Fianán, Cuacha: Irish Cookie Banners

Ashley Sheil
Department of Mathematics and Statistics,
Maynooth University,
Kildare, Ireland.

David Malone
Hamilton Institute / Department of Mathematics and Statistics,
Maynooth University,
Kildare, Ireland.

***Abstract*—Kampanos and Shahandashti extended the OpenWPM software to study the landscape of Greek and English cookie banners. They end their paper by suggesting other researchers use their code to investigate their own country's cookie landscapes. We decided to take up this challenge and compare our findings to their results and The Data Protection Commission (DPC) for Ireland's report on Irish cookie banners. Similar patterns were observed between the studies with some slight improvement on banner prevalence and other results reported in the DPC report. The presence of invisible banners, where HTML for a banner is present but not displayed, were also noted. The Irish for cookies is interchangeably referred to as Fianán or Cuacha and were not commonly found on Irish websites.**

***Index Terms*—Cookie banners; Dark patterns; GDPR; Online tracking**

I. Introduction

Cookie banners are mostly unavoidable in modern web browsing. We conducted a casual Twitter survey which revealed that 55% of participants hit the most obvious button on a cookie banner, 31% carefully chose an option, 7% left the website, with 6% choosing other. The comments following the survey were particularly interesting. Some participants had a procedure, where they will click accept all and eventually clear cookies at a later date. Others choose based on the website itself, where given an all or nothing choice they may leave, depending on whether a website is deemed to be 'trustworthy'. However, for the most part, it appeared participants didn't put much thought into cookies.

Cookies are, of course, useful in how they make perusing the internet easier: allowing websites to remember what is in our online shopping carts and to remember we have already authenticated. These are known as *session cookies* and *authentication cookies* and are the sort of cookies that many people want permitted, perhaps depending on the lifetime of that cookie. The rejection rate of cookies however, is quite high, which shows that customers are being put off by cookies [1]. *Third-party* cookies, which are cookies set by websites other than the one you appear to be visiting, can be traced back as far as 1996 [2] and are significant when regarding users' privacy online, as they allow a user to be tracked as they visit multiple websites. They have been studied for some time, for example Englehardt and Narayana used an automated OpenWPM script and found that news websites contained the most third-party cookies [3]. They are still a live issue: Google had intended to block third-party cookies in Chrome in June 2021, but have now delayed this until 2023.

This combination of cookie usage creates a challenge for users in deciding what cookies they should accept. In general what a person needs to consider when faced with a cookie banner is "... what purpose they serve, how long they endure, and their provenance." [4] Cookie banners (or notices) were created with the intention of informing the user of their rights and full disclosure of what data is being used, while allowing control over what data is stored. The reality may seem to be otherwise: cookies are more of an annoying chore for both website owners and users [5]. The problem appears to be that either people seem less concerned about their privacy [6] or are just ignorant of what is happening to their data.

In this paper, to explore the landscape of Irish cookies, Kampanos's OpenWPM framework was extended to suit Irish cookie language nuances as well as compiling our own list of Irish websites [7], [8]. Combined with the Tranco [9] list of websites, four thousand Irish websites were identified to investigate. Most cookie studies take the most popular websites to analyse, however our list also takes into account lower traffic websites. The data from the crawl was analysed to identify banner and cookie prevalence along with language and visual differences of Irish banners as well as *dark patterns*.

We continue by giving the background on GDP regulations and cookie banner research in Sec. II. Our method for surveying cookies is described in Sec. III. The results of the survey are presented in Sec. IV and then discussed and compared to the literature in Sec. V. Our conclusion is given in Sec. VI.

II. Background

Since the GDPR was written into law in 2018, a common finding in cookie research is the ineffectiveness of cookie banners and websites lack of compliance with GDPR.

A. Regulatory Situation

The EU formulated the General Data Protection Regulation (GDPR) [10] for data protection and privacy in the European Union. Its aim is to enhance an individual's control and rights over their personal data. Apart from *strictly necessary* cookies, a person has the right to control what data is shared and must give consent. In the EU, if a website stores a person's data as cookies, then they must display a cookie banner that clearly states what data is stored, how long it is stored and whether third-party cookies are used. A user must be able to

decline data storage and accept any cookie that is used. The GDPR is enforced by various national authorities. The Data Protection Commission (DPC) for Ireland is responsible for the enforcement of the GDPR and also ePrivacy laws, which are separate but complement the GDPR [11]. As several large companies have European headquarters in Ireland, they come under the bailiwick of the Irish DPC. The various national authorities are under pressure to uphold these laws, with some complaints claiming investigations can be ineffective and privacy is being abused [12]. Despite this, in 2021 Amazon was issued with a hefty fine of 746M euros for violating GDP regulations. In fact, that same year documented some of the highest GDPR-related fines since its commencement in 2018 [13]. Amazon is a well known company and much in the spotlight, but there are many smaller websites that may be flying under the radar while violating regulations.

Consent for the use of cookies is usually sought by a cookie banner. According to article 4(11) in the GDPR, consent means any "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Consent, however, is an abstract concept and seems to be interpreted in different ways. Krisam et al. refer to the difficulty in fulfilling GDPR requirements with cookie banners, given the architecture of the web and lack of standards [14]. Even if the GDPR was followed by websites, if a person doesn't understand the banner, is it doing its job? A question could be posed as to why there isn't a one-size-fits-all banner that adheres to all regulations, adjusting for individual countries.

With increasing regulation and suspicion of cookies, it seems that they may be slowly falling out of favour. Narayanan points out that while giants of the browser world, like Google's Chrome and Apple's Safari, are phasing out third-party cookies, new technologies are emerging like Privacy Sandbox [15] that aim to serve targeted ads without cookies. Some believe that this will have little effect on tracking by Google and Facebook and will have less privacy benefits than expected [16]. The danger is that this technology is already embedded in your browser and therefore you no longer have the choice to opt out. Smaller companies, who do not have access to this technology, may have to resort to more invasive techniques like fingerprinting to compete [6]. The idea of targeting customers without tracking is not new, with a history going back to at least 2010 [17]–[19].

B. Related Research

Studies in this area focus mainly on GDPR compliance, how users interact with and understand cookies, cookie design and dark patterns. We review papers that look at cookie banners in different EU countries with regards to GDPR compliance and dark patterns. The web's open nature, coupled with the GDP regulations being complex and open to interpretation, mean that ascertaining whether websites are 100% compliant with GDP regulations is difficult [20]. Dark patterns are easier to observe and note with more confidence.

Kampanos [21] found that banners were not universal, just 48% of Greek and 44% of the UK websites included a cookie notice. He found also that direct opt-outs were rare and that the majority of banners are positively phrased leading people to think that they can trust the website. They also note that, compared to previous similar studies on Greek and UK cookies, banner prevalence had decreased. This is contrary to what might be expected with GDPR compliance. They point out that is likely to do with their large sample size, which would include smaller and less popular websites.

The Data Protection Commission's cookie sweep reports on 40 Irish websites [22], highlighting examples of dark patterns, one of which comes in the form of cookie bundling. Here, users are asked to accept cookies, with an explanation stating that cookies are necessary for the website, so unless you look further (and often you can't!), you must agree to marketing and tracking cookies. The DPC report also found that 26% of their participants had pre-ticked options.

In another study, 407 banners were studied and showed that 89% violated at least one legal requirement. Other identified issues included misleading statements, technical jargon, and vagueness [23]. They observe another common pattern in banners: 'necessary vs unnecessary' cookies. The lack of clarity around what is strictly necessary, can leave the user to assume all cookies are necessary.

An analysis of 500 websites [24] notes that since GDPR's enforcement, rather than helping people with their actual privacy choices, it has led to more of a sense of false security. Fouad et al. [25] investigate the legal compliance of 20,218 third-party cookies. Of these 12.85% have a corresponding cookie policy where the word cookie is not even mentioned. They found that 95% of cookies do not have an explicitly declared purpose and are therefore impossible to audit for compliance. They also stress the need for policy makers to agree on unified requirements surrounding cookies and tracking in their definitions for purpose.

Bauer et al. found that design had an impact on user interaction with banners [26]. They tested a banner with a green accept button, hidden details for opting out and positive framing. They compared this to a banner with equal access to opting out and neutral framing. They found that dark patterns, such as highlighted buttons, have a significant effect on users' interactions. The former banner style is still prevalent and observed in this study. Machuletz and Böhme [27] also found that users were more likely to click on highlighted buttons over neutral buttons and to subsequently regret their choices: "...users accept more data collection purposes when consent dialogues integrate a highlighted default button that selects all purposes at once" . Another interesting observation from the same study discusses *multiple choice designs*. When presented with multiple choice, users found they were less likely to recall their choices and also regret them afterwards. This highlights that these multiple choices may cause confusion.

Utz et al. found that users interacted more with left-hand corner banners and, given a binary choice, were more likely to allow tracking compared to banners with options and that

overall, nudging has a big impact to users' choices in online tracking [28]. According to Bermejo Fernandez et al., the position of the banner does not affect users' participation with cookie consent, but buttons that were highlighted did have an impact on users' interactions with banners [29].

More recent work on dark patterns in cookie banners comes from Krisham et al. [14], who looked at 500 websites in Germany. They sorted their list into categories based on the options available to the user, for example an 'Accept All' button. They found a strong prevalence towards nudging users into accepting cookies. Graßl et al. [30] point out that "The use of dark patterns can be problematic for legal as well as ethical reasons. While the GDPR (2016) does not explicitly ban all dark patterns, they do breach the spirit of the GDPR". They refer to three most common dark patterns in banners as 'Default' (pre-ticked options), 'Aesthetic Manipulation' (accept button is highlighted) and 'Obstruction' (where it is difficult to opt for more privacy friendly options). They found that dark patterns did not effect users choosing data-unfriendly options but rather it is a conditioned response for users to choose these options. A possible reason for this is that non-EU websites sometimes will not allow access to a page without consenting to tracking.

Habib et al. [31] found in their review of 150 websites, that, although privacy choices were commonly available, they are sometimes difficult to find and understand. They go on to say that privacy-choice text requires a university education to decipher and privacy policies do not do much better. ZeShi Li et al. [32] state that more research is needed in educating software developers with regards to the GDPR. Lack of knowledge was also highlighted in the DPC's report, where websites were unaware of certain violations [22].

Nouwens et al. studied consent management platforms (CMPs) and found that dark patterns and implied consent were ubiquitous. From their survey they note that people ignore controls placed below the first layer in a banner [33]. Matte et al. [34] also look at CMPs by crawling 1426 websites to monitor Internet Advertising Bureau (IAB) Europe's Transparency and Consent Framework. They observe that 141 websites note positive consent before the user has interacted with the banner, 236 websites had pre-ticked options and 27 websites registered positive consent despite the user opting out. They detected at least one violation in 54% of their collected websites.

Papadogiannakis et al. [35] identify "a disparity between (i) what the users perceive about the collection of their data, and (ii) what some websites implement with respect to data processing". They observe that some websites collect and share data with third parties before the user has a chance to register a privacy choices. On some occasions, even if they do decline, data collection increased! They also point out issues with CMPs with regards to GDPR compliance.

III. Cookie Banner Collection Method

A. Full Crawl

Kampanos details the methodology for surveys in their paper. They use OpenWPM [36], a web privacy measurement framework, available as open source software, that scrapes websites for relevant information. It is designed to use automation features of the Mozilla Firefox browser to simulate website visits. OpenWPM can be scripted, allowing it to be easily tailored for specific research questions. Consequently, it has been used in many research studies. For example, Sorenson used OpenWPM to explore the cookie landscape before and after GDPRs activation [2]. To address the research questions relating to cookies, Kampanos made modifications to OpenWPM to identify cookie banners using a list of cascading style sheet (CSS) selectors and then to dump the banner both as HTML and a screenshot in PNG format. Unfortunately, Kampanos's modifications no longer apply cleanly to OpenWPM. Newer OpenWPM versions actually include a more flexible extension framework to make these sort of modifications less intrusive. Porting Kampanos's modifications to this new framework, allowed the use of current versions of OpenWPM and Firefox.

The steps for running the crawl are similar to those in Kampanos's original study. We provide the Tranco [9] list of top websites, and also a list of websites that aims to capture Irish websites outside the `.ie` domain. This list was manually created by amalgamating several lists of top Irish websites found via web search. Websites are included in the candidate list for crawling if they are on the Tranco list and either in the `.ie` domain or are on our list of Irish websites. Again, following Kampanos, we use the current *I don't care about cookies*[1] list of CSS selectors to identify banners, in combination with some additional selectors identified by Kampanos. The `robots.txt` file and terms of service are checked before each website is crawled.

The automated analysis was also extended to consider cookies set during the crawl, by inspecting the data recorded by OpenWPM. It counted the number of cookies set during the crawl of each site and checked if these cookies were third-party cookies. The identification of third-party cookies was achieved by comparing the site URL recorded by OpenWPM with the domain of the cookie stored.

B. Manually Inspected Subset

A manual inspection of a subset of our websites was also performed. Using Cochran's formula a sample size of 362 was calculated to provide a 90% confidence level with 4% margin of error. The 362 were randomly chosen using Excel from the list of websites identified as having banners. Then manual inspection was used to identify if different phrases might have been used in cookie banners, for example if they were in a different language. This allowed adjustment to the list of phrases that are searched for in the banners. The manual inspection was also used to address some other questions, for example regarding the design or placement of the cookie banner. In performing this manual subset check, a lot of false positive and a number of false negatives were noted. It was also noted that many CSS selectors on the *I don't care about*

[1] See https://www.i-dont-care-about-cookies.eu/.

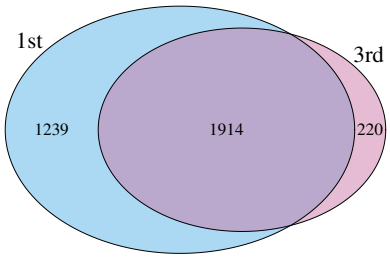

Fig. 1. Websites hosting First & Third-Party Cookies

Fig. 2. Cookie Banner Word Frequency

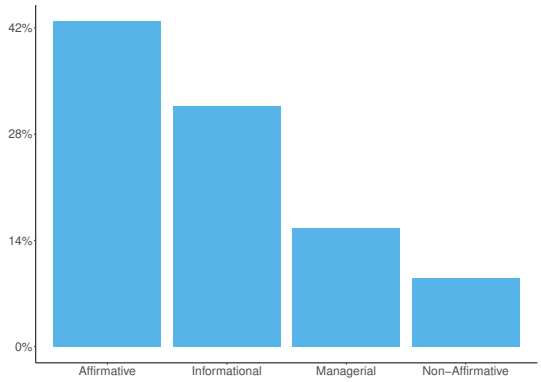

Fig. 3. Irish Banner Call to Actions

cookies that were intended to only be applied to websites in a specific domain were actually being applied to all websites by the system developed by Kampanos. The system was adjusted to ignore CSS selectors that were intended to be more specific. New CSS selectors were discovered and added to a list of extra CSS selectors used to identify banners and the main crawl was re-run.

IV. Results

The results of the overall crawl are first considered, followed by the results of the manually inspected subset. The results of the full crawl are based on our improved run that ignores the overly-specific CSS rules. Our manual results are based on the first crawl, but omitting false positive banners. We manually checked the results and we visually documented what the banners looked like and what details they contained.

A. Full Crawl

The total number of candidate websites was 4528. The framework tested the `robots.txt` for each of these websites and found 4003 suitable for crawling. The framework also checks for terms of service for each of the remaining websites to check if they are for personal use only. After this check, 3782 websites remain. The framework then crawls these websites and obtained results for 3735 of them.

To rule out false negatives, we manually check our list of websites where they are marked as not containing banners. From this list we find an extra 234 websites which do in fact display banners, so while the framework documents 1835 websites with banners, the total number is actually 2069.

A summary of the results for these 3735 websites are provided in Tab. I. During the crawl, a total of 58129 first-party cookies were set, an average of around 15.6 cookies per visit and a total of 22724 third-party cookies, with an average of 6 third-party cookies per visit. Third-party cookies appeared on 2134 of the websites and of all crawled websites approximately 10% had not set any cookies by the time the crawl of that site completed. Fig. 1 shows the overlap of websites with first/third party cookies.

We note the framework does not consent to any cookies being set and although 90% of Irish websites set cookies, only 55% were identified as displaying banners. However, compared to Kampanos's findings, we see a small improvement with regards to third-party cookies; with 57% hosting third-party cookies. Kampanos reports 48% of Greek websites containing banners with 61% of these hosting third-party cookies and 44% of British websites displaying banners with 70% of these containing third-party cookies. The website sample we collected is similar in size to the Greek sample.

Considering options presented by the banners, there are, on average, just under two options identified per banner. The framework classifies these options as affirmative, non-affirmative, managerial and informational, with affirmative and informational being the most common (see Fig 3). A small number of banners had no, or just one option. Interestingly, Kampanos documents no websites with reject only, we find one banner with a reject only option. A summary of the text found in each different type of option is shown in Tab. II.

Figure 2 shows a word cloud based on the text observed in banners. It contains words suggesting positive framing. Using NRCLex [37] we performed automated sentiment analysis of the words used in the banners. We found that overall the positive emotion was most prevalent (85%), followed by trust (71%), anticipation (43%) and lastly joy (28%). No negative emotion was registered in the text, which contrasted Kampanos's findings where they recorded 14% negative [21].

B. Manually Inspected Subset

In our manual inspected subset we noted 6 false positives and also 19 (5%) websites that contained HTML for banners but had no visible banner. Our total, therefore, is 337 visible

Websites visited	3735	Total options found	3542
Websites with cookies	3373	Average options per banner	1.93
Websites setting no cookies	362	Total affirmative options	1531
Websites setting only 3rd party cookies	220	Total non-affirmative options	322
Websites setting only 1st party cookies	1239	Total managerial options	557
Websites setting both 1st & 3rd party cookies	1914	Total informational options	1132
Automatically identified banners	1835	Average word count per banner	249.4
Manually identified banners	234	Banners with no options	124
Websites without banners	1666	Banners with only info option	158
Total third-party cookies set	22724	Banners with only accept option	210
Total first-party cookies set	58129	Banners with only reject option	1

TABLE I
SUMMARY OF CRAWL RESULTS

Accept	**%**	**Decline**	**%**	**Options**	**%**	**Info**	**%**
Accept	26	Reject all	48	Cookie settings	48	Cookie policy	22
Accept all cookies	16	Reject	27	Manage cookies	16	Privacy policy	15
Ok	10	Decline	13	More Options	11	Read more	13
Accept all	10	Disagree	5	Settings	10	Learn more	10
Allow all cookies	9	No	4	Manage	1	Cookie declaration	10
Got it!	5	Decline All	2	Cookie Preferences	0.4	More information	4
I accept	4	Revoke Cookies	0.6	Change Preferences	0.4	Cookie details	4
Allow All	4	Disable Cookies	0.6	Change Settings	0.2	More info	2

TABLE II
CALL TO ACTION, PERCENTAGES TAKEN FROM TOTAL IN EACH CATEGORY

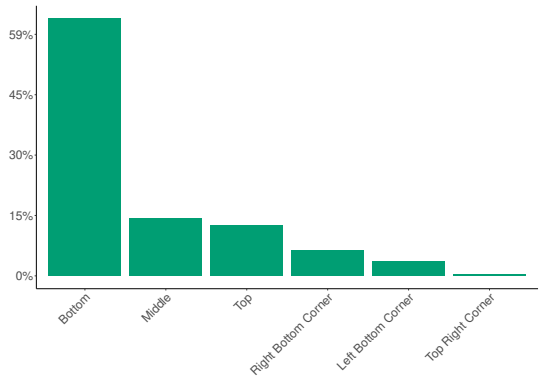

Fig. 4. Subset Banners Positions

Preticked	8%	CMP	25%
Direct Opt Out	19%	TP+CMP	14%
Preferences	53%	TP+Pre-ticked	4%
No Info	10%	CMP+Pre-ticked	1.7%
Accept Only	76%		

TABLE III
FEATURE SUMMARY OF MANUALLY INSPECTED SUBSET

banners and not the full sample of 362. Considering pages including visible or invisible banners ($n = 356$), the fraction of websites containing third-party cookies amounts to 55%.

There is a stark difference between the style of banners. On one end of the scale we have a barely visible sliver on the top or bottom of a page containing only an 'Accept' button. On the other end a large banner in the middle or side with all options and information visible and direct opt-out buttons. Only 19% of the banners were observed to have both an 'Accept' and 'Decline' option, with 76% of banners containing 'Accept' only. We found 8% of the banners had pre-ticked options (e.g. Fig. 5), 56% of the these contained third-party cookies. The majority of banners with pre-ticked options did not have a CMP logo attached. The websites which employed a CMP (25%), are divided among CookieBot, OneTrust, CookiePro and WordPress.org. Three websites redirected to a link explaining cookies 'cookiesandyou.com' and 'allaboutcookies.org'.

One benefit of working with a smaller subset, which has been used in the past [14], [22], [23], [31], is being able look at banners in detail. Fig. 4 displays the most common positions for banners on the page, the bottom of the website position being the clear winner. We also are able to identify cookie banners in the Irish language of which we found few. These were mostly associated with Irish language websites for example the Irish TV station TG4, Google also tends to translate cookie banners to English. We can also identify dark patterns and issues considered in the DPC's report. We noted several similarities. For example, a number of websites declare all cookies to be 'necessary' for the website to function, while not specifying what cookies are 'strictly necessary'. The DPC considered this a form of cookie bundling [22] and was also observed in [23]. Tab. III summarise some of these features.

Another practice, which was also noted in the DPC's report, were websites who assume that informing the user that they can change their privacy settings in-browser implies consent. Other observations noted were: (1) highlighted accept buttons, while in some cases decline buttons were almost opaque. (2) The colour green for accept buttons and red for decline,

Fig. 5. Similar banners style. Pre-ticked options (left) and with direct opt out (right)

which, apart from being a nudging technique (green being a colour synonymous with Go!), can also be problematic for colour blind users. (3) 63% of the websites recorded in the manual crawl had banners on the bottom. We did observe some banners were almost invisible at the bottom or top of the website. Many of these assumed consent by scrolling through the website, which is easier to do with a thin banner at the top or bottom of the page. It might be argued that these websites have discrete banners to avoid annoying their users while also complying with regulations. (4) Some websites included links for more information that did not work or redirected to the same page (also observed by the DPC). On one policy redirect, the banner popped up again in the middle and you could not scroll down to read the cookie information unless you clicked accept! One website's banner contained a 'more info' link which directed you to the cookies Wikipedia page. A few page's 'Learn More' button led to nothing, which might be a fault in the consent management platform (CMP) tool of which the website itself may not be aware of. The same fault applied to some banners, where on clicking 'preferences' results in nothing happening. (5) Other vague banners included an 'Accept' button along with 'Dismiss', which can be misleading, in that you may assume 'Dismiss' means 'Deny Cookies', when in fact you are dismissing the banner and accepting cookies.

One website with third-party cookies used a bottom banner which displayed "This site uses cookies. By continuing to browse the site, you are agreeing to our use of cookies' with a highlighted 'ok' button and a 'learn more' button". When the 'learn more' button is clicked, you are directed to the banner shown in Fig. 6(l). It is not clear whether the buttons are already ticked; the colouring suggests that they are. However, more commonly pre-ticked buttons will have the coloured part to the left which suggests it has already been ticked, the line beside the button says 'click to enable/disable' suggesting then, that these buttons are in the 'enable' position.

Two CMP banners, which were a second level preference list, contained just the option to enable or disable 'strictly necessary' cookies with no other options. This website included third-party cookies, and it was not clear they were all necessary. Another website, also containing third-party cookies, had no cookie banner. This was slightly ironic given it was a cybersecurity and data protection website!

Some banner policies mention that other websites have access to their information via third-party cookies but they do not have responsibility over what that website does and thus the onus is on the user to investigate where their own

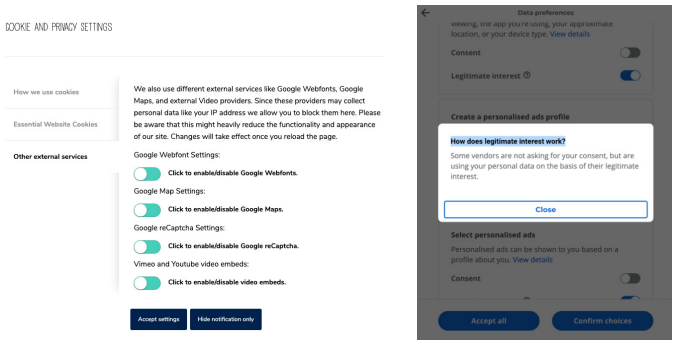

Fig. 6. Banner with vague instructions and pre-ticked buttons (left) and 'Legitimate Interests' banner (right)

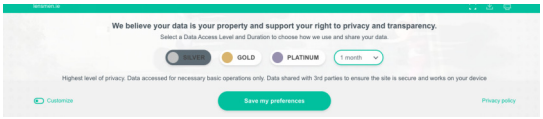

Fig. 7. Data Choices Represented By Precious Metals

data is going. Another banner's preference list consisted of consent buttons for certain data collation. Beneath this there was a pre-ticked 'legitimate interests' button. When you click on 'more information' relating to 'legitimate interest' it states: "How does legitimate interest work? Some vendors are not asking for your consent, but are using your personal data on the basis of their legitimate interest." This does not explain what constitutes as their 'legitimate interests', (e.g. Fig. 6(r)).

One interesting example of a dark pattern noted was data choices represented by silver, gold and platinum (see Fig. 7), where platinum is, as they say, the "Highest level of personalisation. Data accessed to make ads and media more relevant. Data shared with 3rd parties may be use to track you on this site and other sites you visit". This is the only example we have seen that represents the choice in this way. It is likely that people will associate platinum to be the best choice.

V. Discussion

The aim of this study was to get an overall view of what cookie banners in Ireland look like in terms of their prevalence, format and how they compare to similar studies in other European countries. We also wanted to note any dark patterns.

A. Full Crawl

At a high level, there is similarity between the Irish, Greek and English cookie landscape. One difference is that the proportion of websites in Ireland containing third-party cookies

without banners is smaller than UK or Greece. While one reason for this may be better compliance in Ireland, it might also be explained by a more effective list of CSS selectors used to identify banners or improved compliance over time, possibly motivated by fines issued for non-compliance.

Strong positive sentiments were recorded in banner language where it is often presented as being in your best interest to accept cookies. This could be interpreted as a variation on *confirm shaming*[2]. For many websites, advertising is a source of income and allowing people to easily opt out of cookies could reduce their earning power [39]. Consequently, enticing people to choose cookies using positive language is one way to seek financial advantage.

In some cases, choice of cookies appears to be an illusion, particularly for banners which declare they use cookies and only display an 'OK' button. If there are any cookies that are not strictly necessary then there should be a choice or information on how to opt out. While some websites may be technically compiling with GDPR, this type of behaviour seems to be prevalent. It may fall under the heading of dark patterns, which are hard to outlaw.

B. Manually Inspected Subset

We found that opting out of cookies is quite difficult, as noted in other studies [21]. Many websites involve going to at least a second level in order to opt out of cookies or expect you to change your cookie settings in your browser. It has been observed that "placing controls or information below the first layer renders it effectively ignored" [33].

Similar dark patterns emerge in Irish banners as are observed in studies on German banners [14], and other classifications of dark patterns also make it apparent that dark patterns are in use in Irish banners [30]. When it comes to dark patterns and cookie banners it has been observed that there is a "lack of identification of the ways in which particular dark patterns might be connected to legal requirements and the user experience" [40]. Whether banners are intentionally designed to influence users into allowing their data to be easily collected or if it is down to lack of understanding on the part of website creators, is not easy to identify.

Strong similarities to the DPC study were also observed, although the DPC's study was performed on a small hand-picked group of 38 websites. The DPC report highlights examples of bad cookie banners, most notably the thin banner stating "This website uses cookies to ensure you get the best experience on our website. (Learn more) . . . Got it!". This also appeared to be the most common banner in our manual sweep.

Note that the percentage of pre-ticked options dropped significantly compared to the DPC's findings of 26%. This could be explained by the fact that in 2019 the Court of Justice of the European Union delivered a judgment in the Planet49 case, stating that pre-ticked options do not constitute valid consent under the e-Privacy Directive [41]. The DPC acknowledges that their study was conducted before this judgement.

The DPC's report noted that some websites were not aware of their breaches when using an external CMP. As regulations can differ between countries, these banners may be legal in some countries but not others. We observed that the majority of banners with pre-ticked options did not have a CMP logo attached. This suggests that the recent clarifications regarding pre-ticked cookies are being followed, particularly by CMPs.

Another feature, which was also noted in the DPC's report, was the presence of websites who assume informing the user that they can change their privacy settings in-browser implies consent. This may arise because regulations may appear vague, especially regulation 5(4) of the ePrivacy regulations:

> Where it is technically possible and effective, having regard to the relevant provisions of the Data Protection Acts, the user's consent to the storing of information or to gaining access to information already stored may be given by the use of appropriate browser settings or other technological application by means of which the user can be considered to have given his or her consent.

Without a legal background, one might assume that this means you can gain consent by notifying the user that they can change their settings. However, this has been clarified as not an exception to regulation 5(3), which states a person cannot store information unless the user has given clear consent.

Finally, we noted some invisible banners. This is not something that we have seen discussed in previous studies. Without manual inspection, it is difficult to know if a banner is actually displayed, and some often only appear once you scroll down to the bottom of the page. This leads to the question of websites functioning as intended, regardless of whether cookies have been accepted or not. Some website's cookie banners, while not invisible, are so discrete you really have to search for them. These banners may have a decline button, but a person can peruse the website without noticing it.

VI. Conclusion

In this paper, we undertook to survey the use of cookie banners on Irish websites. We used an automated mechanism, similar to Kampanos [21], and also inspected a subset of banners manually. Comparatively, our automated results are broadly similar to Kampanos study with an improvement in terms of websites hosting third-party cookies and displaying banners. Our manual inspection of banners identified the use of a number of common dark patterns identified with some banners displaying confusing and misleading language and instructions. One new contribution of this study is the presence of invisible banners, where it appears that there is code for a banner in the HTML but is not visible on the website.

In addition to our findings via the adjusted OpenWPM framework we suggest banner detection could be improved by more careful interpretation of specific CSS selectors. We would also suggest regular crawls over multiple countries to monitor changes over time and location.

[2]The act of making the user feel guilty to have them agree into opting into something. The option to decline is worded in such a way as to shame the user into compliance. [38]

ACKNOWLEDGEMENTS

This publication has emanated from research supported in part by Science Foundation Ireland under Grant number 18/CRT/6222.

REFERENCES

[1] O. Ray, "Tracking cookies are dead: What marketers can do about it," https://www.invoca.com/blog/tracking-cookies-are-dead-what-marketers-can-do-about-it Accessed: 01-09-2021.

[2] J. Sørensen and S. Kosta, "Before and after GDPR: The changes in third party presence at public and private european websites," in *The World Wide Web Conference*, 2019, pp. 1590–1600.

[3] S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in *2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 1388–1401.

[4] R. Koch, "Cookies, the GDPR, and the eprivacy directive," https://gdpr.eu/cookies/ Accessed: 29-10-2021.

[5] O. Kulyk, A. Hilt, N. Gerber, and M. Volkamer, ""This website uses cookies": Users' perceptions and reactions to the cookie disclaimer," in *European Workshop on Usable Security (EuroUSEC)*, 2018.

[6] L. Narayanan, "Cookies'n'consent: An empirical study on the factors influencing customer attitudes towards cookie consent among Internet users in EU." Ph.D. dissertation, Dublin Business School, 2020.

[7] C. Pope, "400 yes, 400! Irish retailers for all your online christmas shopping," https://www.irishtimes.com/news/consumer/400-yes-400-irish-retailer-for-all-your-online-christmas-shopping, Accessed 27-8-2021.

[8] B. Power, "Shop local from food to fashion to fitness: County by county guide to the best Irish websites for supporting local businesses this Christmas," https://www.independent.ie/irish-news/from-food-to-fashion-to-fitness-county-by-county-guide-to-the-best-irish-websites-for-supporting-local-businesses-this-christmas, Accessed: 27-8-2021.

[9] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, "Tranco: A research-oriented top sites ranking hardened against manipulation," in *26th Annual Network and Distributed System Security Symposium*, ser. NDSS 2019, Feb. 2019.

[10] Online official information on GDPR, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec," https://eur-lex.europa.eu/ Accessed: 31-08-2021.

[11] The Data Protection Commission, "Safeguarding data protection rights by driving compliance through guidance, supervision and enforcement," https://www.dataprotection.ie Accessed: 29-08-2021.

[12] M. Burgess, "Why Amazon's £636m GDPR fine really matters," https://www.wired.co.uk/article/amazon-gdpr-fine Accessed: 23-09-2021.

[13] Tessian, "20 biggest GDPR fines of 2019, 2020, and 2021 (so far)," https://www.tessian.com/blog/biggest-gdpr-fines-2020/ Accessed: 23-09-2021.

[14] C. Krisam, H. Dietmann, M. Volkamer, and O. Kulyk, "Dark patterns in the wild: Review of cookie disclaimer designs on top 500 german websites," in *European Workshop on Usable Security (EuroUSEC)*, 2021.

[15] G. Chrome, "Building a more private, open web," https://privacysandbox.com/ Accessed: 15-12-2021.

[16] D. Geradin, D. Katsifis, and T. Karanikioti, "Google as a de facto privacy regulator: analysing the privacy sandbox from an antitrust perspective," *European Competition Journal*, pp. 1–65, 2021.

[17] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas, "Adnostic: Privacy preserving targeted advertising," in *Network and Distributed System Symposium*, 2010.

[18] S. Guha, B. Cheng, and P. Francis, "Privad: Practical privacy in online advertising," in *USENIX conference on Networked systems design and implementation*, 2011, pp. 169–182.

[19] M. Fredrikson and B. Livshits, "Repriv: Re-imagining content personalization and in-browser privacy," in *2011 IEEE Symposium on Security and Privacy*. IEEE, 2011, pp. 131–146.

[20] C. Santos, N. Bielova, and C. 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.

[21] G. Kampanos and S. Shahandashti, "Accept all: The landscape of cookie banners in Greece and the UK," 2021.

[22] Data Protection Commission, "Report by the Data Protection Commission on the use of cookies and other tracking technologies," https://www.dataprotection.ie/en/news-media/press-releases/report-dpc-use-cookies-and-other-tracking-technologies Accessed: 18-10-2021.

[23] C. Santos, A. R, L. S. Chamorro, K. Bongard-Blanchy, and R. Abu-Salma, "Cookie banners, what's the purpose? Analyzing cookie banner text through a legal lens," *arXiv preprint arXiv:2110.02597*, 2021.

[24] M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz, "We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy," *arXiv preprint arXiv:1808.05096*, 2018.

[25] I. Fouad, C. Santos, F. Al Kassar, N. Bielova, and S. Calzavara, "On compliance of cookie purposes with the purpose specification principle," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 326–333.

[26] J. Bauer, R. Bergstrøm, and R. Foss-Madsen, "Are you sure, you want a cookie? — The effects of choice architecture on users' decisions about sharing private online data," *Computers in Human Behavior*, vol. 120, p. 106729, 2021.

[27] D. Machuletz and R. Böhme, "Multiple purposes, multiple problems: A user study of consent dialogs after GDPR," *arXiv preprint arXiv:1908.10048*, 2019.

[28] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(un) informed consent: Studying GDPR consent notices in the field," in *2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 973–990.

[29] C. Bermejo Fernandez, D. Chatzopoulos, D. Papadopoulos, and P. Hui, "This website uses nudging: Mturk workers' behaviour on cookie consent notices," *ACM on Human-Computer Interaction*, vol. 5, no. CSCW2, pp. 1–22, 2021.

[30] P. Graßl, H. Schraffenberger, F. Zuiderveen Borgesius, and M. Buijzen, "Dark and bright patterns in cookie consent requests," *Journal of Digital Social Research*, vol. 3, no. 1, 2021.

[31] H. Habib, Y. Zou, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, L. Cranor, N. Sadeh, and F. Schaub, "An empirical analysis of data deletion and opt-out choices on 150 websites," in *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019, pp. 387–406.

[32] Z. Li, C. Werner, N. Ernst, and D. Damian, "GDPR compliance in the context of continuous integration," *arXiv preprint arXiv:2002.06830*, 2020.

[33] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence," in *2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[34] C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 791–809.

[35] E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, and E. Markatos, "User tracking in the post-cookie era: How websites bypass GDPR consent to track users," in *Web Conference 2021*, 2021, pp. 2130–2141.

[36] S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in *ACM CCS 2016*, 2016.

[37] M. Bailey, "NRCLex (2019)," https://github.com/metalcorebear/NRCLex Accessed: 03-11-2021.

[38] B. Morrison, C. Sengul, M. Springett, J. Taylor, and K. Renaud, "Mental models of dark patterns," https://spritehub.org/2021/12/08/revealing-young-learners-mental-models-project-team-publish-white-paper Accessed: 9-12-2021.

[39] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P.-A. Vervier, and I. Santos, "Can I opt out yet? GDPR and the global illusion of cookie control," in *ACM Asia Conference on Computer and Communications Security*, 2019, pp. 340–351.

[40] C. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, "Dark patterns and the legal requirements of consent banners: an interaction criticism perspective," in *2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–18.

[41] Court of Justice of the European Union, "Panet49 case ruling," https://curia.europa.eu/juris/document Accessed: 18-10-2021.