DBS Business Review 04 | 2021
ARTICLE | dbsbusinessreview.ie

Cookies ‘n’ Consent: an Empirical Study on the Factors Influencing Website Users’ Attitudes towards Cookie Consent in the EU

Lakshmi N. Jayakumar
Postgraduate
MSc Digital Marketing, Dublin Business School
Dublin, Ireland

Abstract
Since the General Data Protection Regulation (GDPR) came into force in 2018, various firms have been found violating or circumventing the ePrivacy Directive known as the Cookie Law that lays out the cookie consent guidelines for websites. To improve the GDPR compliance rate, several conversations are going on between the EU Commission, data protection agencies, business and website owners and advertising vendors regarding their cookie policy, obtaining user consent for data collection and its usage. One of the key stakeholders, the website users, whose privacy is in question, seems to be left out of the discussions. This study aimed to understand user perception towards website cookie banners that are mandatory under GDPR, and the influence of factors like awareness of cookies, user experience, consent banner design, privacy risk, and brand trust on user’s willingness to accept all cookies, to develop recommendations to improve customers’ motivations to give consent. Using a quantitative approach, the primary data was collected from 132 internet users residing in the EU region through an online survey questionnaire shared in social media networks. The results showed that (i) the majority of respondents had more than moderate level of awareness about cookies, (ii) they are more likely to accept cookies for quick access or task completion, (iii) acceptance of cookies was varied across different categories of online activity and (iv) given a choice they are more likely to opt-out of third-party cookies that are widely used for targeted advertising. Since third-party cookies will be phased out in the near future and are likely to be replaced with more advanced customer tracking technologies that are harder to opt-out of, this study proposes a framework for a Consent for Advertising Directive (CAD) to go beyond the existing Cookie Law, which will improve user data protection regardless of the tracking technology used, and help brands to improve transparency about their data collection and avoid GDPR violations.
Keywords: GDPR; Data protection; Cookie consent; Online advertising; Third-party cookies; Online privacy; ePrivacy Directive.

Introduction

The study aimed to identify the factors influencing user attitudes towards website cookie consent mechanisms by studying how the website cookies are used in terms of online advertising, the design framework for the cookie consent mechanisms, how they affect online user experience, the need for cookie consent as per the GDPR

Cookie policy and what has been the impact of the ePrivacy directive in online privacy so far. The findings of the study were used to identify the gaps in current cookie consent mechanisms in terms of user experience and user privacy and suggest recommendations in existing cookie policy to be more effective in protecting user privacy.

The digital revolution in the last two decades has seen giant leaps in Information and Communications Technology (ICT), making it easier for customers to adopt online and mobile communication, and enterprises to go through a digital transformation in all their functions (Rogers, 2016). More often than not, a customer's first touchpoint with the brand is online, either through a website or an app. Good online user experience is essential in moving the customer from the consideration to the conversion stage of the customer journey (Hoban and Bucklin, 2015). As a result, the lines between traditional marketing and digital marketing have now disappeared (Poole, 2019).

In a business context, user experience can have a significant impact on the value chain of a product, service or system (Marcus, 2016). According to Porter, improving the value chain is one of the strategies through which businesses can achieve competitive advantage (Porter, 1996). The customer experience report from Forrester (Schmidt-Subramanian, 2014) estimated that improving the online customer experience from below-average to above-average will increase the additional revenue by $3 billion for wireless carriers, more than $1 billion for hotels, $262 million for insurers, and $227 million for retailers (Ross, 2014). On the other hand, poor user experience in the consumer products sector can lead to negative word of mouth, poor reviews, decreased sales and negative impact on the brand, which will also increase support and service costs and increase the need for training (Ross, 2014).

In previous studies on the impact of cookie-popups, the data was collected through automated systems and browser engines (Nouwens *et al*., 2020). However, this study collected feedback directly from users about their perception of the cookie-popups, which yielded better insights on the customer pain points that can be helpful for companies to adopt a user-friendly approach for obtaining cookie consent. The findings of this study would be of interest to online businesses, especially for websites which are dependent on the page views, like news media websites, e-commerce websites, social media and entertainment websites (Schofield, 2018).

Theoretical perspectives

The Online Buying Persuasion (OBP) model (San and Camarero, 2009) illustrates how cognitive signals are used by brands to increase customers' satisfaction level in building customer trust towards brands. It is also found that compliance with the GDPR framework, which has Privacy by Design, End-to-End security, Transparency, Respect for the User, as its foundational principles (Kurtz, Semmann and Bã, 2018),

is likely to influence customer perception and trust towards brands which will increase the likelihood of customers transacting with a brand online.

One of the major components of online advertising is Online Behavioural Advertising (OBA). According to the research article by Boerman, Kruikemeier and Zuiderveen Borgesius, OBA is defined as

> the practice of monitoring people's online behaviour and using the collected information to show people individually targeted advertisements

By tracking different websites, the user is visiting and based on consumer interest, suitable ads would be shown on partner websites (Boerman, Kruikemeier and Zuiderveen Borgesius, 2017).

This helps advertisers to target customers, who are already interested in the product or service which makes the conversion, much more easily as they address their immediate needs for products and services (Ur *et al*., 2012). Since their inception, cookies have been a cause of concern (Cranor, Byers and Kormann, 2003), even though their usage is not a direct violation. Many websites require cookies to function properly, especially in situations where personalised website experience is provided. Cookies are used to keep track of user preference during a browsing session, adding or removing items from the cart during an online shopping session, or automatically signing in the user to their email account (Chapman and Dhillon, 2002).

Website owners use cookies termed as first-party cookies (as shown in Figure 1 as A) to track website activities of a website visitor (second party) for analytics purposes. Often, an advertising partner or Ad Vendor (third party) places additional cookies, known as the third-party cookie (as shown in Figure 1 as B) to track user behaviour even after they exit the original website through a process called cookie syncing (as shown in Figure 1 as C). These third-party cookies have been recognised as a privacy threat since their inception (McStay, 2013).

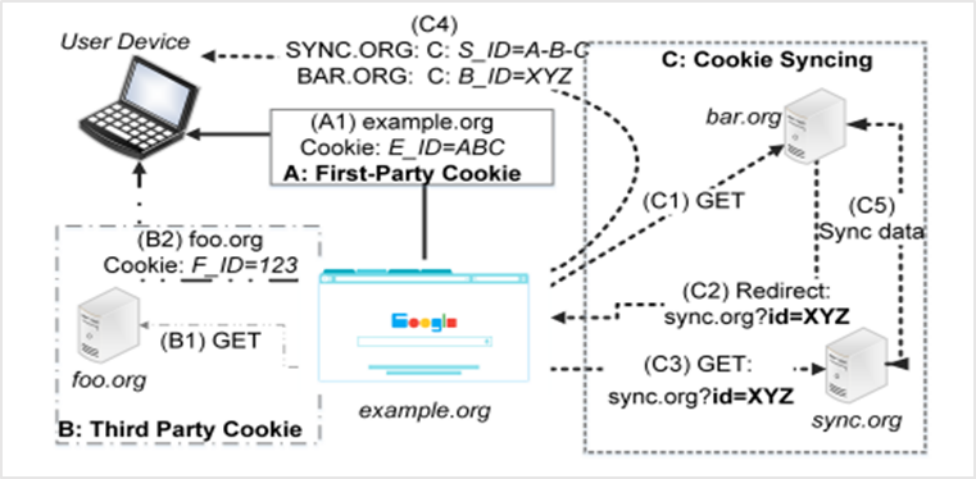

Figure 1: Different types of cookies: (A) a first party cookie - directly set by the visited website, (B) a third-party cookie - set by a third-party embedded in the website, and (C) a synchronized cookie - shared between two parties.
Source: Urban et al., 'The Unwanted Sharing Economy'

Previous studies have shown that while users like the idea of getting relevant ads, they were not comfortable with online profiling or cookie tracking. This is not necessarily because their data is being collected but mostly due to the lack of transparency of when and how much data is collected, and who has access to these data. (Ur *et al*., 2012). Other studies have also pointed out that privacy concerns damage the reputation of brands/websites and lower customer trust in them which often leads to lower usage, adoption and patronage intentions (Chellappa and Sin, 2005; Jarvenpaa, Tractinsky and Vitale, 2000; Jutla and Bodorik, 2005).

GDPR Cookie Policy

To address the privacy concerns specifically related to cookies, since 2009 the EU Commission has made it mandatory for websites to get informed consent from users accessing from the EU region, before installing cookies in their devices. Most websites have been using either a cookie banner or a pop-up to get cookie consent. A 2019 study which covered over 3.5000 websites, has found that 49% of websites are not in compliance with the EU directive and violate the cookie law as it is often referred to. 74% of websites install third party cookies before any user consent (Trevisan *et al*., 2019).

The study also indicates the various reasons from other studies for the cookies' regulatory failure, which are lack of clear opt-out options, non-standardisation implementation of ePrivacy directive among EU nations, enforcement failures, lack of awareness among users and the general public (Cofone, 2016; Leenes, 2015).

Many prominent websites argue on implied consent where, if the user ignores the cookie bar but continues to use the site, it is taken as consent from the user. Other websites do not give a choice to opt-out but merely get an acknowledgement from users that cookies are being used. A 2008 report addressed to the UK Prime Minister and the Secretary of State for Justice, (Walport and Thomas, 2008) presented the difference between genuine consent and enforced consent. They explained consent cannot be passive and needs to be active. The user is required to do something to give consent; a non-response cannot be taken as genuine consent.

Following the Data Sharing Report (Walport and Thomas, 2008), the ePrivacy Directive was amended in 2009 to discipline organisations and regulate their cookie usage. The directive demanded that websites must (i) provide all its visitors with a clear description of all the parties who will be serving cookies or any other tracking mechanisms, (ii) install the cookies or other such tracking mechanisms only after obtaining explicit consent from the user, and (iii) describe how the collected information is being used.

Framework for Cookie Consent Mechanisms

To identify the factors that are likely to influence the user acceptance of cookie consent mechanisms, the Technology Acceptance Model (TAM) (Davis, 1989) was used. Despite some reservations, TAM3 (Venkatesh and Bala, 2008), the third iteration of the Technology Acceptance Model, is used as the general framework for many studies and has been found, consistent with many studies (Stewart and Jürjens, 2018), that the factors like design, perceived usefulness, perceived risk, trust, etc. influence the adoption of new technology. Accordingly, the study aimed to examine if educating the user of the perceived usefulness of giving cookie consent and the perceived ease of use in setting cookie preferences in the cookie banner, would increase trust among users for safer online user experience.

PACT Analysis for UX Design

Systems that are designed following the PACT framework (Marcus, 2016), ensure all the PACT elements fit together seamlessly thus ensuring a delightful user experience. In general practice, there is not much evidence found if the privacy settings of a website or the cookie consent mechanism follow the PACT model or any other particular framework. The current cookie consent programs are only being added as an afterthought for GDPR compliance, and not necessarily following the Privacy by Design principles of GDPR (Cavoukian, 2010).

In September 2010, Neelia Kroes, the EU Commissioner for the Digital Agenda, called for consensus between consumer protection and commercial pragmatism. This emphasised the need for a user-friendly solution for obtaining cookie-consent, instead of using intrusive cookie pop-ups or going the other extreme of burying the cookie and privacy policy deep in the website, which is not easily accessible (Lee, 2011). The Irish Data Protection Commission (DPC) released a report in April 2020 on cookies and other tracking technologies, highlighting the presence of badly-designed, even deliberately-deceptive, cookie banners and consent management tools among prominent sites. It also shed light on dark patterns used by certain consent management platforms like Quantcast which uses cookie banner interfaces with pre-checked boxes before any action taken by the user (Data Protection Commission, 2020).

Impact of GDPR on Online Privacy

The 2019 study of four years showed the percentage of privacy violations have stayed the same, even after GDPR became enforceable in 2018 (Trevisan *et al*., 2019). According to a Capgemini survey conducted in June 2019, fewer than 30% of global businesses were found to be GDPR compliant, one year after the enforcement of GDPR came into effect (Capgemini Research Institute, 2019). A recent study on consent management platforms which emerged after the GDPR enforcement in 2018, found that that only 11.8% of websites were fully compatible with the ePrivacy directive. In many instances, the cookie banner did not affect the installation of cookies, the privacy controls were either buried deep or unnecessarily

complicated. This shows the ineffectiveness of the cookie law and its enforcement, and the need for better approaches to protect consumer privacy.

Phil Lee, an expert in online privacy and digital regulation, in his 2011 journal article, identified seven practical measures website owners can take to mitigate risk when serving cookies for targeted advertising as a middle road to EU and Non-EU privacy policies (Lee, 2011). In line with those measures, recently in April 2020, the Irish DPC issued specific guidelines concerning cookie banners and cookie consent, which included removing pre-checked boxes, removing any nudging for cookie acceptance, very clear accept and reject options in the sliders and checkboxes and keeping the cookie preferences up to date.

On the other hand, Stephen Engberg, an expert in Security Economics, argues consent does not make sense in key areas of data protection as users are not always aware of the implications or causality of providing consent in the collection and processing of personal data (Engberg, 2015). He further states that moving to a Security by Design approach is likely to resolve consent and compliance issues which are not resolved by the current Privacy by Design approach.

Major online ad vendors and browsers have already started dealing with privacy concerns with third-party cookies. While Apple, Microsoft and Mozilla have banned third-party cookies, Google has announced that it will phase them out in the next two years (Lardinois, 2020). This is not to say they will not be tracking online behaviour. They are likely to use some other tracking technologies, and it needs to be seen if the new methods will be less intrusive and how they will impact behavioural advertising. Meanwhile, the updated version of the cookie law called the ePrivacy Regulation (ePR) is expected to replace the 2002 ePrivacy Directive, to bring in more standardisation and enforcement regarding cookie policy and obtaining cookie consent.

While the impact of GDPR cannot be denied, it is far from perfect, which is evident from the low level of compliance, weak enforcement of privacy laws and lack of awareness among customers. The major players are still opting to pay fines instead of striving for full compliance. The influence of the privacy issues in terms of user experience, data security, mitigating risk and earning customer trust is undeniable, and this means companies will have to continuously update and reframe their privacy and data protection policies.

The main research question was to find out which of the external factors shown in Figure 2 are influencing customer attitude towards cookie consent. This will help to identify factors motivating customers to give cookie consent to opt-in or opt-out of cookie usage. By studying the underlying motivations for consent, regardless of the technology or the privacy directive, brands can focus on what motivates customers to give consent and hence mitigate the risk of the volatile legality of using customer data.

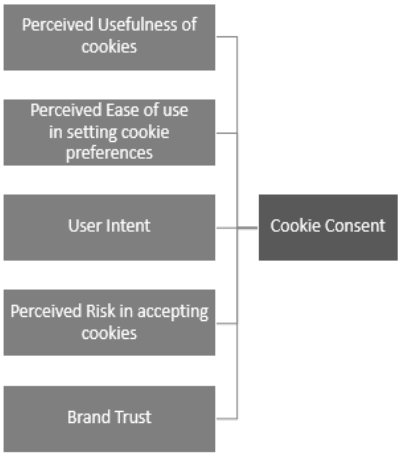

*Figure SEQ Figure * ARABIC 1 Different types of cookies: (A) a first party cookie—directly set by the visited website, (B) a third-party cookie—set by a third-party embedded in the website, and (C) a synchronized cookie—shared between two parties. Source: Urban et al., 'The Unwanted Sharing Economy'*

Methodology

Sample

The study was aimed at general internet users which are considered a wide audience. Hence, the non-probability sampling method of self-selection sampling allowed the researcher to publicise the need for the study through appropriate media and invite users to respond (Saunders, Lewis and Thornhill, 2019). The target demographic for this study was online users above the age of 18, residing in the EU region, who are likely to visit varied types of websites like news media, shopping, social networking and general interest websites, apart from their work or study-related web portals.

Design

The research model was developed by reviewing the Technology Acceptance Model (TAM) (Venkatesh and Bala, 2008), Online Buying Persuasion (OBP) (San and Camarero, 2009) and Stimulus Theoretical Framework (STF) (Lai, 2017) models. Based on the review, the correlation between independent variables like design, security, satisfaction, trust and the factors like perceived usefulness, perceived ease of use, user intent, perceived risk, and brand trust on the dependent variable of cookie consent acceptance (as shown in Figure 2) were examined using the survey results.

Materials

The online questionnaire was designed using Google Forms and had 12 questions in total, 10 of which covered the research topics and were made up of a combination of close-ended, multiple-choice, Likert type and Likert scale questions as shown in Figure 3 below.

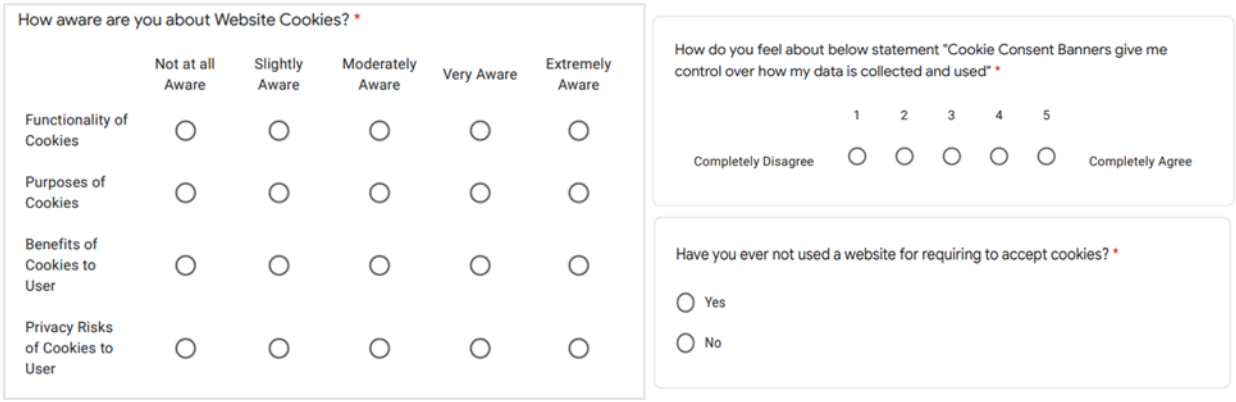

Figure 3: Sample questions from the survey questionnaire

Procedure

The survey was distributed through social media channels, primarily LinkedIn and Facebook. As per GDPR, the questionnaire included the consent form, and no personally-identifiable data was collected. The only demographic detail collected was whether the respondents were residing in the European Region or from Non-EU, so that they could be filtered out. A total of 140 responses were received, including 8 Non-EU responses which were removed to form the final data set of 132 responses.

Results

This section displays the results of the survey with the appropriate charts and description of the results based on the factors (as shown in Figure 2) highlighted in the research design.

Awareness Level of Online Users about Cookies

As shown in Chart 1 below, the majority of users were only moderately aware of the functionality of cookies, their purposes and benefits as well as their risks. More respondents were extremely aware of the risks associated with cookies (21%) than the benefits of cookies for users (14%).

	Functionality of Cookies]	Purposes of Cookies]	Benefits of Cookies to User]	Privacy Risks of Cookies to User]
Not at all Aware	7%	5%	7%	9%
Slightly Aware	23%	16%	27%	22%
Moderately Aware	30%	32%	23%	28%
Very Aware	25%	32%	30%	20%
Extremely Aware	16%	16%	14%	21%

Chart 1 - Awareness of Cookies among users

Influence of Benefits of Cookies towards Cookie Consent

To find out if the user's awareness level of cookie-related benefits motivates users to give cookie consent, crosstab analysis was done between awareness level of benefits of cookies and likeliness of accepting cookies under various categories of online activity as mentioned in the survey. These were: shopping, news media, corporate info, social media, banking and finance, healthcare and education. Chart 2 below shows there is no consistency of cookie acceptance levels across categories, even among users who have stated that they are extremely aware of the benefits of cookies.

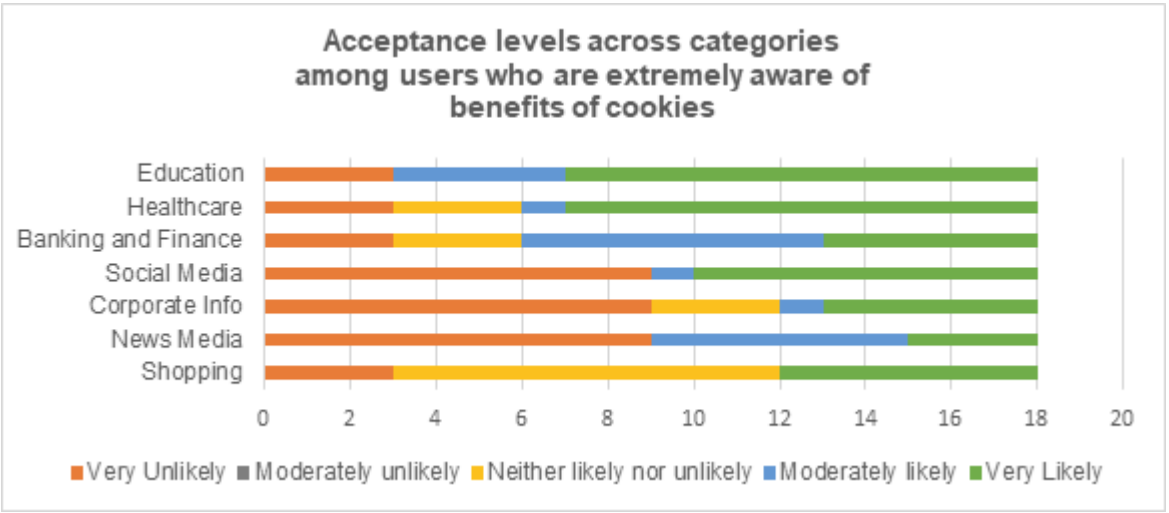

Chart 2: Acceptance Level of Cookies among Users

Influence of User Intent Towards Cookie Consent

To examine if user intent motivates the user to give cookie consent, the acceptance level for cookies across categories was plotted together in one single chart. Chart 3 below shows that there is no consistent level of cookie acceptance across different categories of online activities, which suggests that depending on the purpose of

usage, the acceptance level changes. More than 50% (Q4) of respondents' state that they were willing to accept cookies if it is necessary to complete the task in hand.

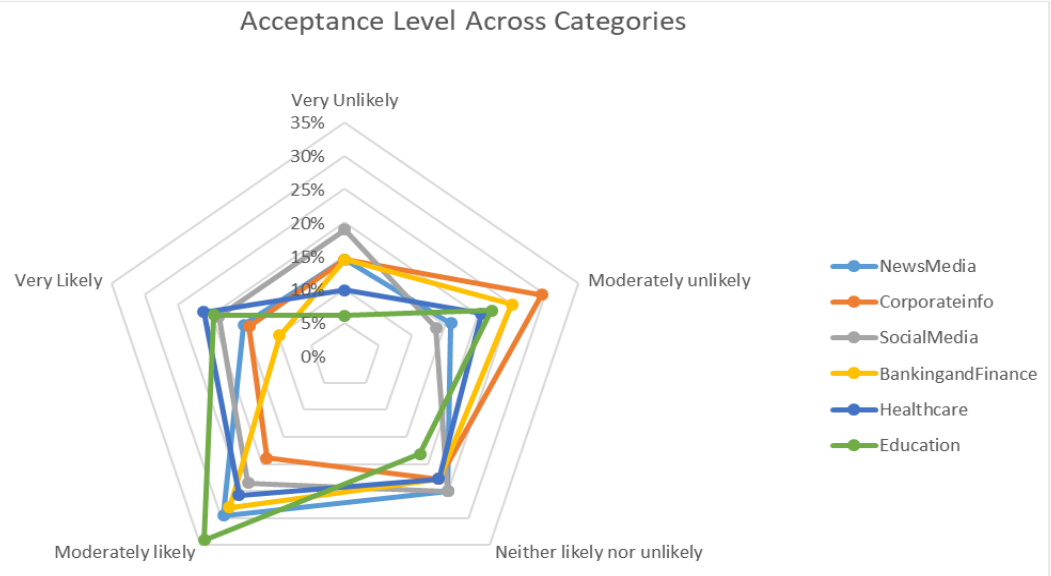

Chart 3: Acceptance Level of Cookies Across Categories

Influence of Brand Reputation towards Cookie Consent

Chart 4, below, is based on the results of a multiple-response question to ascertain the reasons that are likely to motivate the user to accept the cookies which were based on factors like brand trust, quick access, task completion, the regular user or repeat user and content quality. Brand trust and familiarity of the website came in as the third-most reason after quick access and task completion and got only about 40% of votes.

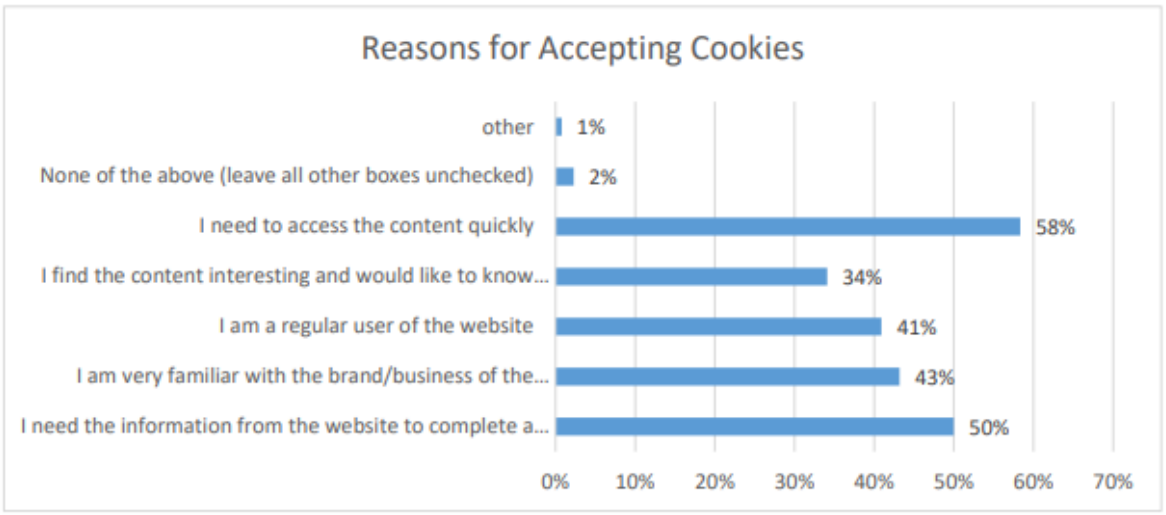

Chart 4: Reasons for Cookie Acceptance

Influence of Perceived Risk of Cookies towards Cookie Consent

Websites that deal with healthcare, finance, banking, education often called YMYL, Your Money or Your Life, websites (McCoy, 2016), often carry a higher risk rate and generally warrant more secure transactions. Chart 5, below, shows the acceptance levels across categories specifically among users who were extremely aware of the privacy risk of browser cookies. Based on the responses, there seems a considerable difference between users who are likely to accept cookies when it comes to education, healthcare and finance. If privacy risks influence cookie acceptance, then there should be a consensus when it comes to these categories as they deal with their health and finances.

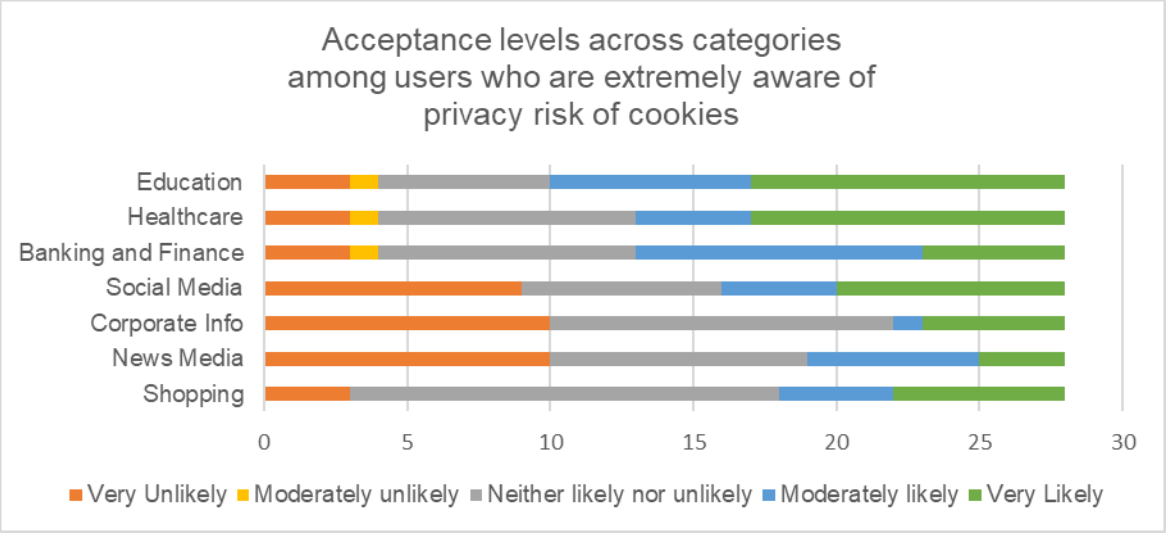

Chart 5: Acceptance Level of Cookies based on Perceived Risk by Users

Influence of User-Friendly Consent Mechanisms towards Cookie Consent

When the design preferences for the cookie banner are plotted in a radar map (refer to Chart 6), there is a clear skew towards opt-out option and managing data choices. Over 40% of respondents preferred cookie banner design with the opt-out option, followed by 31.8% of respondents preferring the option to choose how their data can be used by the website. Overall more than 88% of users wanted some level of choice in the cookie consent banner, to better manage their data choices.

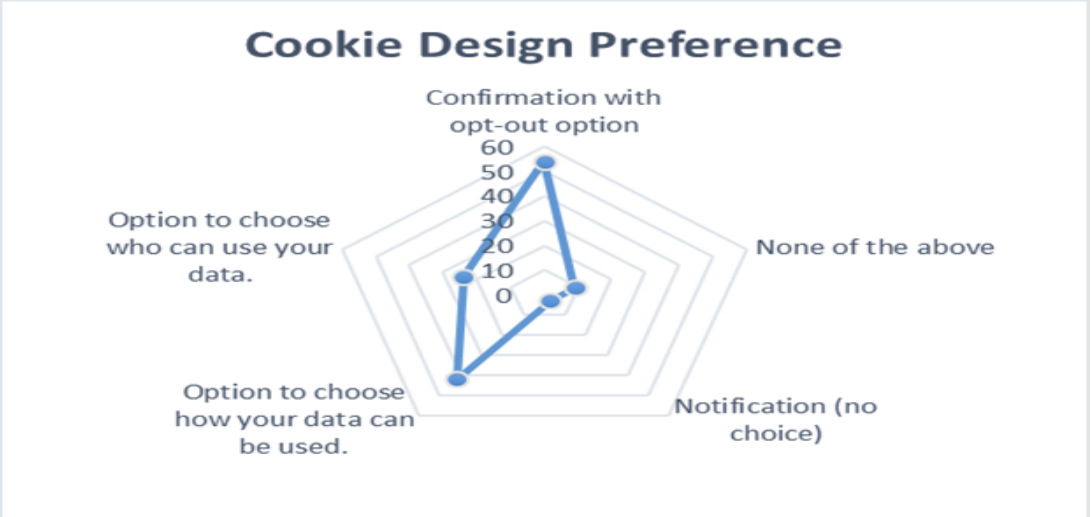

Chart 6: Cookie Design Preference among Users

The overall analysis of the survey results shows that different factors hada different type of influence on the cookie acceptance level of the users. Table1 below gives the summary of the findings on the relation between the independent variables (as per Figure 2) and the dependent variable of cookie acceptance.

Table 1: Influence of Factors on Cookie Acceptance

Objective Parameter	Influence on Cookie Acceptance	Remarks
Perceived Usefulness of Cookies	Very little or No Influence	Awareness of cookie benefits did not produce consistent acceptance levels
Perceived Ease of Use in setting Cookie Preferences	Negative Influence	A user-friendly cookie banner design is likely to increase the rate of opting out from cookies by users.
User Intent when visiting the website	Strong Influence	The purpose of visiting a website seems to play a significant role in acceptance rates which differs across different website categories
Perceived risk in accepting cookies	Very little or no Influence	No consensus among users in acceptance of high risk (e.g. Financial) and low risk (e.g. Corporate info)

Brand trust (Trust of the website owner)	Very little or No Influence	Not ranked among the important factors for cookie acceptance.

It is clear that user intent is the most influencing factor for the user to accept website cookies and given a choice, users are most likely to opt-out from accepting cookies.The other variables had very little or no influence on motivating the user for accepting cookies.

Discussion

The lack of awareness of the benefits of cookies (as shown in Chart1), raises some questions about the ideal level of awareness, and whether the users are informed enough to give consent to the cookies. Asking users to give consent without making sure if they know what they are giving consent to, is a problematic issue ethically and even legally in some cases. Website owners should take responsibility for making sure users have been presented enough information about cookies in simple and clear language on their data choices, before asking for their consent for cookie usage.

Even when users are aware of the benefits of cookies, they do not increase or decrease the acceptance rates of cookies(as shown in Chart 2). This indicates that there may be other factors like user intent, brand trust etc. which might also influence the users' cookie acceptance behaviour.

As shown in Chart 3, user intent does influence the acceptance rate of cookies, even if it's not the prime motivator. Depending on the purpose of the website and the intention of the user, the user is likely to accept or reject the cookies, given there are suitable provisions to manage their data choices.

As shown in Chart 4, the familiarity of the brand was voted as the third factor by users which impacts their decision in accepting cookies. Being a regular user of the website came in as the fourth factor influencing their cookie acceptance rate. This suggests that even if they are familiar with the brand, they may or may not accept cookies depending on the purpose of the website visit. When it comes to banking and finance, there was no consensus on the acceptance of cookies among users. It is highly unlikely that the user is carrying out a banking or financial transaction without being familiar with the website or lack of trust in the brand. So it is safe to assume, brand reputation or brand trust does not have a strong influence in convincing users to accept the cookies.

Interestingly, more users were unlikely to accept cookies when accessing a corporate website to get some general information, where the risk of privacy or security breach is very low (as shown in chart 5). Based on these patterns, it can be stated that the privacy risk of accepting cookies is not likely to influence the user to accept or reject all website cookies.

Among the various design choices given to the respondents, the majority of the users chose the cookie consent banner with a clear opt-out option (as shown in Chart 6). Users had previously cited the quick access to the website as one of the key factors in accepting cookies. However, the cookie banner with notification only design, which did not require any action from the users, and the banner design with just the 'accept' button which can be objectively quicker for users to accept cookies were among the least preferred. This indicates that users are likely to prefer a design that will help them opt out quicker, and whenever given a choice, users would rather opt-out from accepting cookies.This suggests that while a better design of a cookie consent banner has some benefits in user experience, it's not likely to increase the acceptance rate of cookies among users and most likely increase the opt-out rate of users.

Recommendations

The European Commission has been discussing stringent cookie consent laws,including standardising the language, consent banner design and accountability for managing data choices (Legroju, 2017). These changes were expected to come into effect in 2020. However,due to various delays such as BREXIT and Covid-19 crisis implementing these changes might at least take another year and an additional couple of years for it to be fully enforced.It is to be noted, advertisers are likely to move away from cookies to advanced technologies for tracking and advertising in the coming years, rendering the changes as inadequate and redundant.The cookie law and related directives seem to focus on the cookie technology itself, rather than obtaining consumer consent for using their data.

Based on the findings of this research, users simply are not interested in cookies or managing their cookie settings. Moreover, placing the burden on them to understand every aspect of the technology to give their informed opinion is unfair. The European Commission and other regulatory bodies should focus on developing a futureproof framework for targeting and advertising to website/internet users. This should help data protection agencies to keep up with the various technological advancements in the online advertising industry.

In addition to the existing cookie law, a new framework for obtaining user consent for advertising should be developed keeping the foundation principles of GDPR in mind. Such a framework will help developing directives to regulate organisations forgetting consent from users. This consent should apply to use customer data for advertising and marketing purposes regardless of the technologies they might employ to serve targeted ads.Organisations must maintain high levels of transparency of what data is being collected and the purposes they are used. They should also clearly display how users can opt-out of getting targeted ads, where possible..

Consent for Advertising Directive

To that effect, this study proposes a Consent for Advertising Directive (CAD) that can be incorporated with the current ePrivacy regulations (ePR). Figure 4, below, highlights the key points of the proposed framework to form the Consent for Advertising Directive (CAD) to increase transparency and obtain informed consent from users.

Figure 4: Framework for Consent for Advertising Directive (CAD)

Table 2, below, highlights the key points of differentiation between the existing ePrivacy Directive and the proposed Consent for Advertising Directive and the possible benefits of adopting and implementing CAD.

Table 2: Differences between existing ePrivacy Directive and proposed Consent for Advertising Directive

ePrivacy Directive (Cookie Law)	Consent for Advertising Directive
Focuses only on usage of cookies and cookie-related consent	Focus on user consent for all types of targeted advertising
Not Future Proof as 3rd party cookies are becoming obsolete	Future Proof as CAD focuses on consent rather than technology
Violations are mainly dealt with monetary penalties for web publisher	Violations will be dealt with a temporary and permanent suspension of ad vendor in addition to monetary fines to the web publisher
Can be circumvented easily through alternate mechanisms like device fingerprinting	Circumventing will be difficult as consent mechanism is not based on the technology used by the ad vendor for ad targeting
Does not cover mobile app targeted advertising.	CAD will cover all kinds of tracking and targeted advertising regardless of device, operating system, browser or other software.

CAD will not only strengthen the effectiveness of GDPR compliance but also help brands to avoid GDPR violations as the consumer consent obtained through the framework will be applicable for all types of advertising. Brands will benefit from a robust consent policy by becoming more transparent and removing any ambiguity of what the customers are giving their consent for. Engaging with the website users with more transparency will help brands to strengthen their consumer trust by championing the data protection rights of their customers.

Conclusion

Future of Online Advertising

Segmenting and targeting of prospective customers have always been in the foundation of advertising strategy (Kotler, 1984). Online Advertising has only made targeting more granular with the use of various web and mobile technologies that has benefited marketers to offer tailor-made advertisements at an individual level. Given their enormous success, it is unlikely that advertisers will scale back their efforts in profiling users to serve them in highly targeted ads. But just like with any advertising, consumer trust with the brand is key when it comes to conversion (Hoffman, Novak and Peralta, 1999).

If a consumer develops a negative perception towards the brand on how the brand handles their user data or becomes aware of them engaging in invasive practices, then all the personalised ads will not be able to help them to recover from that. Advertisers and web technology providers should develop technologies, processes and protocols with the consumer's right to data privacy at their core so that the industry is sustainable in the long-run.

Future of Cookies Technology

There is ample evidence to suggest that the European Commission has taken great strides in regulating the data protection rights of the consumer compared to their American or Asian counterparts (GDPR.EU, 2019). Amending the e-Privacy directive implementing GDPR has had an impact on organisations taking data privacy and security more seriously. However, there is also enough evidence that organisations are treating their GDPR efforts as a compliance issue. For them, especially the tech giants, it's yet another red tape to deal with, adding to the cost of doing business, instead of implementing effective measures with the true focus on their user data protection rights (Beckett, 2020).

The case against using third party cookies, which were considered invasive since their inception is now even stronger. Tech giants like Google, Apple and Microsoft who dominate the web browser market have already announced that they are committed to phasing out these cookies (Bohn, 2020). In a few years, it is conceivable that only essential cookies are being used and individual consent for every website visit may not be required at all. But that is only half the story. Ad giants like Google have already announced new technologies like Privacy Sandbox, that helps to track, measure and serve targeted ads without using cookies (Slefo, 2020). While Google says the data will be completely anonymous, unlike cookies which are simple text files, this new age tracking software is embedded within the browser, which makes it impossible for the user to make any choices or completely opt-out. There are also more worrying concerns that ad vendors who do not have a foot on the web browser market might resort to more opaque techniques like device fingerprinting that are much more invasive and much harder to opt-out when compared to cookies.

Future of Consent

On the surface, phasing out third party website cookies seem to resolve the issue of obtaining explicit cookie consent and related complications. However, it only leaves the users more vulnerable as they no longer have any option to manage their data choices. Given the technological changes in targeted advertising, user consent for managing their data must go beyond the domain of website cookies and related issues. Users should always have their privacy rights protected and have control over the types of data being collected from them, the purposes for which the data is used for and who will access the data. In other words, User consent for tracking, measurement and targeted advertising should move beyond cookie consent. To better protect consumer rights, consent should be taken from users for using their data regardless of the technology or mechanism used by the organisation, brand, or website owner. In addition to existing consumer data protection rights like Right to Privacy and Right to be Forgotten, it's time to include Right to Consent in all future data protection regulations in its various forms around the world.

Future Studies
Based on the findings of this research, there are further opportunities to explore consumer attitudes towards personalised ads, and what are the boundaries which consumers expect brands to maintain when employing targeted advertising. It will be interesting to study if there are various degrees of consent for various types of data usage. Additionally, it can be examined what type of data is the user comfortable sharing at different stages of the customer journey.

References

Beckett, P. (2020) '*GDPR: two years on*'. Available at: https://www.alvarezandmarsal.com/insights/gdpr-two-years (Accessed: 20 August 2020).

Boerman, S. C., Kruikemeier, S. and Zuiderveen Borgesius, F. J. (2017) 'Online behavioral advertising: a literature review and research agenda', *Journal of Advertising*, 46(3), pp. 363–376. https://doi.org/10.1080/00913367.2017.1339368.

Bohn, D. (2020) '*Google to 'phase out' third-party cookies in Chrome, but not for two years*'. Available at: https://www.theverge.com/2020/1/14/21064698/google-third-party-cookies-chrome-two-years-privacy-safari-firefox (Accessed: 20 August 2020).

Capgemini Research Institute (2019) *'Championing data protection and privacy: a source of competitive advantage in the digital century'*. Available at: https://www.capgemini.com/wp-content/uploads/2019/09/Report_Championing-Data-Protection-and-Privacy.pdf (Accessed: 4 April 2020).

Cavoukian, A. (2010) '*Privacy by design: the 7 foundational principles*'. Available at: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/ (Accessed: 20 August 2020).

Chapman, S. and Dhillon, G. S. (2002) 'Privacy and the internet: the case of the DoubleClick, Inc.', in Chapman, S. and Dhillon, G.S. (eds.) *Social Responsibility in the Information Age: Issues and Controversies*. IGI Global, pp. 75–88.

Chellappa, R. and Sin, R. (2005) 'Personalization versus privacy: an empirical examination of the online consumer's dilemma', *Information Technology and Managemen*t, 6, pp. 181–202. https://doi.org/10.1007/s10799-005-5879-y.

Cofone, I. N. (2016) 'The way the cookie crumbles: online tracking meets behavioural economics: Table A1', *International Journal of Law and Information Technology*, 25(1), pp. 38-62. https://doi.org/10.1093/ijlit/eaw013.

Cranor, L. F., Byers, S. and Kormann, D. (2003) *An analysis of P3P deployment on commercial, government, and children's web sites as of May 2003*. Washington, DC: Federal Trade Commission.

Data Protection Commission (2020) *Report by the Data Protection Commission on the use of cookies and other tracking technologies*. Available at: https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Report%20by%20the%20D

PC%20on%20the%20use%20of%20cookies%20and%20other%20tracking%20technologies.pdf (Accessed: 28 June 2020).

Davis, F. D. (1989) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', *MIS Quarterly*, 13(3), pp. 319-340. https://doi.org/10.2307/249008.

Engberg, S. (2015) 'When Consent does not make sense, Security by Design must be required', *FUTURIUM - European Commission*. Available at: https://ec.europa.eu/futurium/en/content/when-consent-does-not-makes-sense-security-design-must-be-required (Accessed: 18 August 2020).

GDPR.EU (2019) *GDPR fines after one year: key takeaways for businesses.* Available at: https://gdpr.eu/gdpr-fines-so-far/ (Accessed: 3 April 2020).

Hoban, P. R. and Bucklin, R. E. (2015) 'Effects of internet display advertising in the purchase funnel: model-based insights from a randomized field experiment', *Journal of Marketing Research*, 52(3), pp. 375–393. https://doi.org/10.1509/jmr.13.0277.

Hoffman, D., Novak, T. and Peralta, M. (1999) 'Building consumer trust online', *Communications of the ACM*, 42, pp. 80–85. https://doi.org/10.1145/299157.299175.

Jarvenpaa, S., Tractinsky, N. and Vitale, M. (2000) 'Consumer trust in an internet store', *International Journal of Information Technology and Management*, 1, pp. 45-71. https://doi.org/10.1023/A:1019104520776.

Jutla, D. and Bodorik, P. (2005) 'Sociotechnical architecture for online privacy', *IEEE Security & Privacy*, 3(2), pp. 29–39. https://doi.org/10.1109/MSP.2005.50.

Kotler, P. (1984) *Marketing Essentials*. Hoboken, N.J.: Prentice-Hall.

Kurtz, C., Semmann, M. and Bã, T. (2018) 'Privacy by design to comply with GDPR: a review on third-party data processors', *AMCIS 2018*.

Lai, P. (2017) 'The literature review of technology adoption models and theories for the novelty technology', *Journal of Information Systems and Technology Management*, 14(1), pp. 21-38. https://doi.org/10.4301/S1807-17752017000100002.

Lardinois, F. (2020) 'Google wants to phase out support for third-party cookies in Chrome within two years', *TechCrunch*, 14 January. Available at: https://social.techcrunch.com/2020/01/14/google-wants-to-phase-out-support-for-third-party-cookies-in-chrome-within-two-years/ (Accessed: 29 June 2020).

Lee, P. (2011) 'The impact of cookie "consent" on targeted adverts', *Journal of Database Marketing & Customer Strategy Management*, 18(3), pp. 205–209. https://doi.org/10.1057/dbm.2011.20.

Leenes, R. (2015) 'The Cookiewars – from regulatory failure to user empowerment?', in van Lieshout, M. and Hoepman, J-H. (eds.) *The Privacy & Identity Lab: 4 years later* (pp. 31-49) The Privacy & Identity Lab.

Legroju (2017) *Proposal for an ePrivacy Regulation*. Brussels: European Commission. Available at: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (Accessed: 3 April 2020).

Marcus, A. (ed.) (2016) *Design, User Experience, and Usability: Design Thinking and Methods*. 5th International Conference, DUXU 2016, Held as Part of HCI International 2016, Toronto, Canada, July 17–22, 2016, Proceedings, Part I. Springer.

McCoy, J. (2016) 'EAT, YMYL, & Beneficial Purpose: what do Google's quality standards mean for search?', *SEMrush Blog*, 26 September. Available at: https://www.semrush.com/blog/eat-and-ymyl-new-google-search-guidelines-acronyms-of-quality-content/ (Accessed: 15 October 2020).

McStay, A. (2013) 'I consent: an analysis of the Cookie Directive and its implications for UK behavioral advertising', *New Media & Society*, 15(4), pp. 596–611. https://doi.org/10.1177/1461444812458434.

Poole, B. (2019) 'Welcome to the end of digital marketing', *Think with Google*. Available at: https://www.thinkwithgoogle.com/marketing-resources/data-measurement/digital-marketing-mindset/ (Accessed: 8 November 2019).

Porter, M. E. (1996) 'What Is strategy?' *Harvard Business Review*, 74(6), pp. 61-78.

Rogers, D. L. (2016) *The Digital transformation playbook: rethink your business for the Digital Age*. New York: Columbia University Press.

Ross, J. (2014) *The business value of user experience.* Available at: http://www.infragistics.com/media/335732/the_business_value_of_user_experience-3.pdf (Accessed: 24 June 2020).

San, M. S. and Camarero, C. (2009) 'How perceived risk affects online buying', *Online Information Review*, 33(4), pp. 629–654. https://doi.org/10.1108/14684520910985657.

Saunders, M., Lewis, P. and Thornhill, A. (2019) *Research methods for business students*. 8th edn. Harlow: Pearson Education.

Schmidt-Subramanian, M. (2014) 'The business impact of customer experience, 2014', Available at: http://resources.moxiesoft.com/rs/moxiesoft/images/Business_Impact_Of_CX_2014.pdf (Accessed: 8 November 2019).

Schofield, J. (2018) 'What should I do about all the GDPR pop-ups on websites?', *The Guardian*, 5 July. [Online]. Available at: https://www.theguardian.com/technology/askjack/2018/jul/05/what-should-i-do-about-all-the-gdpr-pop-ups-on-websites (Accessed: 4 April 2020).

Slefo, G. P. (2020) 'Behind Google's decision to remove third-party cookies from Chrome', *AdAge*, 14 January. Available at: https://adage.com/article/digital/behind-googles-decision-remove-third-party-cookies-chrome/2227126 (Accessed: 20 August 2020).

Stewart, H. and Jürjens, J. (2018) 'Data security and consumer trust in FinTech innovation in Germany', *Information and Computer Security*, 26(1), pp. 109-128. https://doi.org/10.1108/ICS-06-2017-0039.

Trevisan, M., Traverso, S., Bassi, E. and Mellia, M. (2019) '4 Years of EU Cookie Law: results and lessons learned', *Proceedings on Privacy Enhancing Technologies*, 2019(2), pp. 126–145. https://doi.org/10.2478/popets-2019-0023.

Ur, , Leon, P.G., Cranor, L.F., Shay, R. and Wang, Y. (2012) 'Smart, useful, scary, creepy: perceptions of online behavioral advertising', in Proceedings of the Eighth Symposium on Usable Privacy and Security. Washington, D.C.: ACM Press, p. 1. https://doi.org/10.1145/2335356.2335362.

Venkatesh, V. and Bala, H. (2008) 'Technology Acceptance Model 3 and a research agenda on interventions', *Decision Sciences,* 39(2), pp. 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x.

Walport, M. and Thomas, R. (2008) Data sharing review report. Available at: https://amberhawk.typepad.com/files/thomas-walport-datasharingreview2008.pdf (Accessed: 11 October 2020).