experiments. Second, we do no log into the services that require login in order to offer their services (17 apps, no websites). In some of these apps, we observed the privacy consent is implicitly blended with other items in the login and/or registration pages (which is also another non-compliant practice [8]). We have not included those cases in our results. We acknowledge that for a more inclusive study those apps need to be studied too and we will consider this in our future work. Finally, we plan to perform further analysis on a subset of the websites in our current list in which their apps are available. In this way, we will be able to directly compare those services across platforms.

Tracking behaviour measurement: We have evaluated the tracking behaviour of these services only by visiting the first page and before the user interaction with the privacy notice. Previous research has shown that subsites show a significant increase in privacy-invasive techniques. For example, when crawling websites more deeply, the use of cookies increases by about 36% [24]. Our results show that on such constrained test condition (visiting the landing page and not logging in), the tracking behaviour of these services is still intrusive. Though, we plan to conduct a more in-depth measurement by extending our studies beyond the first page via simulating the user interaction with the service (e.g. accept or reject the cookies) and observing the tracking practices of these services across platforms.

Large-scale experiments: What we have presented in this paper is only a snapshot of the current privacy notices and tracking practices across platforms. We plan to scale up our studies by evaluating a bigger dataset following our cross-platform approach. For that, we need to automate most parts of our methodology e.g. by using machine learning algorithms for privacy notice analysis and natural language and image processing tools for user control options and other PETs.

User studies: We believe that it is equally important to explore the user mental models, perceptions and adoption of tracking protection technologies. We would like to identify the correct and incorrect mental models that underpin users' beliefs in order to evaluate the factors affecting their practices and adoption of these PETs. We would also like to explore how more broad mental models and security and privacy perceptions (general online privacy) impact the user decision making processes for tracking protection. More specifically, we would like to (i) explore user feelings and emotions concerning online tracking and protection, and (ii) find out how the identified inconsistencies in this paper would impact user perception and practice of tracking protection PETs.

8. Conclusion

This paper is the first cross-platform study evaluating user online privacy practices of 116 top EU websites and their corresponding Android apps (101 apps). Our experiments include analysis of the privacy consent notice and user options, observing the tracking behaviour (before user engagement with the privacy consent), and exploring the PETs for tracking protection offered by these online services. We found inconsistencies at different levels across browsers (Firefox, Chrome, Brave) and platforms (PC browser, mobile browser, mobile app). Our results show that the privacy consent banner and user options are presented to the users in various and inconsistent ways across these services and platforms, where most of them are not complying to the GDPR. We also discovered that these services start tracking the user once the service (website, app) starts running and before the user's interaction with the privacy consent; another non-compliant practice violating user's privacy.

This paper, once again, confirms that current practices for protecting user online privacy are not effective and the blind spots are increasing as online services are being offered on various platforms such as mobile and IoT.

Acknowledgment

I would like to thank the reviewers of this paper for their constructive feedback. I thank Dr Abbas Razaghpanah from UC Berkeley, US, for his insight on Lumen, and Dr Hamed Haddadi from Imperial College London, UK, for his valuable feedback on the use of Brave. I also want to thank Dr Ehsan Toreini, from Durham University, UK, for his feedback on the design of the experiments of this paper.

References

[1] Anupam Das, Gunes Acar, Nikita Borisov, and Amogh Pradeep. The web's sixth sense: A study of scripts accessing smartphone sensors. In *ACM Computer and Communications Security*, 2018.

[2] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. In *Network and Distributed System Security Symposium*, 2018.

[3] DLA Piper Law Firm. Uk: Understanding the full impact of brexit on uk: Eu data flows. *Privacy Matters*, 2019, blogs.dlapiper.com/privacymatters/uk-gdpr-brexit-flowchart/.

[4] Gertjan Franken, Tom Van Goethem, and Wouter Joosen. Exposing cookie policy flaws through an extensive evaluation of browsers and their extensions. *IEEE Security & Privacy*, 17(4), 2019.

[5] Mohammad Ghasemisharif, Peter Snyder, Andrius Aucinas, and Benjamin Livshits. Speedreader: Reader mode made fast and private. In *The World Wide Web Conference*, 2019.

[6] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. An empirical analysis of data deletion and opt-out choices on 150 websites. In *Symposium on Usable Privacy and Security*, 2019.

[7] Majid Hatamian. Engineering privacy in smartphone apps: A technical guideline catalog for app developers. *IEEE Access*, 2020.

[8] Information Commissioner Office (ICO). How do we comply with the cookie rules? *ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/ visited May 2020.*, 2020.

[9] Muhammad Ikram, Rahat Masood, Gareth Tyson, Mohamed Ali Kaafar, Noha Loizon, and Roya Ensafi. The chain of implicit trust: An analysis of the web third-party resources loading. In *The World Wide Web Conference*, 2019.

[10] Umar Iqbal and Peter Snyder. Adgraph: A graph-based approach to ad and tracker blocking. *IEEE Security and Privacy*, 2020.

[11] Christophe Leung, Jingjing Ren, David Choffnes, and Christo Wilson. Should you use the app for that? comparing the privacy implications of app-and web-based online services. In *Internet Measurement Conference*, 2016.

[12] Célestin Matte, Nataliia Bielova, and Cristiana Santos. Do cookie banners respect my choice? measuring legal compliance of banners from iab europe's transparency and consent framework. *IEEE Security and Privacy Conference*, 2019.

[13] Maryam Mehrnezhad and Ehsan Toreini. What is this sensor and does this app need access to it? In *Informatics*, volume 6, page 7. Multidisciplinary Digital Publishing Institute, 2019.

[14] Nurul Momen, Majid Hatamian, and Lothar Fritsch. Did app privacy improve after the gdpr? *IEEE Security & Privacy*, 17(6), 2019.

[15] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark patterns after the gdpr: Scraping consent popups and demonstrating their influence. *ACM Computer and Human Interaction Conference*, 2020.

[16] Benjamin Livshits Peter Snyder, Antoine Vastel. Who filters the filters: Understanding the growth, usefulness and efficiency of crowdsourced ad blocking. In *ACM SIGMETRICS*, 2020.

[17] Abbas Razaghpanah, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, and Phillipa Gill. Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. *Network and Distributed System Security Symposium*, 2018.

[18] Abbas Razaghpanah, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Christian Kreibich, Phillipa Gill, Mark Allman, and Vern Paxson. Haystack: In situ mobile traffic analysis in user space. *arXiv preprint arXiv:1510.01419*, 2015.

[19] Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. In *USENIX*, pages 603–620, 2019.

[20] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. Can i opt out yet? gdpr and the global illusion of cookie control. In *ACM Asia Computer and Communications Security*, 2019.

[21] Cristiana Santos, Nataliia Bielova, and Célestin Matte. Are cookie banners indeed compliant with the law? deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners. *arXiv preprint arXiv:1912.07144*, 2019.

[22] Peter Snyder. Next steps for browser privacy: Pursuing privacy protections beyond extensions. USENIX, 2019.

[23] Panagiotis Tigas, Samuel T King, Benjamin Livshits, et al. Percival: Making in-browser perceptual ad blocking practical with deep learning. *arXiv preprint arXiv:1905.07444*, 2019.

[24] Tobias Urban, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. Beyond the front page: Measuring third party dynamics in the field. In *The Web Conference 2020*, 2020.

[25] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (un) informed consent: Studying gdpr consent notices in the field. In *ACM Computer and Communications Security*, 2019.

[26] Janus Varmarken, Hieu Le, Anastasia Shuba, Athina Markopoulou, and Zubair Shafiq. The tv is smart and full of trackers: Measuring smart tv advertising and tracking. *Privacy Enhancing Technologies*, 2020.

[27] Zhiju Yang and Chuan Yue. A comparative measurement study of web tracking on mobile and desktop environments. *Privacy Enhancing Technologies*, 2020.

Appendix

1. List of Top EU Websites and Their Corresponding Android Apps

no.	Website	Android App	Install no.	no.	Website	Android App	Install no.
1	Amazon.co.uk	Amazon	100M+	59	Siemens.com	Industry Online Support	100K+
2	Theguardian.com	Guardian	5M+	60	Lyst.co.uk	NA	
3	Bbc.co.uk	BBC News	10M+	61	Rightmove.co.uk	Rightmove	1M+
4	Who.int	OpenWHO	1M+	62	Tnt.com	TNT - Tracking	.5M+
5	Google.co.uk	NA		63	Theoutnet.com	The OUTNET	100K+
6	Webex.com	Cisco Webex Meetings	10M+	64	Selfridges.com	Selfridges	100K+
7	cnn.com	CNN	10M+	65	Johnlewis.com	John Lewis & Partners	.5M
8	Dailymail.co.uk	Daily Mail Online	5M+	66	Thetimes.co.uk	The Times	.5M
9	Rt.com	RT News	1M+	67	Fxstreet.com	FXstreet	100K+
10	Asos.com	ASOS	10M+	68	Dailystar.co.uk	Daily Star	100K+
11	Cambridge.org	English Grammar in Use	1M+	69	Asda.com	ASDA	1M+
12	Ebay.co.uk	eBay	100M+	70	Ucas.com	NA	
13	Reuters.com	Reuters News	1M+	71	Here.com	HERE WeGo	10M+
14	Bet365.com	bet365	1M+	72	Standard.co.uk	Evening Standard	100K+
15	Dw.com	DW	1M+	73	Wipo.int	WIPO Delegate	1K+
16	Hm.com	H&M	10M+	74	Gumtree.com	Gumtree	10M+
17	Ft.com	Financial Times	1M+	75	Brownsfashion.com	NA	
18	Telegraph.co.uk	The Telegraph	.5M+	76	Prnewswire.com	NA	
19	Independent.co.uk	The Independent	100K+	77	Newscientist.com	New Scientist	.5M+
20	Thesun.co.uk	The Sun Mobile	.5M	78	Radiotimes.com	NA	
21	gov.uk	HMRC	1M+	79	Hotukdeals.com	hotukdeals	1M+
22	Express.co.uk	Daily & Sunday Express	10K+	80	Harrods.com	Harrods	50K+
23	Euronews.com	Euronews	1M+	81	Virginmedia.com	Virgin Media Connect	1M+
24	Oup.com	Oxford Learner’s Bookshelf	100K+	82	Currys.co.uk	Currys PC World	100K+
25	Uk.search.yahoo.com	Yahoo Search	1M+	83	Topshop.com	Topshop	.5M+
26	Eset.com	ESET	10M+	84	Chrono24.com	Chrono24	1M+
27	Britishcouncil.org	LearnEnglish Grammar	1M+	85	Itv.com	ITV Hub	10M+
28	Sky.com	My Sky	1M+	86	Quidco.com	Quidco	.5M+
29	Sap.com	SAP Fiori Client	.5M	87	Easyjet.com	Easyject	10M+
30	Mirror.co.uk	The Mirror App	.5M	88	Hsbc.com	HSBC	1M+
31	Weforum.org	World Economic Forum	10K+	89	Sainsburys.co.uk	Sainsbury’s Groceries	.5M+
32	Metro.co.uk	Metro Newspaper	100K+	90	Riverisland.com	River Island	1M+
33	News.sky.com	Sky News& World	5M+	91	Macworld.co.uk	Macworld Digital Magazine	100+
34	Jdsports.co.uk	JD Women	100K+	92	Serif.com	NA	
35	Ubs.com	UBS Mobile Banking	.5M+	93	Harveynichols.com	Rewards Harvey Nichols	50K+
36	Economist.com	The Economist	1M+	94	Yougov.com	YouGov	.5M+
37	Espncricinfo.com	ESPNCricinfo	10M+	95	Aeroflot.ru	Aeroflot	1M+
38	Thomann.de	Thomann Official	.5M+	96	Nme.com	NA	
39	Cosmopolitan.com	Cosmopolitan	100K+	97	Active.com	Active	100K+
40	nhs.uk	NHS App	.5M+	98	Indeed.co.uk	Indedd job search	100M+
41	Royalmail.com	Royal Mail	.5M+	99	Meltwater.com	Meltwater Mobile	10K+
42	Aruba.it	Aruba PEC Mobile	1M+	100	Nokia.com	NA	
43	United.com	United Airlines	10M+	101	Sportsdirect.com	Sports Direct	1M+
44	Next.co.uk	Next	1M+	102	Belgium.be	NA	
45	Bt.com	My BT	1M+	103	Santander.co.uk	Santander Mobile Banking	1M+
46	Rte.ie	RTÉ News Now	1M+	104	Swissinfo.ch	swissinfo.ch	50K+
47	Tesco.com	Tesco Groceries	1M+	105	Swisscom.ch	Swisscom Storebox	5K+
48	Newsnow.co.uk	NA		106	Barclays.co.uk	Barclays	5M+
49	Voanews.com	VOA News	1M+	107	Diplomatie.gouv.fr	NA	
50	Childrensalon.com	Childrensalon	10K+	108	Rwth-aachen.de	RWTHApp	50K+
51	Thelancet.com	The Lancet	50K+	109	Iop.org	Physics World	10K+
52	Babyshop.com	NA		110	Credit-suisse.com	Credit Suisse Direct	100K+
53	Argos.co.uk	Argos	5M+	111	Opencorporates.com	NA	
54	Skysports.com	Sky Sports	5M+	112	Missguided.co.uk	Missguided	.5M+
55	Channel4.com	All4	10M+	113	Ilo.org	ILO Ergonomic Checkpoints	10K+
56	Ryanair.com	Ryanair	10M+	114	Marksandspencer.com	M&S	1M+
57	Irishtimes.com	Irish Times News	100K+	115	Premierleague.com	PL	10M+
58	Advfn.com	ADVFN Tocks & Shares	100K+	116	Justgiving.com	NA	

TABLE 5. Top 116 EU websites and 101 Android apps