



Consent banners, dark patterns, and GDPR infringements in online gambling: Evidence from a systematic audit and online experiment

Jack McGarrigle^a, Jamie Torrance^a, Martyn Quigley^a, Simon Dymond^{a,b,*}

^a GREAT Centre, School of Psychology, Swansea University, United Kingdom

^b Department of Psychology, Reykjavik University, Iceland

ARTICLE INFO

Keywords:

Online gambling
Dark patterns
Consent banners
Data protection

ABSTRACT

Online gambling operators collect vast amounts of consumer data to track behaviour and personalise inducements. Under the General Data Protection Regulation (GDPR), access to these data requires user consent, obtained via pop-up consent banners. However, such banners tend to exhibit “dark patterns” or designs which nudge users towards accepting data sharing. To date, little is known about the extent of such dark patterns in online gambling. Here, we investigated the format of consent banners used on UK gambling websites and assessed how they may influence behaviour. Study 1 reports an audit of all UK-licensed gambling sites ($n = 624$). We found that 86% of banners exhibited at least one dark pattern, while GDPR infringements were also identified: 24% of sites offered no option to reject tracking and over two-thirds (67%) processed personally identifiable data prior to obtaining consent. Only 1 in 7 or 14% of sites were GDPR compliant. In Study 2, an online randomised experiment was conducted, whereby participants ($n = 615$) were assigned to different consent banners within a simulated gambling platform. The most common banner identified in Study 1 significantly increased acceptance of tracking and produced significantly lower alignment between user choices and preferences. No association between banner decisions and self-reported gambling harm severity was detected. Overall, our findings reveal widespread dark patterns and non-compliance of GDPR requirements on UK online gambling sites, influencing users towards unintended data sharing. These findings highlight the need for stronger regulatory enforcement and stricter consent banner design standards to protect consumers.

1. Introduction

The modern digital ecosystem is driven in large part through surveillance capitalism, characterised by targeted and personalised advertising based on user behavioural and demographic data (Zuboff, 2023). Within this ecosystem, the UK gambling industry is estimated to spend between £1.1 to £2 billion per annum on advertising, with over two-thirds of this advertising being conducted online (Alvarez & Marsal, 2025; WARC, 2025). Gambling marketing content is personalised and targeted based on user behaviours, with the goal of increasing consumption and losses (Guillou-Landreat et al., 2021; Newall et al., 2019; Torrance et al., 2021), and individuals with higher levels of gambling severity report receiving more personalised marketing messages (Syvertsen et al., 2022). Given that online gambling is associated with significant risks of consumer harm (Gainsbury, 2015; Tran et al., 2024), and that a disproportionate share of industry profit is derived from individuals who regularly experience gambling harms (Fiedler et al., 2019), several regulatory and consumer advisory bodies have

therefore identified online gambling as an area of intensified risk of consumer harm caused by targeted marketing (Centre for Data Ethics and Innovation, 2020; FTC, 2025; Information Commissioner's Office (ICO) & Competition and Markets Authority (CMA), 2023).

Industry use of consumer data is proprietary and largely outside public scrutiny, and yet the scale and granularity of behavioural data held by industry operators enables practices which may leave vulnerable consumers at risk of harm due to increased consumption and expenditure (Hing et al., 2025). Given the unique characteristics of the gambling industry, in that operator gain is structurally tied to consumer loss, operator access to and use of consumer data raises several important questions surrounding the protection of vulnerable consumers. Namely; how operators access and process consumer data, whether any distinction is made between targeting “profitable” user behavioural patterns and harmful gambling behaviours, and the degree to which at-risk consumers are protected from these practices. The present study aims to take a first step in research in this area by exploring the first key question: how do gambling operators access and process consumer data?

* Corresponding author. Swansea University, Singleton Campus, Swansea, SA28PP, United Kingdom.

E-mail address: s.o.dymond@swansea.ac.uk (S. Dymond).

<https://doi.org/10.1016/j.chbr.2026.101270>

Received 17 March 2026; Received in revised form 3 August 2026; Accepted 18 August 2026

Available online 20 August 2026

2451-9588/© 2026 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

Gambling operator interest in consumer data is not a new phenomenon. The introduction of loyalty cards in the 1980s, inserted by players into casino slot machines, transformed physical gambling machines from analogue terminals into “electronic surveillance devices”, recording what, when, and how users played (Schüll, 2012, p. 145). These data enabled casinos to segment their player base and develop personalised marketing strategies to the level of the individual user. In the internet age, both the scope and granularity of consumer data have expanded significantly. Loyalty cards are no longer necessary, with users’ every action and reaction tracked within the platform itself. An investigation into digital profiling in the online gambling industry revealed that limited engagement with gambling platforms led to over 2000 data transmissions to 40 third-parties, with an operator logging 186 different attributes on a single customer, including a “win-back” value of £1,190, equating to the estimated amount of money the customer would lose if they returned to the platform (Christl, 2022). The platform in question was subsequently reprimanded by the ICO for unlawfully processing data without user consent (ICO, 2024). Online gambling operators have also been shown to track users even when consent is withheld, in breach of data privacy regulations (Guardian, 2025). In addition, in *RTM vs Bonne Terre Limited* (2025), it was determined that an operator used consumer data to systematically target an individual experiencing gambling harms. A representative from the operator in question acknowledged that for this individual, gambling during early morning hours was treated both as a signal of harm as well as a cue to deliver personalised inducements at those times. This conflict of incentives reflects the business model of gambling operators, for whom an individual experiencing gambling harms is a likely profitable consumer, whose behaviour can be analysed and targeted to amplify their consumption.

Consumer data can also be used to track users across the web, even when they are not directly engaging with the platform itself. This is enabled through the use of tracking cookies – small files stored on a device containing a unique user identifier, linking activity across different sites (ICO, 2025). When these identifiers are in place, users can be tracked from one platform to the wider web and vice-versa, meaning that users who have shown an interest in gambling can be targeted with personalised gambling advertising on third-party sites (e.g., social media). Online gambling operators can also gather data from these third-party sites, such as browsing habits, search histories and demographics to further enhance targeting, creating a circular environment in which users can experience difficulty in disengaging from gambling (Englehardt & Narayanan, 2016).

There is scarce public, peer-reviewed information surrounding exactly how consumer data are used by online gambling operators. However, insight can be gleaned from industry publications, such as promotional materials from iGaming adtech providers, who advertise their services of personalising inducements by leveraging user data. One such provider outlines so-called “best practices”: “a good time to encourage players to place additional bets is right after they experience a big win, while they are still feeling euphoric” (Optimove, 2020, p. 1). Also described are strategies for using data to explicitly “discourage withdrawals”: “triggered by a withdrawal being initiated, offer different promotions to each player. Players who have had no previous withdrawals in the last three months ... should receive heavier promotions” (Optimove, 2020, p. 1). Behavioural triggers to sustain play are also promoted: “if a player spends over a certain amount or logs in at specific times, you can send real-time pop-ups or notifications that encourage just the right action — maybe that extra push towards depositing more funds.” (Scaleo, 2024, p.1). Another provider describes delivering personalised inducements aimed at “prevent[ing] valuable players from leaving, approaching them with individualised bonuses”, reflecting a digital parallel to the practices described by Schüll (2012) in physical casinos: “is a player looking likely to leave? You’ll get a recommendation to send them an offer” (Sportradar, 2025, p. 1). It is pertinent to note that valuable players in this context refers to those with heavy losses on

the platform. It is unclear how or if these providers can discern “valuable” customers from those suffering from gambling harms, and what mechanisms are in place to ensure vulnerable consumers are not targeted with these practices.

Crucially, under EU and UK General Data Protection Regulation (GDPR), websites are legally required to obtain “freely given, informed, and unambiguous” consent from users before collecting any personally identifiable data not essential for security or operation of the site (GDPR, 2016 p.33). In practical terms, this means that without explicit user consent, sites cannot track user behaviour for marketing purposes, build user profiles, or share personal data with third-party vendors for profiling or advertising. Consent is gathered via consent banner pop-ups, however the choice architecture of these banners often obfuscate user choice through dark patterns (user interface designs which influence behaviour to the benefit of the platform designer; Gray et al., 2023, pp. 188–193), nudging users towards accepting tracking (Graßl et al., 2025; Matte et al., 2020; Norwegian Consumer Council, 2018; Nouwens et al., 2020; Papenmeier et al., 2025; Soe et al., 2020, pp. 1–12; Utz et al., 2019, pp. 973–990). Studies have also shown evidence of websites unlawfully processing user data prior to obtaining consent, or even after consent is explicitly denied (Papadogiannakis et al., 2021; Sanchez-Rola et al., 2019, pp. 340–351).

In online gambling, the design of consent interfaces in online gambling carries heightened significance relative to other sectors, as this data collection directly enables the potential targeting of vulnerable consumers. To date, no large-scale audit has been conducted on consent banner designs or data processing by online gambling operators, though this is an industry in which consumers are at particular risk of harm from these practices (ICO & CMA, 2023). Moreover, by combining a large-scale systematic audit with a randomised experimental design, the present study provides an empirical account of gambling operator data practices and evidence of their behavioural consequences. Beyond documenting prevalence, this study contributes to theoretical understanding of how digital choice architecture can systematically undermine consumer autonomy in high-risk commercial environments, with broader implications for the design of consent interfaces across the digital economy. In doing so, we aim to address the pressing need to assess the design of consent banners on online gambling sites, the behaviour of users in their interactions with these banners, and the extent to which data privacy regulations are adhered to.

2. Study aims

It is important to distinguish between three related but conceptually distinct issues examined in the present study. First, unlawful GDPR practices refer to demonstrable legal violations, such as consent banner designs which are non-compliant with data privacy law. Second, dark patterns refer to interface designs which manipulate user behaviour towards privacy-unfriendly choices, which may or may not constitute legal violations but are deceptive by design. Third, broader ethical concerns surrounding behavioural targeting in gambling extend beyond the scope of data protection law and raise wider questions about consumer protection and public health.

In the online gambling industry, where consumer and operator incentives are fundamentally misaligned, and where user data is a highly valued asset, an examination of data privacy practices is required to ensure that consumer rights are upheld. Loyalty programmes, cross-site tracking, and personalised inducements fine-tuned to each user’s gambling patterns may create an environment whereby vulnerable consumers are targeted and incentivised to continue gambling. Despite an abundance of evidence of dark patterns in data privacy practices in wider online spaces, little is known about how such practices manifest on online gambling platforms, or how they influence consumer behaviour in these environments. The present study aims to address this gap by examining both the design of consent banners on UK-licensed gambling platforms, and the behavioural responses of users in their

interaction with them. Given the personal and public health risks posed by personalised marketing strategies, this research will provide important evidence for policymakers with regard to data privacy practices in the online gambling industry.

The aims of the present study were.

- To systematically audit the design of consent banners on UK-licensed gambling platforms, and to identify the presence of dark patterns in these designs.
- To identify the degree to which user data is processed prior to consent.
- To determine the influence of consent banner designs on user behaviour in online gambling environments.
- To determine whether there is an association between self-reported gambling harm severity and susceptibility to dark patterns in consent banner designs.

3. Study 1

3.1. Methodology

We conducted a manual systematic analysis of cookie consent banners and network traffic on all casino and sports betting websites licensed by the UK Gambling Commission, conducted between April and June 2025. A comprehensive list of licensees was obtained from the Gambling Commission website ($n = 934$). We excluded lottery operators, bingo sites, inactive websites, miscellaneous non-gambling services, and duplicates, resulting in $n = 624$ websites included in the analysis. The study was pre-registered, and the full dataset and screenshots of analysed websites are available at <https://osf.io/p2reh/files>. All sites were visited using Google Chrome (version 126) in incognito mode, with no browser extensions enabled, no VPN active, and default browser security and privacy settings, on a MacBook Air running macOS Sequoia. Sites were accessed from a UK IP address to ensure consistent geolocation-based banner presentation. For each site, we collected raw data including a screenshot of the landing page with the cookie consent notice, and, where relevant, screenshots of network traffic on page load, prior to any interaction with the consent banner. Network traffic was captured using the Chrome DevTools Network panel, which records all outbound HTTP requests made by the browser on page load. For each site, the network log was inspected prior to any interaction with the consent banner, and requests were examined for the presence of persistent unique user identifiers transmitted to known third-party data analytics endpoints. A request was classified as constituting pre-consent data processing where it contained a persistent unique identifier and was directed to a non-essential third-party service (e.g. Google Analytics, Meta Pixel, advertising networks) prior to any user interaction.

Each consent banner was evaluated using a structured coding framework. The following variables were extracted: whether personal data was collected prior to user consent; the design type of the banner (accept/settings, binary, category, or no option); the number of clicks required to reject cookies; the presence and type of dark patterns implemented in banner designs; overall compliance with GDPR. Banner design types were operationalised according to Utz et al. (2019, pp. 973–990), with accept/settings banners requiring multiple clicks to reject; binary banners offering equal accept and reject options; category banners allowing one-click accept, reject, or granular management; and no option banners providing no means to reject data processing. Dark pattern categories were operationalised following Gray et al. (2023, pp. 188–193) and Nouwens et al. (2020), encompassing visual emphasis of the least privacy-friendly option, pre-selection of privacy-unfriendly settings, and the concealment of the reject option behind a secondary layer. Coding was conducted by the lead author using these frameworks. Ambiguous cases were resolved through discussion with co-authors.

3.2. Results

3.2.1. Processing of personal data prior to consent

Our analysis found that 67% of online gambling sites (418 of 624) processed personally identifiable data prior to obtaining user consent. This was evidenced by the presence of persistent unique user identifiers in outbound network requests sent to third-party analytics and marketing platforms immediately upon page load, before any user interaction with the consent banner (Fig. 1). Many of these requests corresponded to Google Analytics 4 (GA4) tracking endpoints. Google Analytics is a web analytics service that tracks user behaviour, recording data such as page views, session duration, click events and interactions, and device and browser information to provide operators with insights into how users interact with their platform (Google, 2025). GA4 identifiers are uniquely assigned to each user and persist across sessions, making it possible to track individuals over time and across websites, used for marketing analytics and behavioural profiling. GDPR, (2016 Arts. 6(1), 7) stipulates that any collection or processing of such data requires a valid legal basis in the form of freely given, specific, informed, and unambiguous consent, unless the processing is strictly necessary for providing a service explicitly requested by the user (e.g. security or fraud prevention). As analytics and marketing tracking are not essential for the functionality of gambling websites, we treat the deployment of scripts of this kind prior to consent as constituting unlawful processing. On this basis, we interpret the observed transmissions as violations of GDPR.

3.2.2. Consent banner designs

We found a variety of consent banners used across the sample, which we categorised into four main types in line with Utz et al. (2019, pp. 973–990): Accept/Settings, Binary, Category, and No Option (Fig. 2). 2% of sites had no consent banner at all, in breach of GDPR, and 22% of sites employed a no option banner, which merely inform users that their data is being collected, also in breach of GDPR. Only category and binary banners allow rejection of cookies in one-click, while accept/settings banners require users to go through multiple layers to reject.

Accept/settings. An accept/settings banner was employed by 47% of sites. These banners offer two options on the first layer: accept all cookies, and a second option typically called “settings”, “manage cookies”, or “more information”. While tracking can be accepted in one click, rejecting involves navigating through multiple layers, taking up to 15 clicks on some sites. In addition, the accept option is almost always (99%) visually emphasised. In one example (Fig. 2, Banner 2), the “manage cookies” option was almost invisible due to poor contrast, a clear example of obfuscation of the privacy-friendly option.

Binary. A binary banner was employed by 5% of sites, in which two options are available: accept or reject. These banners are more user-friendly as it is as easy to reject as to accept, however in almost half (48%) of sites, the banner visually emphasised the accept option, nudging users towards privacy-unfriendly options.

Category. Category banners were employed by 24% of sites. These banners are perhaps the most user-friendly, as they allow the user to accept, reject, or manage their cookies in one click. However, we again found a significant proportion (44%) of sites exhibiting dark patterns, in which the reject and settings buttons were smaller, shaded in lower contrast, and more difficult to find than the accept button.

No Option. No Option banners were employed by 22% of sites. These banners simply inform users that their personal data is being collected and offers users no ability to exercise their data privacy rights, in breach of GDPR.

No banner. On 2% of sites, there were no consent banners at all, offering users no choice to select their data privacy preferences, in breach of GDPR.

3.2.3. Dark patterns

Of the 624 sites in our sample, 538 (86%) exhibited at least one dark

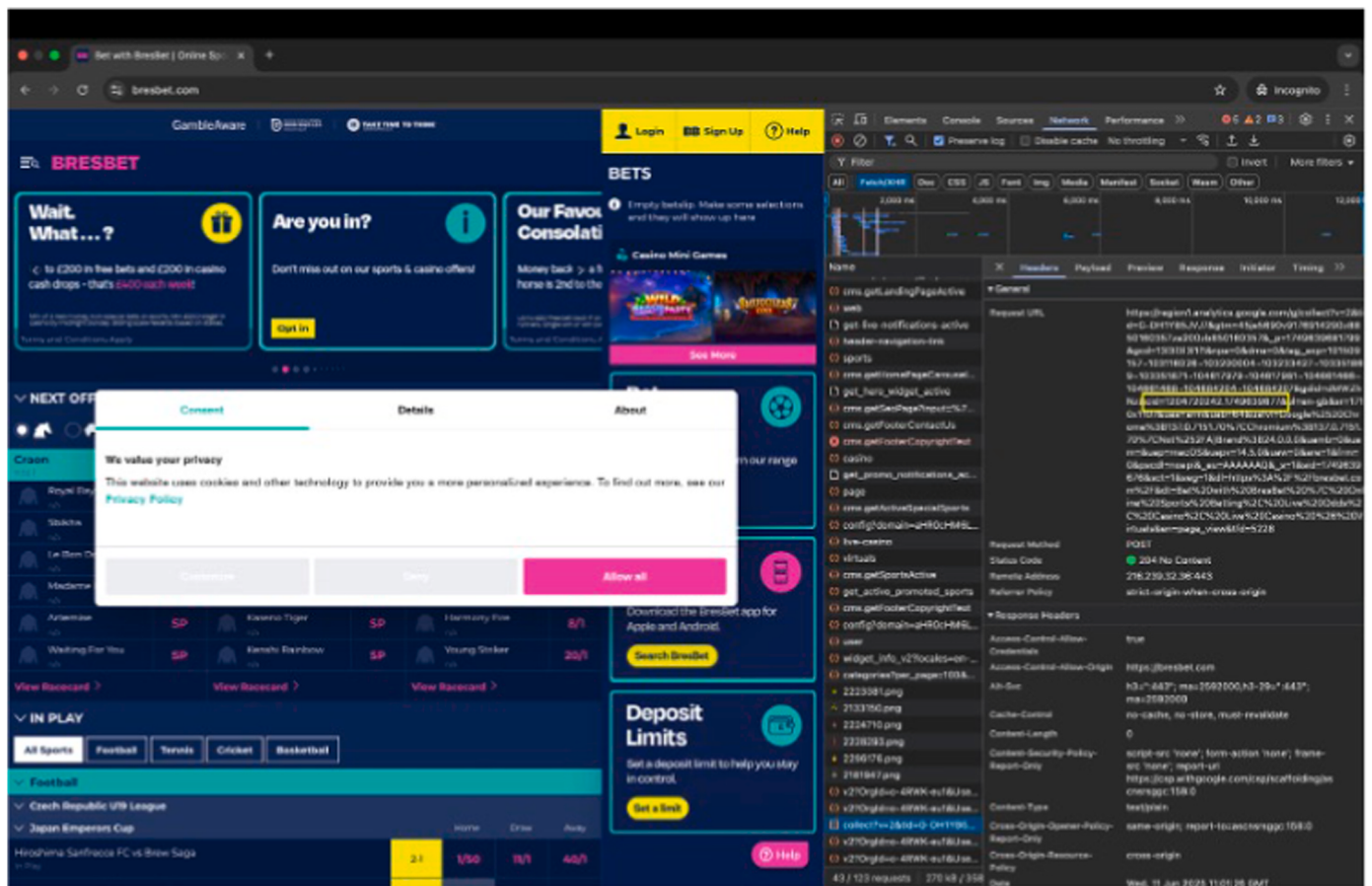


Fig. 1. Example of a site processing personally identifiable data prior to interaction with the consent banner.

pattern in their banner design, varying between visual emphasis of the least privacy-friendly option (60%), pre selection of privacy-unfriendly settings (29%), and the reject option being hidden behind a second layer (47%). 22% of sites did not give the user any option to reject, while 2% of sites did not have a consent banner at all (Table 1, Fig. 2C). Cross-tabulation of dark pattern types by banner design revealed striking differences across banner types (Table 2). Accept/settings banners exhibited the highest prevalence of all three dark pattern types, requiring a mean of 3.38 clicks to reject ($SD = 1.94$, range 2–15), compared to exactly one click for both binary and category banners.

3.2.4. Clicks to reject

Only 29% of banners allowed users to reject tracking as easily as they could accept it (i.e. within one click; Fig. 2D). In some cases, it took 15 clicks to reject tracking, creating a substantial barrier for users wishing to exercise their privacy preferences. 24% of banners offered no ability to reject tracking at all, in breach of GDPR.

3.2.5. GDPR compliance

Matte et al. (2020) identified four key legal violations of GDPR principles based on the Interactive Advertising Bureau's (IAB) Transparency & Consent Framework (TCF): storing consent before a choice is made, absence of an opt-out option for tracking, use of pre-selected consent choices, and failure to respect user preferences once expressed, finding that 54% of sites in their sample violated at least one of these principles. Applying the same criteria to our sample, we found that 86% (536/624) of sites violated at least one of these principles, leaving only 14% of sites in compliance with GDPR. This assessment reflects a research-based evaluation rather than a formal legal

determination, which would ultimately depend on jurisdictional enforcement and judicial interpretation.

4. Study 1: discussion

Our audit reveals widespread deceptive choice architecture in consent banner designs, and systemic non-compliance of data protection law across UK-licensed online gambling sites. Over two-thirds of sites were found to process personal data prior to obtaining user consent, in direct breach of GDPR. In addition, consent banners are often designed deceptively, and in many cases unlawfully, across our sample. 22% of sites employ consent banners which merely inform users that their data is being collected and processed, not allowing for any user choice regarding their data privacy preferences. When choice is offered, it is often obfuscated by a variety of dark patterns designed to influence users towards the least privacy friendly options. 86% of consent banner designs hide or make less prominent options to reject tracking, while almost half (47%) require users to click beyond the first layer to find the reject option, with accept always being available within one click. It took up to 15 clicks to reject cookies on some sites, reflecting designs which frustrate the user into accepting, rather than gathering their freely stated preferences, as intended by GDPR. In total, only 1 in 7 (14%) sites were fully compliant with GDPR. Given the role of personal data in enabling targeted marketing, these findings raise questions about the degree to which vulnerable users are protected from algorithms whose outputs may serve commercial rather than consumer interests. Many of the practices described undermine the GDPR principles of user autonomy and informed control over personal data, and necessitate strong regulatory action to ensure data protection regulations are upheld.

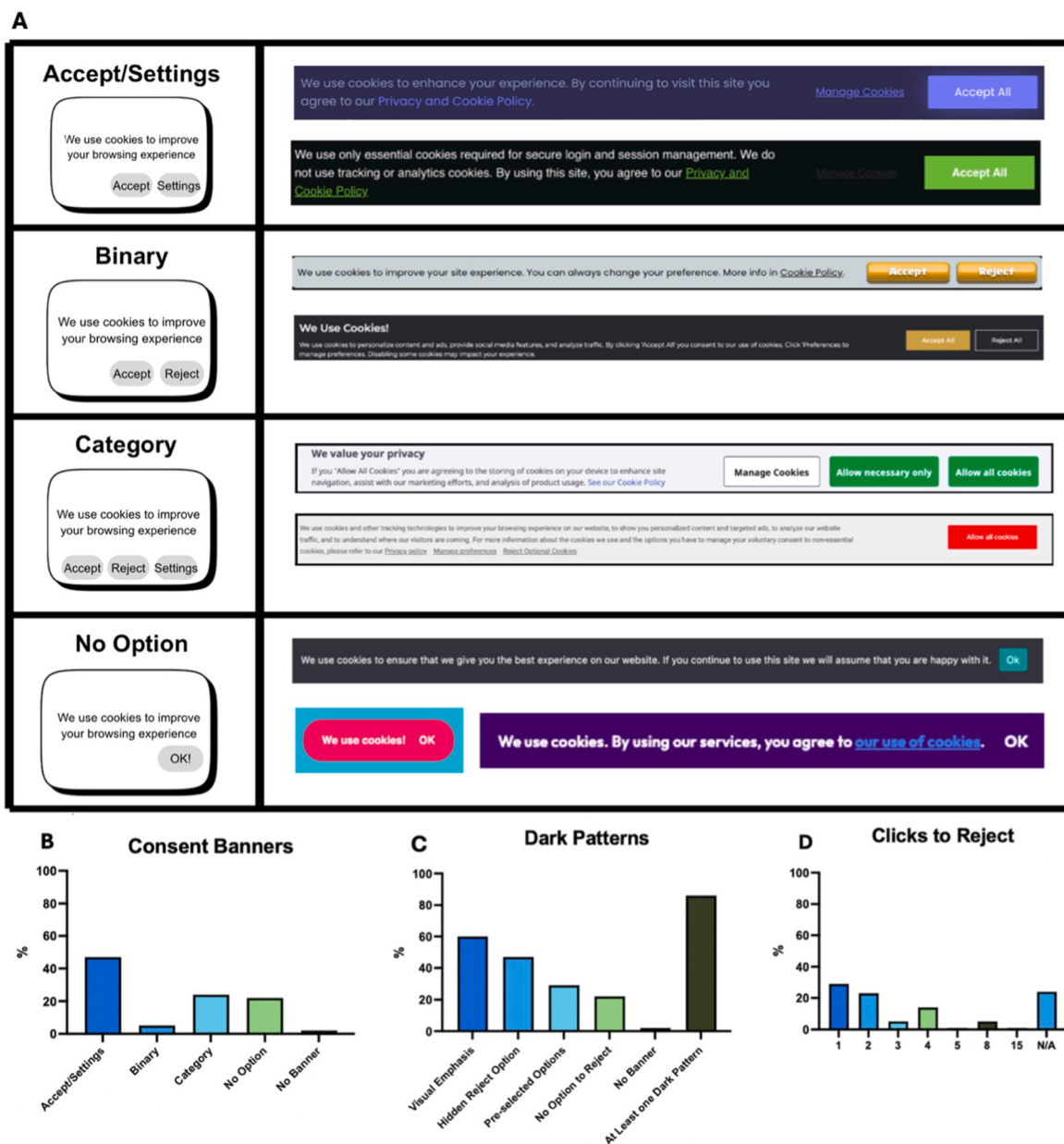


Fig. 2. Consent banner characteristics identified across UK-licensed online gambling websites ($N = 624$). (A) The four consent banner types identified in the audit, with schematic illustrations (left) and real-world examples from audited sites (right). (B) Prevalence of each consent banner type as a percentage of audited sites. (C) Prevalence of each dark pattern category identified within consent banners. (D) Distribution of the number of clicks required to reject tracking across audited sites; N/A indicates sites where rejection was not possible.

Table 1

Summary of dark patterns identified in the audit, including operational definition, prevalence, and GDPR compliance status.

	Definition	Prevalence, n (%)	GDPR Compliance
Dark pattern			
Visual emphasis	The accept option is visually emphasised through colour, size, contrast, or positioning	375 (60%)	Compliant
Pre-selected options	Privacy-unfriendly options are pre-selected by default	181 (29%)	Non-Compliant
Hidden reject option	The reject option is not available on the first layer of the banner	293 (47%)	Debatable — inconsistent with the requirement that consent be as easy to withdraw as to give
No Option to Reject	The banner informs users that data is being collected but provides no option to reject	137 (22%)	Non-Compliant
No Banner	No consent banner is present on the site	12 (2%)	Non-Compliant

Table 2
Frequency of dark patterns and clicks to reject by consent banner design type.

	Accept/Settings (n = 295)	Binary (n = 29)	Category (n = 151)
Dark patterns, n (%)			
Visual emphasis	292 (99.0%)	14 (48.3%)	66 (43.7%)
Pre-selected options	148 (50.2%)	0 (0%)	32 (21.2%)
Hidden reject option	295 (100%)	0 (0%)	0 (0%)
Clicks to reject			
Mean (SD)	3.38 (1.94)	1.00 (0.00)	1.00 (0.00)
Range	2–15	1	1

Dark patterns in consent banner designs like those described in our sample have been widely documented across online websites (Norwegian Consumer Council, 2018; Nouwens et al., 2020; Soe et al., 2020, pp. 1–12; Utz et al., 2019, pp. 973–990), and have been found to significantly increase the proportion of users accepting tracking cookies (Graßl et al., 2025; Nouwens et al., 2020; Utz et al., 2019, pp. 973–990). It is not yet known how online gambling users interact with consent banners, the manner in which their behaviour is influenced by banner designs, or how this behaviour interacts with measures of gambling severity. Study 2 explores this interaction.

5. Study 2

5.1. Introduction

Following our audit of consent banners on UK-licensed online gambling sites, Study 2 examined how banner designs influence consumer behaviour in online gambling environments. Ideally, this would be tested directly on real life gambling platforms, however, given the challenges of obtaining access to proprietary gambling operator data to test safer designs (McGarrigle et al., 2026), we developed an experimental design to simulate an online gambling environment in as authentic a manner as possible.

Our research questions were: how do users interact with consent banners in an online gambling environment? How do banner designs influence choice in an online gambling environment? And, does gambling severity predict susceptibility to dark patterns in consent banners in an online gambling environment? Study 2 tested the

following hypotheses.

Hypothesis 1. Consent banners exhibiting dark patterns will lead to higher rates of acceptance compared to neutral banners.

Hypothesis 2. Participants with higher levels of problem gambling severity, as measured by the Problem Gambling Severity Index (PGSI) will be more likely to accept tracking when exposed to consent banners exhibiting dark patterns.

5.2. Methodology

The experiment was pre-registered (<https://osf.io/p2reh>). Participants (n = 600) were recruited via Prolific at a rate of £9 per hour and were informed that they would be interacting with an online gambling platform. A total of 647 participants were recruited, of whom 32 were excluded due to incomplete responses, resulting in a final analytic sample of N = 615. To capture natural behaviour, the true nature of our study was not disclosed to participants until after the experiment, during a full debriefing. The simulated gambling platform resembled the landing page of a real-life platform, with details of bets which could be placed, and sports fixtures on the week the study took place (Fig. 4). Inclusion criteria required participants to be at least 18 years old, residents of the UK, and to have used an online gambling platform within the previous 12 months. Drawing directly from the banner designs observed in the observational audit of Study 1, six different consent banners were designed and implemented on the simulated gambling platform as they would appear in real life (Fig. 3). The banners comprised three types - binary, accept/settings, and category, each with a “neutral” and “dark” (in visual emphasis) banner design, to determine whether behavioural influence was due to the banner type, the dark patterns, or some combination thereof. As users have no choice with “no option” banners, this banner type was not included, as no behavioural outcome can be measured. Participants first completed the *Problem Gambling Severity Index* (PGSI), and were then randomly assigned to receive one of the six consent banners on the simulated gambling platform. A follow-up survey gathered users’ normative preferences with regard to their data privacy choices online. Ethical approval was obtained from Swansea University Ethics Committee (approval number: 3 2025 14134 13909, approval date: 06/10/2025). The use of partial deception was considered necessary to preserve the ecological validity of the behavioural outcome measure, as prior disclosure of the research focus on consent banners may have altered participants’ interactions

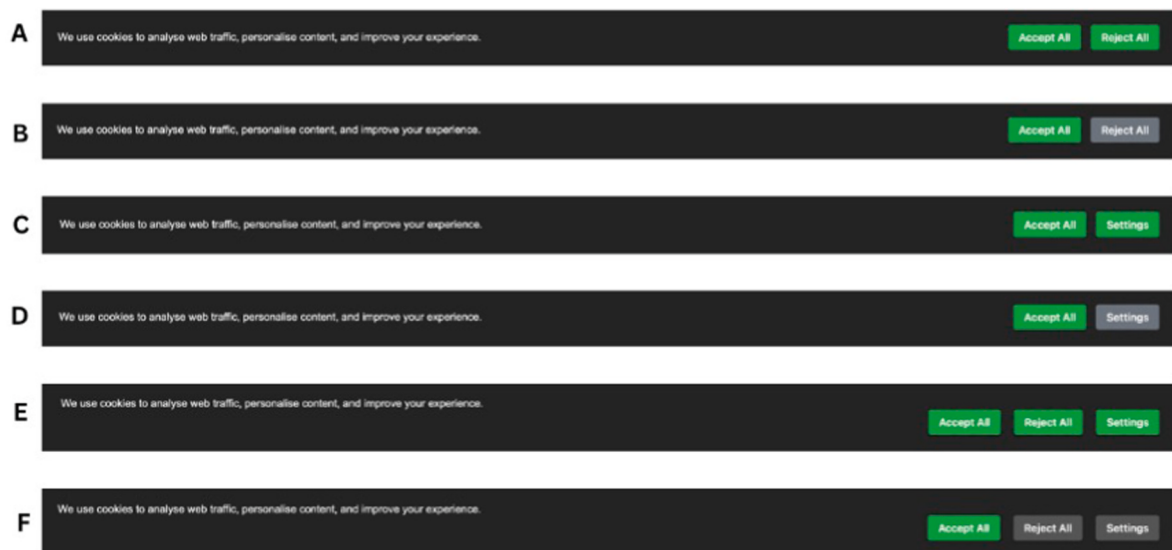


Fig. 3. Cookie consent banners used in the experiment. (A) Binary-Neutral, (B) Binary-Dark, (C) Settings-Neutral, (D) Settings-Dark, (E) Category-Neutral, and (F) Category-Dark.

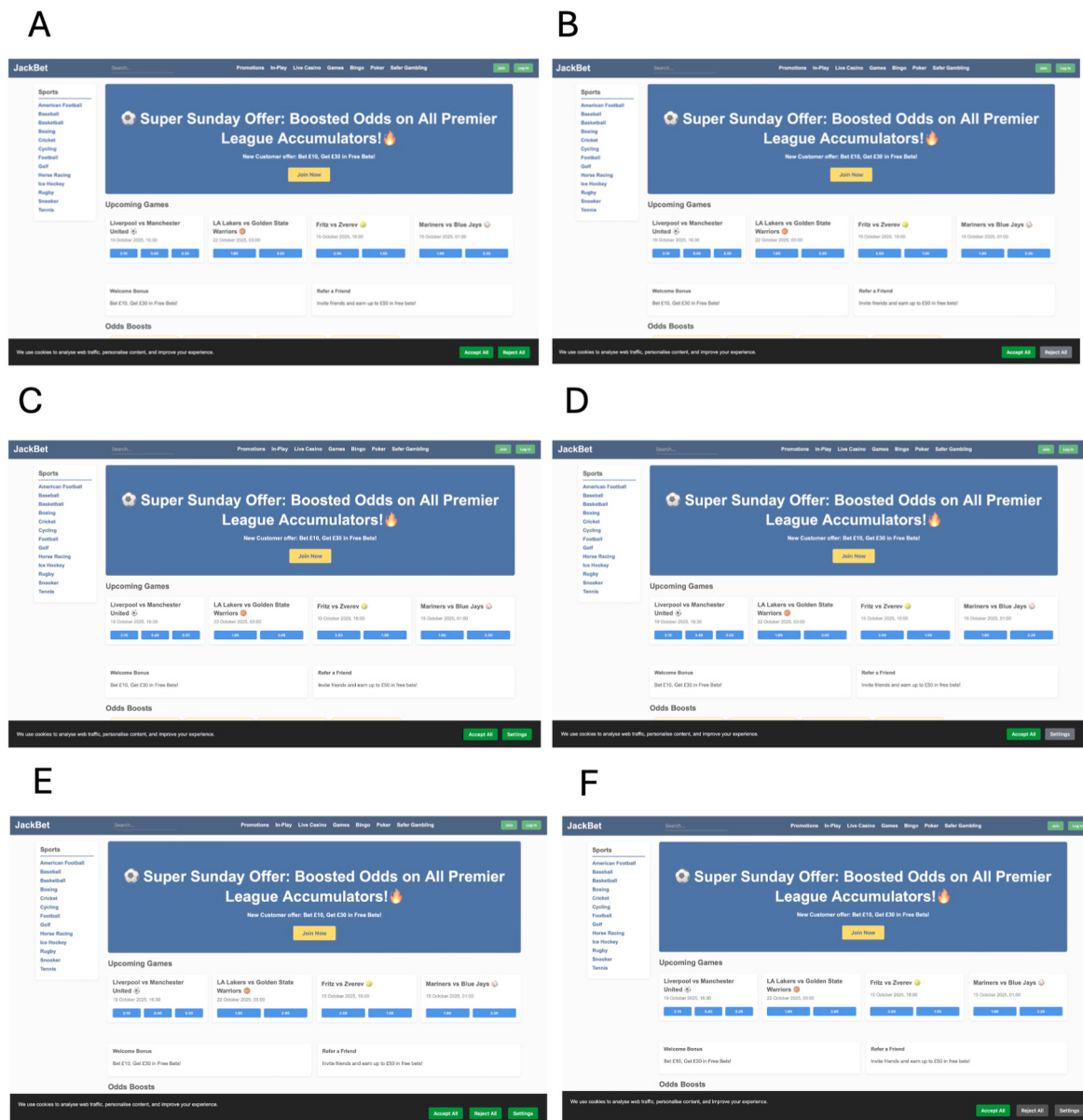


Fig. 4. Simulated gambling site with the six consent banners used in the experiment. A – Binary Neutral, B – Binary Dark, C- Accept/Settings Neutral, D – Accept/Settings Dark, E – Category Neutral, F- Category Dark.

with same. All participants were fully debriefed immediately following the study, including disclosure of the nature and purpose of the deception, and were informed of their right to withdraw their data without consequence.

5.2.1. Statistical analyses

Cookie banner acceptance was analysed using binary logistic regression, with banner type entered as a categorical predictor and the Binary Neutral condition as the reference category. Effects are reported as odds ratios with 95% confidence intervals, indicating how much more or less likely acceptance was for each banner type relative to the reference condition. Gambling severity was assessed using the PGSI and analysed both categorically using chi-square tests of independence and continuously within logistic regression models controlling for banner type. Additional logistic regression models examined the influence of banners which exhibited visual emphasis and hidden reject options, as well as their interactions with PGSI. Evidence for non-significant effects was quantified using Bayes factors (BF_{01}), where values greater than 3 indicate evidence for the null hypothesis. Perceived alignment between

banner choice and participants data privacy preferences was compared using independent-samples t-tests, and differences across banner types were examined using one-way ANOVA with Tukey post-hoc tests where appropriate. All tests used an alpha level of 0.05. A priori power analysis indicated that $n = 100$ per group (total $N = 600$) would provide 0.87 power to detect a large effect (Cohen's $f = 0.40$, $\alpha = .05$) in the primary between-subjects comparison. The obtained sample of $N = 615$ exceeded this target.

5.3. Results

A total of 615 participants completed the study. The mean age of the sample was 42.1 ($SD = 12.7$), with the majority of participants being white (88%) and male (67%). With respect to gambling risk, over half of the sample fell within the moderate to high-risk PGSI categories (51%). Full participant characteristics are presented in Table 3.

The sample included an even split between lower-risk (non-problem and low-risk) and elevated-risk (moderate and high-risk) participants. Though this reflects higher rates of at-risk gambling than would be

Table 3
Characteristics table.

Characteristic	n (%) or Mean (SD)
Total participants	615
Age (years)	42.1 (12.7)
Gender	
Male	413 (67%)
Female	200 (33%)
Other/prefer not to say	2 (1%)
Ethnicity	
White	543 (88%)
Asian	18 (3%)
Black	29 (5%)
Mixed	20 (3%)
Other	5 (1%)
PGSI Group	
No risk	159 (26%)
Low risk	147 (24%)
Moderate risk	200 (33%)
High risk	109 (18%)
Gambling frequency	
Less than once a month	58 (9%)
Monthly	114 (19%)
Weekly	215 (35%)
Daily or almost daily	85 (14%)

N.B. Percentages may not sum to 100% due to rounding.

observed in the general population, the balanced distribution provides adequate variance across the full PGSI range to examine whether effects hold across all levels of gambling risk severity.

5.3.1. Acceptance rate by banner type

Binary logistic regression examined whether banner type predicted acceptance of the cookie banner. The overall model was significant, $\chi^2(6) = 21.84$, $p < .001$, indicating that acceptance rates differed across banner types. Compared to the reference condition (Binary Neutral), participants who viewed the Accept/Settings Neutral banner (OR = 3.10, 95% CI [1.47, 6.55]) or the Accept/Settings Dark banner (OR = 3.97, 95% CI [1.83, 8.60]) were significantly more likely to accept all cookies. No other banner types differed significantly from the reference condition, or with any other banner (Fig. 5).

5.3.2. Overall acceptance rate by PGSI group

Chi-square testing found no significant differences in acceptance across PGSI risk groups, $\chi^2(3, N = 615) = 4.04$, $p = .26$. Similarly, when PGSI was treated as a continuous variable and banner type was controlled for in a logistic regression, PGSI did not significantly predict acceptance ($B = 0.035$, $SE = 0.023$, $p = .12$, $OR = 1.04$).

5.3.3. Acceptance rate of “deceptive” banners by gambling severity

5.3.3.1. Visual emphasis. Binary logistic regression tested whether gambling severity (as measured by PGSI) predicted banner acceptance differently for deceptive (in visual emphasis) versus neutral banners. The overall model was not significant, $\chi^2(3, N = 615) = 4.26$, $p > .05$. Neither PGSI ($B = 0.03$, $SE = 0.03$, $p = .37$, $BF_{01} = 1.29$) banner deception ($B = -0.05$, $SE = 0.25$, $p = .83$, $BF_{01} = 2.98$), nor their interaction ($B = 0.02$, $SE = 0.05$, $p = .74$, $BF_{01} = 2.08$) significantly predicted acceptance.

5.3.3.2. Reject option behind second layer. A binary logistic regression tested whether gambling severity moderated the effect of reject option accessibility (Accept/Settings vs. other banner types) on cookie acceptance. The overall model was significant, $\chi^2(3, N = 615) = 28.07$, $p < .001$, indicating that the predictors jointly explained a significant

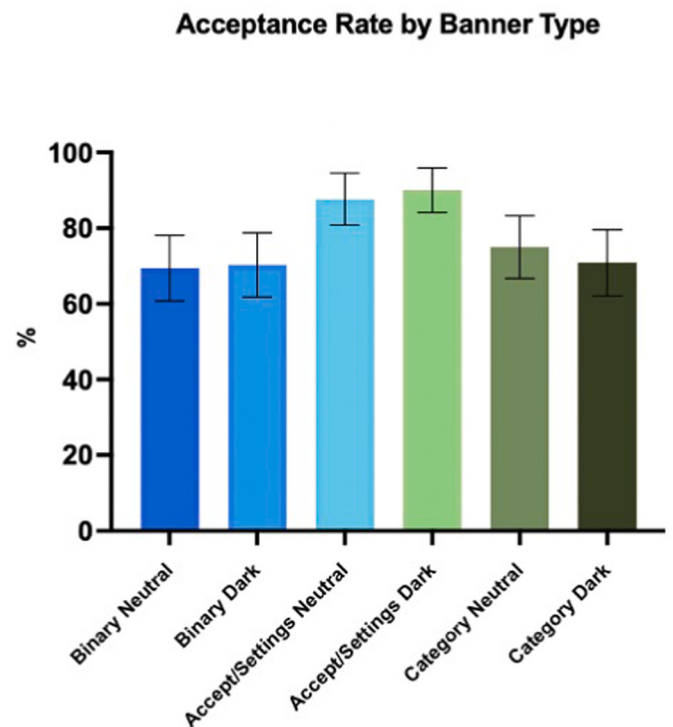


Fig. 5. Acceptance rate by banner type. Error bars represent 95% confidence intervals.

proportion of variance in acceptance. Participants exposed to the Accept/Settings banners were significantly more likely to accept cookies ($B = 0.98$, $SE = 0.33$, $p = .003$, $OR = 2.67$, 95% CI [1.38, 5.18]). However, gambling severity ($B = 0.03$, $SE = 0.03$, $p = .29$, $OR = 1.03$, 95% CI [0.97, 1.10], $BF_{01} > 100$), and the interaction between PGSI and banner type was non-significant ($B = 0.05$, $SE = 0.07$, $p = .42$, $OR = 1.06$, 95% CI [0.93, 1.21], $BF_{01} = 25$).

5.3.4. Does banner choice reflect user preferences?

Following the banner choice, participants were asked: “To what extent does the choice you made on the cookie banner in this experiment reflect your ideal data privacy preferences?” (0 = not at all, 10 = completely). Participants who accepted cookies reported significantly lower perceived alignment between their choice and their ideal data privacy preference ($M = 4.36$) than those who rejected cookies ($M = 7.86$) (Fig. 6). An independent-samples t -test confirmed this difference, $t(264.29) = 15.70$, $p < .001$, 95% CI [3.06, 3.94], $d = 1.40$.

One-way ANOVA tested whether perceived alignment varied by banner type. The analysis revealed a significant effect of banner type, $F(5, 609) = 3.34$, $p = .006$, $\eta^2 = 0.03$. Post-hoc Tukey tests showed that participants who received the Binary-Neutral banner ($M = 5.68$, $SD = 2.88$) reported significantly higher perceived alignment between their decision and their preferences than those who viewed the Accept/Settings-Neutral ($M = 4.45$, $SD = 2.82$, $p = .036$) or Accept/Settings-Dark ($M = 4.53$, $SD = 2.76$, $p = .049$) banners. No other pairwise comparisons were significant.

6. Study 2: discussion

The results of study 2 demonstrate that the type of banner most commonly found on UK online gambling sites (Accept/Settings) significantly influences users toward accepting personal data processing. In addition, participants who received these banners reported that their subsequent decision reflected their true privacy preferences to a significantly lesser degree than those who received a neutral banner,

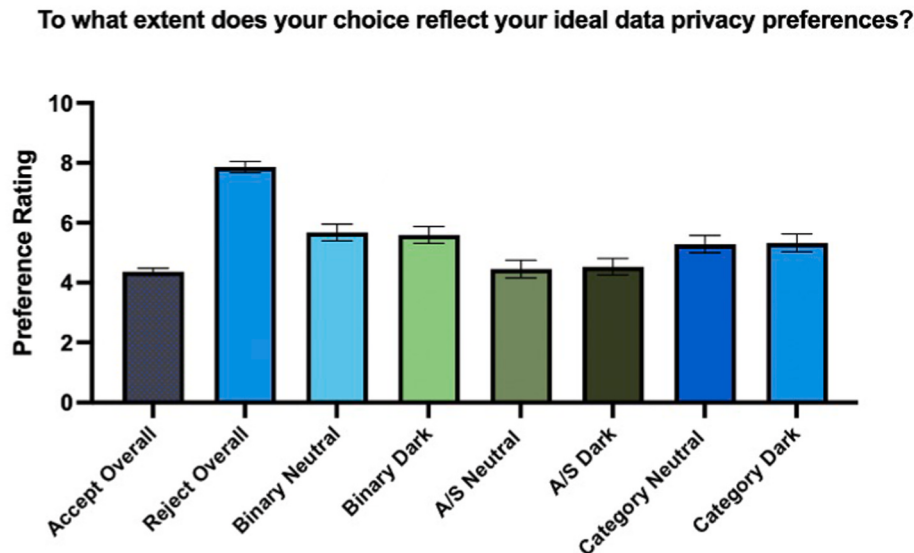


Fig. 6. Mean perceived alignment between cookie-banner choice and ideal privacy preferences by banner type. Error bars represent the standard error of the mean.

suggesting that their choices reflect the influence of the banner design, rather than a true expression of their preferences. There was no significant interaction between banner behaviour and self-reported problem gambling severity, suggesting that the influence of dark patterns in consent interfaces is general, underscoring the need for broad regulatory controls which protect all users.

7. General discussion

The present study revealed systemic infringements of data privacy law across UK online gambling sites, and widespread use of consent banners which exhibit dark patterns. The results of our experiment illustrates not only that these dark patterns significantly influence users towards accepting tracking in an online gambling environment, they also lead to choices misaligned with users' true data privacy preferences.

Study 1 uncovered that over two-thirds (67%) of UK-licensed online gambling sites processed personally identifiable information prior to obtaining user consent, in breach of GDPR. Almost one-quarter (24%) of sites gave users no option to control their data privacy preferences, also in breach of GDPR. In addition, the majority (86%) of sites employed consent banners which exhibit dark patterns, steering users towards the least privacy-friendly options. Rejection of tracking is more difficult than acceptance, with less than one-third (29%) of banners allowing rejection of tracking within one-click, taking up to 15 clicks on some sites. Study 2 provides further understanding of this choice environment, by analysing the behaviour of users when presented with different consent banner designs in a simulated online gambling environment. Users are significantly influenced by common banner designs, in particular the reject option being hidden behind a secondary layer, leading to higher acceptance of tracking and lower alignment between user choice and preference. No interaction was found between gambling severity and influence to dark patterns, all users appear to be equally influenced, suggesting that these dark patterns operate at a general cognitive level rather than exploiting gambling-specific vulnerabilities. While the overall effect of banner type on alignment with data privacy preferences was statistically significant, the effect size was small ($\eta^2 = 0.03$), reflecting the fact that individual differences in privacy attitudes account for substantial variance in alignment scores regardless of banner type. The Accept/Settings banner (the most commonly observed design across UK-licensed online gambling sites) produced odds of acceptance three to four times higher than the Binary Neutral condition (OR = 3.10–3.97), reflecting a strong influence on consent behaviour.

Overall, our findings reveal an environment of systemic data privacy breaches in which consumer choice and right of data control are rarely respected, and one in which, even when personal data is not processed prior to consent, consent banners are designed in such a way as to steer users towards accepting tracking, leading to choices misaligned with their true preferences.

Our results highlight the need for greater regulation of consent banners in online gambling. The most practical way to do so would be to implement stricter user interface design requirements in the form of standardised consent banner designs, as has been posited by researchers in the wider dark patterns literature (Naithani, 2025; Nouwens et al., 2020; Soe et al., 2020, pp. 1–12). Current regulations, while clear in their principles of obtaining “freely given, informed, and unambiguous” consent (GDPR, 2016 p.33), are ambiguous in prescribing specific design requirements to achieve these principles, and this ambiguity has led to the prevalence of deceptive banner designs we see today. The UK Gambling Commission recently introduced stricter licensing conditions on direct marketing, with operators now required to obtain user consent to receiving such communications (Gambling Commission, 2025). Encouragingly, dark patterns considerations appear to have informed the design of this licensing condition, with an opt-out default, one-click choice point, and strict instructions surrounding how the structure and wording of this decision be laid out. We argue that such conditions must be extended to the data consent choice point (i.e. consent banners) also, as current regulations do not protect consumers against dark patterns with regard to initial personal data processing. Indeed, the present study finds dark patterns to be widespread on UK-licensed gambling sites, influencing consumers towards selecting the least privacy-friendly options.

In the online gambling industry, there is particular risk of harm caused by access to and use of consumer data (ICO & CMA, 2023), yet the methods by which operators use this data for segmentation, profiling, and targeted marketing are largely unknown. In an industry whereby the consumers at most risk of harm are also the most loss-heavy (Fiedler et al., 2019), the profit opportunities enabled by identifying and targeting high-risk behavioural patterns for commercial gain necessitates strong regulatory action on the industry's ability to collect and use consumer data. Given that the characteristics used to segment and target users significantly overlap with those used to identify harmful gambling behaviours, the most pragmatic solution may be that individualised targeting in this industry be prohibited altogether. Future research which explores the behavioural throughlines of the use of personal data

in the online gambling industry could further establish this case, though the inherent methodological difficulties in doing so (McGarrigle et al., 2026; Newall et al., 2024) behoves increased scrutiny and stronger action from regulatory bodies.

Previously, harmful products existed in an analogue environment, in which the producers of such products were unable to gather real-time data on their most vulnerable consumers. We are now in an era in which many addictive behaviours take place online (e.g. gambling, pornography, social media, gaming), and the producers of these products can track and target users they deem most susceptible to inducement. If the tobacco industry at the height of their powers had thousands of data points on what, when, and how often their customers smoked, craving levels could have been predicted and used to send an alert to induce users into buying another packet. Free cigarettes could have been offered to users attempting to quit, and users determined most susceptible to picking up the habit could have been identified and targeted with personalised inducements. It could be argued that this parallel is in effect today in the online gambling industry. The scale of consumer data in the hands of online gambling operators enables highly accurate modelling of the behavioural patterns of the most loss-heavy gambling users, which can be used to deploy personalised inducements designed to increase consumption, further exacerbating an already asymmetric relationship between operator and consumer. Under the framework of GDPR, consumers have a right of control of this data. However, the present study has shown that on UK-licensed online gambling sites this right is rarely respected, with personal data often being processed prior to consent, and consent banners designed in such a way as to steer users towards accepting tracking against their preferences. Stronger scrutiny and enforcement from regulatory bodies is urgently required to protect consumers from these practices.

8. Limitations

The findings of this research are subject to several limitations. First, the audit was confined to UK-licensed gambling operators and findings may not generalise to EU-wide jurisdictions. Cross-national replication would be a valuable direction for future research. Second, the audit was conducted during a fixed time window (April–June 2025) and may not reflect the full range or evolution of consent practices in the sector. Operator practices may change over time, particularly in response to regulatory enforcements or updated guidance. Longitudinal replication would enable tracking of whether practices improve following increased regulatory scrutiny. Third, coding of consent banner interfaces was conducted by a single researcher without formal inter-rater reliability assessment. Fourth, in Study 2, perceived realism of the experimental platform was not formally assessed. Future research may benefit from incorporating perceived realism checks to further establish the ecological validity of experimental consent paradigms. In addition, study 2 is necessarily limited to observable frontend consent interfaces and network traffic captured on page load, and cannot account for backend data practices or the full scope of data processing that may occur thereafter.

9. Conclusion

Consent banners on UK online gambling platforms frequently exhibit dark patterns which influence consumer choice, leading users to disclose more personal data than intended, against their stated preferences. In addition, personal data is often processed prior to consent, and a significant proportion of banners give no data privacy choice to the consumer whatsoever, in breach of GDPR. Access to these data enables the design and deployment of targeted marketing, and the tracking of gambling consumers across the web, with the goal of maintaining engagement and consumer losses. The particular risk posed by data surveillance in online gambling, given the structural overlap between profitable behavioural patterns and harmful gambling behaviours,

underscores the importance of data consent design as a consumer protection issue.

Current regulations, while explicit in their principles, are ambiguous in prescribing specific consent banner design requirements, which are necessary to prevent the prevalence of dark patterns we have observed on online gambling platforms. Given the particular risk of harm that can come to gambling consumers as a result of data surveillance, there is a strong argument that the use gambling behavioural data for marketing purposes should be forbidden altogether. At a minimum, sharing of these data with regulatory bodies and independent researchers would allow for the implementation of safeguards using real-time indicators of harm, rather than for commercial opportunities. Future research should examine how and when gambling consumers are targeted with personalised inducements, with particular attention to the degree to which vulnerable users are exposed to such practices.

CRedit authorship contribution statement

Jack McGarrigle: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software, Validation, Visualization, Writing – original draft, Writing – review & editing. **Jamie Torrance:** Conceptualization, Methodology, Supervision, Writing – review & editing. **Martyn Quigley:** Conceptualization, Methodology, Supervision, Writing – review & editing. **Simon Dymond:** Conceptualization, Methodology, Supervision, Writing – review & editing.

Ethics declaration

Written informed consent to take part in the study and to publish the article has been obtained from all participants or their legal representatives. The privacy rights of participants have been observed.

This study was performed in compliance with relevant laws, regulatory frameworks and guidelines where the research took place. This study was approved by the Swansea University. (Approval No. 3 2025 14134 13909)

Declaration of the use of AI

During the preparation of this work, the authors did not use any AI or AI-assisted technologies.

Funding statement

The lead author is funded by a Welsh Graduate School for the Social Sciences (WGSSS) scholarship. The funding sponsors played no role in this research.

Data availability

The study was preregistered prior to data collection and all data, materials, analysis code, and screenshots of audited websites associated with this study are openly available on the Open Science Framework at <https://osf.io/p2reh/files>.

References

- Alvarez & Marsal. (2025). Annual gambling advertising sponsorship report. <https://www.azarplus.com/wp-content/uploads/2026/02/Gambling-Advertising-and-Sponsorship-Report-2025-Executive-Summary.pdf>.
- Centre for Data Ethics and Innovation. (2020). Online targeting: Final report and recommendations. <https://www.gov.uk/government/publications/cdei-review-of-online-targeting/online-targeting-final-report-and-recommendations#fn:13>.
- Christl, W. (2022). Digital profiling in the online gambling industry. <https://cdn.sanity.io/files/btrscf0/production/e23ea75fe93f775d9f9ed795427f4b5ed8d67016.pdf>.
- Englehardt, S., & Narayanan, A. (2016). Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 16 pp. 1388–1401. CCS. <https://doi.org/10.1145/2976749.2978313>.

- Fiedler, I., Kairouz, S., Costes, J.-M., & Weißmüller, K. S. (2019). Gambling spending and its concentration on problem gamblers. *Journal of Business Research*, 98, 82–91. <https://doi.org/10.1016/j.jbusres.2019.01.040>
- FTC. (2025). FTC surveillance pricing 6(b) study: Research summaries A staff perspective. https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf
- Gainsbury, S. M. (2015). Online gambling addiction: The relationship between internet gambling and disordered gambling. *Current Addiction Reports*, 2(2), 185–193. <https://doi.org/10.1007/s40429-015-0057-8>
- Gambling Commission. (2025). LCCP condition 5.1.12—Direct marketing preferences. <https://www.gamblingcommission.gov.uk/licensees-and-businesses/lccp/condition/5-1-12-direct-marketing-preferences>
- General. (2016). *Data protection regulation*, L119/33. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- Google. (2025). *Google marketing platform*. https://marketingplatform.google.com/intl/en_uk/about/analytics/features/?_gl=1*1sb4i3l*_up*MQ..*_ga*N DQyMjgwNDYxLjE3NjI5NTYwOTI.*_ga_177S7Q8J6Q*_czE3NjI5NTYwOTIkbzEkZzAkdDE3NjI5NTYwOTIkaJYwJGwwJGgw
- Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., & Buijzen, M. (2025). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, 3(1), 1–38. <https://doi.org/10.33621/jdsr.v3i1.54>
- Gray, C. M., Sanchez Chamorro, L., Obi, I., & Duane, J.-N. (2023). Mapping the landscape of dark patterns scholarship: A systematic literature review. *Designing interactive systems conference*. <https://doi.org/10.1145/3563703.3596635>
- Guardian. (2025). *We didn't click 'consent' on any gambling website. So how did Facebook know where we'd been?* <https://www.theguardian.com/technology/2025/feb/08/we-didnt-click-consent-on-any-gambling-website-so-how-did-facebook-know-where-wed-been>
- Guillou-Landreat, M., Gallopel-Morvan, K., Lever, D., Le Goff, D., & Le Reste, J.-Y. (2021). Gambling marketing strategies and the internet: What do we know? A systematic review. *Frontiers in Psychiatry*, 12, Article 583817. <https://doi.org/10.3389/fpsyt.2021.583817>
- Hing, N., Browne, M., Russell, A. M. T., Rockloff, M., & Rawat, V. (2025). The high cost of direct marketing from wagering operators, tipsters and affiliates: An ecological momentary assessment of how wagering promotions drive betting, expenditure, and harm. *Journal of Behavioral Addictions*, 14(3), 1355–1367. <https://doi.org/10.1556/2006.2025.00067>
- Information Commissioner's Office. (2024). *Bonne terre limited reprimand*. <https://ico.org.uk/media2/migrated/4031023/bonne-terre-limited-reprimand.pdf>
- Information Commissioner's Office. (2025). *What are storage and access technologies? ICO*. <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/what-are-storage-and-access-technologies/>
- Information Commissioner's Office & Competition and Markets Authority. (2023). *Harmful design in digital markets: How online choice architecture practices can undermine consumer choice and control over personal information*
- Matte, C., Bielova, N., & Santos, C. (2020). Do cookie banners respect my choice? : Measuring legal compliance of banners from IAB europe's transparency and consent framework. *2020 IEEE symposium on security and privacy (SP)*. <https://doi.org/10.1109/sp40000.2020.00076>
- McGarrigle, J., Smith, J., Griffiths, J., Torrance, J., Quigley, M., & Dymond, S. (2026). Dark patterns in online gambling: A scoping review and classification of deceptive design practices. *Journal of Behavioral Addictions*. <https://doi.org/10.1556/2006.2025.00096>
- Naithani, P. (2025). Standardised cookie banner: A solution to the cookie consent problem. *International Review of Law, Computers & Technology*, 39(2), 213–230. <https://doi.org/10.1080/13600869.2024.2364995>
- Newall, P., Allami, Y., Andrade, M., Ayton, P., Baker-Frampton, R., Bennett, D., Browne, M., Bunn, C., Bush-Evans, R., Chen, S., Collard, S., De Jans, S., Derevensky, J., Dowling, N. A., Dymond, S., Froude, A., Goyder, E., Heirene, R. M., Hing, N., ... Roberts, A. (2024). 'No evidence of harm' implies no evidence of safety: Framing the lack of causal evidence in gambling advertising research. *Addiction*, 119(2), 391–396. <https://doi.org/10.1111/add.16369>
- Newall, P. W. S., Moodie, C., Reith, G., Stead, M., Critchlow, N., Morgan, A., & Dobbie, F. (2019). Gambling marketing from 2014 to 2018: A literature review. *Current Addiction Reports*, 6(2), 49–56. <https://doi.org/10.1007/s40429-019-00239-1>
- Norwegian Consumer Council. (2018). Deceived by design. How tech companies use dark patterns to discourage us from exercising our rights to privacy. <https://sto rage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf>
- Nouwens, M., Llicardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI conference on human factors in computing systems*, 20 pp. 1–13. CHI. <https://doi.org/10.1145/3313831.3376321>
- Optimove. (2020). Optimove use case: Contextualizing realtime player marketing. <https://www.optimove.com/pdf/Optimove-Use-Contextualizing-Realtime-Player-Marketing.pdf>
- Papadogiannakis, E., Papadopoulos, P., Kourtellis, N., & Markatos, E. P. (2021). User tracking in the post-cookie era: How websites bypass GDPR consent to track users. *Proceedings of the web conference 2021* (pp. 2130–2141). <https://doi.org/10.1145/3442381.3450056>
- Papenmeier, F., Halama, J., & Reichert, C. (2025). Accepting cookies: Nudging, deceptive patterns and personal preference. *Computers in Human Behavior*, 168, Article 108641. <https://doi.org/10.1016/j.chb.2025.108641>
- RTM vs Bonne Terre Limited. KB-2023-000775 (High Court of Justice January 23, 2025). <https://www.awo.agency/files/RTM-v-Bonne-Terre-judgment.pdf>
- Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.-A., & Santos, I. (2019). Can I opt out yet?: GDPR and the global illusion of cookie control. *Proceedings of the 2019 ACM Asia conference on computer and communications security*. <https://doi.org/10.1145/3321705.3329806>
- Schüll, N. D. (2012). *Addiction by design: Machine gambling in Las Vegas*. Princeton University Press. <https://doi.org/10.1515/9781400834655>
- Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design—Dark patterns in cookie consent for online news outlets. *Proceedings of the 11th nordic conference on human-computer interaction: Shaping experiences*. Shaping Society. <https://doi.org/10.1145/3419249.3420132>
- Sportradar. (2025). CRM and retention marketing for sportsbooks and casinos. http://s://goto.sportradar.com/1/533382/2023-12-11/7p222c/533382/1702299364F buU3Dld/Sportradar_vaix_crm_marketing_english.pdf
- Syvtersen, A., Erevik, E. K., Hanss, D., Mentzoni, R. A., & Pallesen, S. (2022). Relationships between exposure to different gambling advertising types, advertising impact and problem gambling. *Journal of Gambling Studies*, 38(2), 465–482. <https://doi.org/10.1007/s10899-021-10038-x>
- Torrance, J., John, B., Greville, J., O'Hanrahan, M., Davies, N., & Roderique-Davies, G. (2021). Emergent gambling advertising; a rapid review of marketing content, delivery and structural features. *BMC Public Health*, 21(1). <https://doi.org/10.1186/s12889-021-10805-w>
- Tran, L. T., Wardle, H., Colledge-Frisby, S., Taylor, S., Lynch, M., Rehm, J., Volberg, R., Marionneau, V., Saxena, S., Bunn, C., Farrell, M., & Degenhardt, L. (2024). The prevalence of gambling and problematic gambling: A systematic review and meta-analysis. *The Lancet Public Health*, 9(8), e594–e613. [https://doi.org/10.1016/S2468-2667\(24\)00126-9](https://doi.org/10.1016/S2468-2667(24)00126-9)
- Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*. <https://doi.org/10.1145/3319535.3354212>
- WARC. (2025). AA/WARC expenditure report Q2 2025. <https://www.warc.com/about-media/expenditure-report>
- Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory Re-Wired* (3rd ed.). Routledge.