Dissertation submitted in partial fulfilment of the requirements for the degree of M.Sc. in Digital Marketing at Dublin Business School

Cookies ‘n’ Consent:
An empirical study on the factors influencing customer attitudes towards cookie consent among internet users in EU.

SUPERVISOR: EVA PEREZ

STUDENT NAME: LAKSHMI NARAYANAN

STUDENT NUMBER: 10526790
Declaration

I, Lakshmi Narayanan, declare that this research is my original work and that it has never been previously presented to any institution or university for the award of Degree or Diploma. Also, I have referenced correctly all literature and sources used in this work and this work is fully compliant with the Dublin Business School’s academic honesty policy.

Signature: [Signature]

DBS Student Number: 10526790

Date: 24.08.2020
Acknowledgement

I would like to thank my dissertation supervisor Eva Perez for her unparalleled support, guidance and encouragement throughout this research. Her prompt and specific feedback helped in improving the overall quality of the study.

Next, I would like to express my appreciation towards all the lecturers and supporting staff of Dublin Business School for their constant support and knowledge sharing throughout this Master’s Degree. The learning environment and resources provided by Dublin Business School were extremely motivating for successfully completing the course especially during the Covid-19 Crisis.

I am also grateful for the respondents who participated in the study for their valuable time and inputs. Finally, I would like to thank my family and friends for believing in me and encouraging me at every step of my life. This dissertation is dedicated to all these inspiring people.
Abstract

The study aimed to understand user perception towards website cookie banners, which are mandatory under GDPR and the factors which are likely to influence their consent for accepting all cookies, to develop recommendations to improve consent mechanisms. 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 the majority of respondents had more than moderate level of awareness about cookies and are more likely to accept cookies for quick access or task completion. Acceptance of cookies was varied across different categories of online activity and given a choice they are more likely to opt-out of 3rd party cookies which is widely used for targeted advertising. This study proposes a framework for Consent for Advertising Directive (CAD) to go beyond the existing Cookie Law which will improve user data protection, and help brands to improve transparency and avoid GDPR violations.
# TABLE OF CONTENTS

1. **INTRODUCTION** ........................................................................................................... 8

   1.1. Growth Of Online Businesses .................................................................................. 8

   1.2. Online Behavioural Advertising ............................................................................. 8

   1.3. Third-Party Cookies ............................................................................................... 9

   1.4. Privacy ................................................................................................................... 9

   1.5. GDPR Regulations ................................................................................................. 9

   1.6. Need For Consent: ............................................................................................... 10

   1.7. User Experience: .................................................................................................. 10

   1.8. Future Of Cookies And GDPR Policy: ................................................................. 11

2. **RESEARCH AIM** ....................................................................................................... 13

   2.1. Research Questions And Objectives ..................................................................... 12

   2.2. Research Significance .......................................................................................... 13

3. **LITERATURE REVIEW** ............................................................................................ 14

   3.1. User Experience And Competitive Advantage ..................................................... 14

   3.2. Technology Acceptance Model ............................................................................ 14

   3.3. Pact Analysis For Ux Design ................................................................................ 16

   3.4. Building Consumer Trust And Mitigating Risk ................................................... 16

   3.5. Introduction Of GDPR ......................................................................................... 18

   3.6. Principles Of GDPR: .......................................................................................... 19

   3.7. Aftermath Of GDPR ............................................................................................ 20
6. **FINDINGS AND DISCUSSION** ........................................................................................................51

6.1. Objective A: To Evaluate The Awareness Level Of Online Users About Cookies. ..................51

6.3. Objective C: To Examine If User Intent Motivates The User To Give Cookie Consent. .......53

6.4. Objective: To Investigate The Influence Of Brand Reputation In Getting Cookie Consent...54

6.5. Objective: To Examine If Perceived Risk Of Cookies Influences Users In Giving Consent.....54

6.6. Objective: To Investigate If User-Friendly Mechanisms Motivate User To Give Consent....55

6.7. Summary Of Findings And Analysis ..................................................................................................................57

7. **CONCLUSION AND RECOMMENDATIONS** ..........................................................................................58

7.1. Future Of Cookies Technology.......................................................................................................................58

7.2. Future Of Consent: ........................................................................................................................................59

7.3. Future Of Online Advertising: .......................................................................................................................59

7.4. Recommendations For Managing User Consent ..........................................................................................60

7.5. Limitations And Future Research Opportunities .........................................................................................62

8. **BIBLIOGRAPHY** ........................................................................................................................................63

9. **APPENDIX** .................................................................................................................................................67

Appendix 1: Questionnaire ...............................................................................................................................67

Appendix 2: Spss Output.....................................................................................................................................72
1. Introduction

1.1. Growth of Online Businesses

The internet boom in the late 1990s led to the digital revolution which saw the emergence of a wide variety of online businesses. In the past decade, the distinctions between online and traditional businesses have been getting blurred with every type of organisation/industry going through a digital transformation. The lines between traditional marketing and digital marketing have now disappeared. (Poole, 2019) With every business having an online/digital touchpoint, online user experience is not something that can be ignored or discounted, even with varying levels of priority across industries. More often than not, customers 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 consideration to conversion stage. (Hoban and Bucklin, 2015)

1.2. Online Behavioural Advertising

Businesses also use online advertising in moving the customers though the goal funnel. One of the major components of online advertising is Online Behavioural Advertising (OBA), which is defined as the practice of monitoring people's online behaviour and using the collected information to show people individually targeted advertisements. (Boerman, Kruikemeier and Zuiderveen Borgesius, 2017).

Website owners partner with advertising partners often referred to as vendors who use cookies, which are text files placed in the user devices to identify and track their online activity even after they exit the original website. This helps them track the different websites the user is visiting and based on consumer interest, suitable ads will be shown on partner websites. This helps advertisers to target customers who are already interested in the product or service which makes the conversion much easier as they address their immediate needs for products and services (Ur et al., 2012).
1.3. Third-Party Cookies

Online Behavioural Advertising has always been contentious when it comes to user privacy as it requires the usage of third-party cookies. While the website owner uses First party cookies to track the website activity of the website visitor (2nd party) for analytics purposes, oftentimes, a third party who is an advertising partner or Ad Vendor places additional cookies to track the user behaviour even after they exit the original website. These third-party cookies have been recognised as a privacy threat since their inception (McStay, 2013).

1.4. Privacy

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

1.5. GDPR Regulations

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 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 35000 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. 74% of websites install third part cookies before any user consent. (Trevisan, Traverso, Bassi, 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-standardization implementation of ePrivacy directive among EU nations, enforcement failures, lack of awareness among users and the general public. (Cofone, 2016) (Leenes, 2017)
1.6. Need for Consent:

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 gets an acknowledgement from users that cookies are being used. In a 2008 report presented to the UK Prime Minister and the Secretary of State for Justice, Thomas and Walport (2008) presented the difference between genuine consent and enforced consent. They explain consent cannot be passive, but active. The user is required to do something to give consent, a non-response cannot be taken as genuine consent.

1.7. User experience:

In September 2010, Neelia Kroes, the EU Commissioner for the Digital Agenda, called for the middle way between consumer protection and commercial pragmatism, emphasizing 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 Ireland DPC released a report in April 2020 on Cookies and other tracking technologies, revealing the fact that not much progress has been made in the last decade in finding the middle way. The report highlights the presence of badly designed, even deliberately deceptive, cookie banners and consent management tool among prominent sites. It also sheds light on dark patterns used by certain Consent Management Platforms like Quantcast which uses cookie banner interfaces which are deliberately confusing and have pre-checked boxes and sliders before any action taken by the user. (Data Protection Commission, 2020)

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 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 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 increased need for training (Ross, 2014).

1.8. Future of cookies and GDPR policy:
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 it will phase them out in the next 2 years. (Lardinois, 2020). This is not to say they will not be tracking the online behaviour, they might use some other tracking technologies and if they will be less intrusive and how it 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, which is expected to bring in more standardization and enforcement regarding cookie policy and obtaining cookie consent.
2. Research Aim

Even if third-party cookies become obsolete soon, there are already other alternatives through which customer can be tracked and their data being used by ad vendors. It will not be hyperbole to predict, that the e-privacy directive will catch up quickly to bring in regulations to curb the different technologies which deal with customer data. Several conversations are going on between EU commission, Data protection agencies, business & websites owners and Ad vendors regarding the cookie policy, obtaining consent, data collection and its usage. One of the key stakeholders who is the user of the websites, whose privacy is in question seems to be left out from the conversations. The main aim of the study is to find the motivation factors which will encourage customers to give out 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.

2.1. Research Questions and Objectives

2.1.1. Main Research Question:

What are the external factors influencing customer attitude towards cookie consent?

2.1.2. Sub-questions and objectives:

A. Question: Are users familiar with cookies and it’s perceived benefits?
   Objective: To evaluate the awareness level of online users about cookies.

B. Question: Are users more likely to accept cookies if they know its benefits?
   Objective: To examine if the usefulness of cookies motivates the user to give cookie consent.

C. Question: Are users more likely to accept cookies if it helps them achieve their task?
   Objective: To examine if user intent motivates the user to give cookie consent.

D. Question: Are users more likely to accept cookies if they trust the brand/business?
   Objective: To investigate the influence of brand reputation in getting cookie consent from users.
E. Question: Are users more likely to accept cookies if they don’t feel it’s risky to their privacy or security?
   Objective: To examine if the perceived risk of accepting cookies influences users in giving consent.

F. Question: Are users likely to accept cookies, the privacy controls are better designed to give consent?
   Objective: To investigate if the user-friendly consent mechanisms motivate the user to give cookie consent.

2.2. Research Significance

While there are existing studies on the impact of cookie-popup, the data was collected through automated systems and browser engines (Nouwens et al., 2020). Collecting feedback directly from users about their perception of about the cookie-popups will help to generate better insights on the customer pain points which can be helpful for companies to adopt a user-friendly approach for obtaining cookie consent. As of May 2020, stricter ePrivacy regulations are under review (Legroju, 2017), which are likely to come into effect by 2021. This allows businesses to get ahead of the privacy and consent issues by considering alternative options and redesign their cookie consent delivery process by reviewing customer motivations to encourage users to give consent for the cookies. This will help online businesses significantly, especially which are depended on the website traffic like news media websites, e-commerce websites, social media and entertainment websites (Schofield, 2018).
3. Literature Review

3.1. User experience and competitive advantage

The term User Experience in the modern world was first cited in a conference paper about Human Interface at Apple Computers. (Norman, Miller and Henderson, 1995). User Experience can be defined as the combination of emotions, feelings, thoughts and sensations users experience while engaging in an activity. (Benyon, 2019). In a business context, user experience can have a significant impact on the value chain of product, service or a system (Marcus, 2016) and according to Porter M.E., improving the value chain is one of the strategies through which businesses can achieve competitive advantage (Porter, 1996).

3.2. Technology Acceptance Model

The Technology Acceptance Model suggests that there are 2 main factors for adoption of technology, one being the Perceived Usefulness (PU) and the other being Perceived Ease of Use (PEOU) (Davis, 1989). The model was later extended as TAM2 to include social influence processes (subjective norm, voluntariness, and image) and cognitive instrumental processes (job relevance, output quality, result demonstrability, and perceived ease of use) (Venkatesh and Davis, 2000) and further expanded to develop a more integrated model known as TAM3 (Venkatesh and Bala, 2008) which included the determinants of perceived ease of use which include Computer Self-Efficacy, Perception of External Control, Computer Anxiety, Computer Playfulness, Perceived Enjoyment, Objective Usability.

As TAM3 became more comprehensive, it has been criticized for having too many variables which do not have a significant impact on each other (Bagozzi, 2007). However, it is still used as the general framework for many studies and has been found consistent with many studies of the factors influencing the adoption of new technology.
A 2018 empirical study on the adoption of financial technology (FinTech) in Germany, confirms that data security, customer trust and user design interface, influence the adoption rate of FinTech very much in line with the Technology Acceptance Model. (Stewart and Jürjens, 2018).

One could argue that 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, could increase trust among users for safer online user experience.
3.3 PACT Analysis for UX Design

Designing a User Experience can be done effectively through a PACT analysis which comprises of the people who will be using the system, the activities they intend to perform in the system, the context under which the activities are performed and the technologies involved in carrying out those activities. (Benyon, 2019).

Systems which are designed following the PACT framework, ensure all the PACT elements fit together seamlessly thus ensuring a delightful user experience. They also help in scoping out the design problem and solving them keeping in mind the ethical standards are met. (Marcus, 2016).

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).

3.4 Building Consumer Trust and Mitigating Risk

The most effective way for e-businesses to build long term customer relationships is by earning the trust of its consumers. Customers who do not trust a brand or have prior experience with the brand is unlikely to buy the brand online (Chen Yu-Hui and Barnes Stuart, 2007). This online trust of customers towards the brand depends on various factors like online security, privacy policies, website design and presentation which influences the online experience of customers towards the brand. (Hoffman, Novak and Peralta, 1999).

The Online Buying Persuasion (OBP) model (San and Camarero, 2009) illustrates how cognitive signals are used by brands to increase the satisfaction level of customers which helps in building customer trust towards the brands.
Brands can create awareness among customers by establishing cognitive signals like security and privacy policies which help to increase the likelihood of customers transacting with the brand online (San and Camarero, 2009). The relationship of design and security and their influence on customer intention to transact online is illustrated by the Stimulus Theoretical Framework (STF) (Help University, Malaysia and Lai, 2017) which also explains how Perceived Usefulness and Perceived Ease of Use impacts customer motivations in their online transactions.
Based on the above-mentioned frameworks, it is can be seen 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 Bä, 2018) is likely to influence customer perception and trust towards the brand which in turn increases the likelihood of them transacting with the brand online.

3.5 Introduction of GDPR

Around the beginning of 2010s, high-speed internet and smartphones were becoming mainstream (Cisco, 2010) which prompted businesses across the globe to undergo a digital transformation to adapt their business models and value propositions in the new digital era where electronic communication devices were ‘always connected’ (Berman, 2012). Companies soon realised it is inevitable that data will become one of their most valuable assets to preserving their competitive advantage (Rotella, 2012).

To gain and preserve their competitive advantage, the business started adopting the approach of data-driven decision making, (McKinsey Global Institute, 2016), which involved ramping up their data analytics efforts more aggressively, which eventually led to the era of Big Data (Columbus, 2016).

Given that the 1995 Data Protection Directive was outdated (Rossow, 2018) and the lack of uniformity of data protection laws among the member states of the European Union, compliance issues started to increase as businesses started to accelerate their data collection and analytics.

In efforts to better regulate the data privacy issues, the European Commission unveiled the updated set of data protection laws called General Data Protection Regulation (GDPR) in April 2016 to. The purpose of GDPR was to ‘... facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations while ensuring a high level of the protection of personal data.’ (European Parliament and Council of the European Union, 2016). GDPR is considered the most consequential when it comes to data protection regulations and came into enforcement on 25 May 2018, two years after it was adopted (Hoofnagle, Sloot and Borgesius, 2019).
According to a 2017 Deloitte report, there were 8 key changes in the updated version of GDPR, which included Explicit and retractable Consent and Privacy by Design.

The report highlights there was a ‘significant shift in the role of consent’ which was to be obtained by organisations demonstrating that they were ‘freely given, specific, informed and unambiguous’ and Privacy by Design (PbD) is now integral to GDPR which requires a high-level organisational mindset change, which will have privacy built-in in the design, build and deployment of new technologies, process and protocols (Danon, 2017).

3.6 Principles of GDPR:

There are 7 foundation principles as stated in Article 5 of GDPR based on which the various regulations were developed (Principles of Data Protection | Data Protection Commission, 2016).

1. Lawfulness, fairness, and transparency: Personal data must be always processed fairly and lawfully. Organisations must communicate transparently about the data processing to the Individuals whose data are being processed in easy to understand, plain language.
II. **Purpose Limitation**: Organisations must explicitly state the specific purposes of the data collection and processing. The data cannot be used for purposes not stated or communicated to the individuals during the time of the data collection with an exception of historical research or statistical purposes.

III. **Data Minimisation**: Organisations should not collect personal data more than required for fulfilling the customer’s requirement. Any personal data considered irrelevant to serve customers purposes cannot be stored by the organisation in other words they should be limited to a strict minimum.

IV. **Accuracy**: Data controllers must make sure all personal data are kept up to date with reasonable accuracy. Organisations must have process and protocols set up to ensure the accuracy of data collected and stored and any outdated data must be removed or corrected without any delay.

V. **Storage Limitation**: Appropriate time limits must be set and followed for storing personal data. The time frame should be determined based on the type of data and their usefulness in serving customer purposes.

VI. **Integrity and confidentiality**: Personal data must be collected, processed and stored with appropriate security to ensure confidentiality of data is maintained and that the data is protected from any unauthorised access, theft or destruction using technical process and organisational policies.

VII. **Accountability**: Organisations who operate as data controllers are held accountable for handling personal data and it’s their responsibility to maintain records and adhere to data policies in compliance of GDPR. In case of a data breach, data controllers will be held responsible to investigate, communicate and ultimately rectify the vulnerability within an appropriate time frame.

3.7 **Aftermath of GDPR**

Within the first year of enforcement of GDPR, about 206,326 cases of privacy violations were reported according to The European Data Protection Board (EDPB) (GDPR.EU, 2019b). Hundreds of companies including tech giants like Google and Facebook found in violation and raked up fines up to €114 million within the first 20 months.
Even though the bulk of the fines were from the major tech companies, most of them treated these fines as rounding errors (gdpr.eu, 2020), on the other hand, the small and medium businesses were affected most even though the fines were relatively smaller since they were the most vulnerable due to their inherent resource limitations especially when it comes to people and technology dedicated for data compliance.

According to the 2019 GDPR Small Business Survey, close to half of the respondents (44%) said they were not confident with their GDPR compliance even while acknowledging that one time fine can be a fatal blow to them (GDPR.EU, 2019a).

However, on a positive note, the majority of the respondents (86%) who were business leaders said they have the corporate buy-in to prioritise their efforts to achieve total compliance for a multitude of reasons like statutory compliance, to avoid fines, to protect data and to uphold the right to privacy (GDPR.EU, 2019a).

### 3.8 Impact of GDPR in Online Behaviour and Consumer Awareness

An earlier research study on the impact of GDPR on European Web Traffic & e-commerce (Goldberg, Johnson and Shriver, 2019), concluded there was no considerable impact by GDPR enforcement on user behaviour. The study was based on internet user data which measured the standard web performance metrics like time duration per visit and page views per visit collected between late Jan to mid-Sep 2018 (to avoid the shopping period) and was compared with 2017 data for the same period. It is to be noted that even though GDPR was adopted in 2016, the enforcement effect came into effect in May 2018 and the study does not specify whether the analytics data used in came from GDPR compliant websites.

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). This could also mean that the Adobe Analytics data used in European Web Traffic & e-commerce study (Goldberg, Johnson and Shriver, 2019) could have very much from sites which were not fully GDPR compliant and hence the there was no impact of GDPR on the online user behaviour.
As per a recent survey among European car consumers, 83% had a general awareness of GDPR, but only about 30% of the users were aware of how GDPR applies to individuals and benefits for the same. However, the study was about GDPR awareness concerning connected smart cars which had data collection touchpoints and not about online user experience or behaviour.

3.9 Website cookies and its types:

To identify and track individual users who use the website, text files are commonly known as Cookies onto a user’s hard drive and depending on the configuration, they can reside there for days, months or years. (Bayan, 2001). Since their inception, cookies have been a cause of concern (Cranor, Byers and Kornmann, 2003), even though their usage is not a direct violation as many websites require cookies to function properly, especially in situations where personalized website experience is provided or 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). While this kind of activity tracking by the website to provide better user experience, is not invasive, the collection and usage of such data for other purposes which are not directly concerning the user activity, constitutes an invasion of privacy. (Miyazaki, 2008).

Marketers have long been using cookies to profile the users based on devices, location, language and their corresponding online activity to create better product offerings.
(Caudill and Murphy, 2000). With the advent of online advertising, these cookies were used for tracking, collecting user data and activity to serve highly targeted ads to users. The success of those ads has made ad vendors and online businesses more aggressive in their user data collection and activity tracking.

This has led to a surge in the use of third-party cookies which are cookies installed by third-party servers from a different domain such as a Content Delivery Network (CDN) who are not the website owners (First party) (Trevisan, Traverso, Metwalley, et al., 2019). This surge without any checks or regulations has led to a huge scale of privacy violations from deceptive use of cookies, unauthorised collection and sharing of user data, tracking without consent etc. (Berghel, 2002)

3.10 Purposes of Cookies:

While technically Cookies work in the same way, they can be configured for multiple purposes. The various purposes can be roughly classified to 4 main groups (Machuletz and Böhme, 2020) namely,

a) Necessary – These are cookies essential for the website to function properly. They are configured by the website owner to make sure the user can have a stable user experience. Websites usually need consent from the user, for using these cookies, but they need to inform the user about the usage and its purposes.

b) Preferences – These are cookies which are used to personalize the browsing experience for the individual user by remembering their websites preferences such as login information, form data for auto-fill, language preferences and other user settings. These set of cookies tend to be the most beneficial to the users as they enhance the user experience with the website.

c) Statistics – These are cookies used by the website directly or through a third-party (e.g. Google Analytics) to measure different types of user browsing activity for analytics like the number of visitors to the website, page views, link clicks, location, device, language, duration of visit, entry and exit pages etc. These cookies may not benefit the user, but are very beneficial for the website owner
to understand the browsing behaviour of users which help in generating insights to optimize the website further in terms, design, content and technology.

d) Marketing – These are cookies often configured by Third-party ad vendors (allowed by website owners), to collect multiple data points of user activity similar to the statistical cookies, but use those data points to create detailed user profiles, based on which users are served highly targeted ads which generate advertising revenue for the website owners and ad vendors. These cookies are considered the most invasive when it comes to the online privacy of users. (Ackerman, Cranor and Reagle, 1999)

3.11 **Cookie Concerns and Consent Regulations:**

As the online advertising grew more and more, the usage of third party cookies for marketing purposes became increasingly aggressive, which caused concern among European Union which termed these cookies are being used in violation of their Data protection directive issued in 1995. In 2009. This directive was amended to discipline organisations and regulate their cookie usage. The directive demanded, 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.

3.12 **Impact of Cookie Consent Pop-up:**

To comply with the EU directive, websites started using cookie consent pop-ups or banners to inform the users about cookie usage. A 2008 study shows that consumer trust among adult online shoppers decreased when the detection of cookie usage and data collection was found. However prior disclosures over cookie usage, especially under high-risk conditions enhanced trust. (Miyazaki, 2008).

Since 2009, Cookie consent notifications have been mandatory and this was expected to have a significant impact on the usage of third-party cookies and behavioural advertising. (McStay, 2013).
However recent audits have shown, cookie pop-ups have not impacted the advertising industry in the EU region as much as expected. Majority of the websites are in direct violation of the cookie law and very few websites have become fully GDPR compliant. The handful of major online ad vendors are responsible for the use of third-party cookies in the majority of websites. Google, arguably the biggest online ad vendor, is alone responsible for 20% of violation cases. The 2019 Study of 4 years shows the percentage of privacy violations have stayed the same, even after GDPR became enforceable in 2018 (Trevisan, Traverso, Bassi, et al., 2019). This shows the ineffectiveness of the cookie law and its enforcement and the need for better approaches to protect consumer privacy.

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 of the instances, the cookie banner did not affect the installation of cookies, the privacy controls were either buried deep or unnecessarily complicated. It is not clear whether these dark patterns in the design are the result of poor user design or thy are being intended to be deceptive to confuse the user for consent. (Nouwens et al., 2020). Either way, it is clear that compliance has not being taken seriously because of various factors notably, the non-standardization of the cookie law among the EU region and lack of enforcement by Data Protection Commission for cookie law violations.

### 3.13 Cookie Banner design and user behaviour

Since their introduction, the cookie consent banner did not have any standardisation, some banners merely served as notification without getting explicit consent from users which violated the EU privacy directive. Due to the lack of standardisation and non-uniformity among the EU member states, compliance in getting cookie consent was hard to come by (Lee, 2011).

A 2020 user study of cookie consent dialogs, provides empirical evidence that seems to prove that the cookie banners are designed in a deliberate way to deceive users into accepting cookies (Machuletz and Böhme, 2020), which is in accordance to the dark patterns mentioned in the CMP study cited earlier (Nouwens et al., 2020).
The user study confirms that design elements used in the cookie consent banners and pop-ups, like colours, position, toggle switches, slider design etc. influence the user behaviour in accepting or rejecting cookie consent.

3.14 Cookie Consent and Compliance:

There are enough reports and studies which have enough guidelines on the proper way to design the cookie consent mechanism. Phil Lee, an expert in online privacy and digital regulation, in his 2011 journal article, identified 7 practical measures website owners can take to mitigate risk when serving cookies for targeted advertising which included,

a) Identifying the cookies served by the websites to assess the number, identity, purpose and duration of cookies served. This will increase cookie transparency which helps build consumer trust.

b) Assessing the intrusiveness of the cookies, by making it clear to the user, if the cookies are from the first part, website owner or a third party (ad vendor or analytics provider).

c) Prior disclosure of the list of third-party cookies, the identity of the third-party, along with the nature of the cookies, the purposes they are used for and their duration in clear and simple language.

d) Offering ‘enhanced notices’ around the targeted advertisements, so that users can clearly distinguish targeted ads which will also help users to learn more about the ad, who is serving the ad and based on which user data they are being targeted.

e) Providing simple means for accepting or rejecting targeted advertising, so that users can easily ‘opt-out’ of targeted advertising instead of them going through multiple privacy policy pages and cumbersome privacy and data settings.

f) Apportioning data privacy responsibilities with third-party ad vendors will help in clearly establishing the roles and responsibilities of the website owners and vendors in terms of accountability and responsibility of compliance with privacy directives when using personal data for targeted advertising. For each
type of data collected, a data controller must be established who will be held accountable for the compliance requirements in collection, processing, usage and storage of user data. Any violation or breach of data privacy will fall under the purview of the data controller which could be the website owner or the ad vendor, depending on the nature of the data.

g) Proactively adopting ‘do not track’ browser functionality which will help reduce the burden on the user to opt-out every time they visit a website without having to deal with multiple cookie consent pop-ups. Leading Browser providers including Google, Mozilla and Microsoft have launched various privacy control measures, including private browsing sessions and ‘do not track’ functionality.

While the above-mentioned principles (Lee, 2011) were offered as a middle road to EU and Non-EU privacy policies, more specifically and recently in April 2020, the Ireland Data Protection Commission has issued specific guidelines concerning cookie banners and cookie consent, which include 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 current Privacy by Design approach.

3.15 Conclusion

Based on the literature review, it is clear that customer data privacy is being treated just as a compliance issue. 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, lack of awareness among customers, the major players still opting to pay fines instead of striving for full compliance.
The upcoming ePR changes strongly suggest that the privacy regulations will continue to evolve and are likely to become more stringent to catch up with technological advancements and societal changes. 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. This will not only increase compliance costs but also in some cases jeopardise business operations, like new-age businesses like online media, e-commerce, social networks which will result in a volatile revenue stream.

Businesses should focus on the principles of the data protection and privacy and integrate them into their organisational culture which will help retain customer trust, so every time there are changes in regulations, there is minimal impact on the core operations of the organisation and customer trust is still maintained to get consent easily as per the new compliance regulations rather than having to pivot the entire business operation and culture of the company.
4. Research Methodology:

4.1. Research Design:

The main aim of the research is to find which external factors are influencing customer attitudes towards cookie consent. The data must be collected to ascertain if there is a causal relationship between the independent variables (online usage factors) and the dependent variable (cookie consent).

The research design for this study can be explained using the research onion (Saunders, Lewis and Thornhill, 2019).

![Research Onion Diagram](image-url)
4.2. Research Framework:

Based on the research onion shown above, a suitable framework was developed to conduct the study with a proper empirical approach. The research philosophy, the research approach, the methodology for primary research, the data collection strategy, a realistic time frame and data analysis techniques which were relevant and appropriate for the study were identified, which is illustrated in the chart below.

PROPOSED FRAMEWORK FOR THIS STUDY

<table>
<thead>
<tr>
<th>Philosophy (Epistemological position)</th>
<th>Approach - Deductive</th>
<th>Data Collection and Data Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positivism</td>
<td>Causal relationship</td>
<td>Data Collection Strategy</td>
</tr>
<tr>
<td>Explaining Human Behaviour</td>
<td>Testing Hypothesis</td>
<td>Online Survey</td>
</tr>
<tr>
<td>Focus on Facts</td>
<td>Generalization</td>
<td>Time horizon</td>
</tr>
<tr>
<td></td>
<td>Mono Method</td>
<td>Cross-sectional</td>
</tr>
<tr>
<td></td>
<td>Quantitative</td>
<td>Snapshot of fixed time</td>
</tr>
<tr>
<td></td>
<td>Representation of</td>
<td>12 weeks</td>
</tr>
<tr>
<td></td>
<td>sample to population</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Highly Structured</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-Probability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sampling</td>
<td></td>
</tr>
</tbody>
</table>

4.2.1. Positivism:

According to Saunders, philosophy of positivism deals with ‘working with observable social reality and that the end product of such research can be law-like generalisations similar to those produced by the physical and natural scientists’ (Saunders, Lewis and Thornhill, 2019). This study is set to study user behaviour in regards to cookie consent which can be replicated. This will help to derive functional relationships between causal and explanatory factors (independent variables) and outcomes (dependent variables) (Park, Konge and Artino, 2020).
4.2.2. Deductive Approach:

A deductive approach starts with the applies well-established theory to test their validity by collecting data and analysing them. A deductive approach addresses the need to explain the causal relationship between variables through a highly structured approach to collect quantitative data. (Saunders, Lewis and Thornhill, 2019). This approach fits with the study as the research aims to address the factors influencing cookie consent behaviour of website users.

This approach also requires to select samples of sufficient size, so they are representative enough to generalize the outcome (conclusions) at the end of the study. (Wilson, 2010).

4.2.3. Quantitative Data:

A quantitative approach is defined as the approach to research might draw a large and representative sample from the population of interest, measure the behaviour and characteristics of that sample, and attempt to construct generalizations regarding the population as a whole. (Hyde, 2000). Since the study is following a deductive approach by applying existing theory, a quantitative approach fits very well and results can be used for comparison. (Wilson, 2010).
4.3. Research Model:

Based on the Technology Acceptance Model (TAM), Online Buying Persuasion (OBP) and Stimulus Theoretical Framework (STF) models discussed earlier, the link between variables like Design, Security, Satisfaction, Trust and the factors like Perceived Usefulness, Perceived Ease of Use, user intent, perceived risk, brand trust has been established.

For purposes of this study, a causal framework to examine the influence of these variables on user intention to give cookie consent is presented here. This framework will form the basis of analysing the results and answer the research questions discussed above.
4.4. Sampling

The study is aimed at general internet users which are considered a wide set of audience. Hence, a non-probability sampling method such as self-selection sampling will be a more practical approach for the data collection.

Self-selection sampling method allows 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 is 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.

By using the sampling, it ensures the respondents have some opinions on the subject matter and have the desire to take part in the research. It also ensures the response is completely voluntary and is more likely to be genuine (Dhivyadeepa, 2015), unlike some feedback surveys which are mandatory to proceed with the task.

4.5. Data Collection

4.5.1. Online Survey

The data collection will be done through an online survey since this research is established as a quantitative study. Since the study is focused on internet users, an online survey ensures, the respondents are familiar with online user experience. The questionnaire is will be shared through social media as they tend to be cost-effective, less time consuming and can help to reach a broader sample which could be more representative of the population.

4.5.2. Questionnaire design

The questionnaire will be designed using Google Forms as it will be easier to distribute among the target audience. The questionnaire will have filter questions to determine the respondents are above the age of 18 and they are from the EU region and likely to spend more time browsing websites than average.
The questionnaire will employ a mix of Likert techniques like Likert scale, Likert item & Likert-type items. (Boone and Boone, 2012). The questions will relate to different variables mentioned in the framework, namely perceived usefulness of cookies, perceived ease of use of cookie banners, User Intention to accept cookies to complete the task, the perceived risk of accepting cookies and trust in the brand to accept cookies.

Questions regarding cookie design have been based on questions used in previous studies on cookie banner design (Machuletz and Böhme, 2020), especially the design variations of consent dialogue options.

4.5.3. Data Analysis Tools
Since the survey is developed using Google forms, the responses will be automatically recorded in a Google spreadsheet which will be used for the analysis of the data collected. Appropriate charts and tabulations will be generated for relevant questions to analyse the respondent’s answers.

4.5.4. Ethical Considerations:
In addition to adhering to the rules and regulations indicated in dissertation guidelines issued by the institution, the utmost care has been taken to make sure that there are no ethical violations in conducting the research (McKee and DeVoss, 2007).

A consent form has been included at the beginning of the questionnaire, to make sure the respondent is fully aware of the purpose of the study, why the data is collected and how will it be used. This is to ensure the respondent has given informed consent rather than implied consent. Respondents are given the choice not to participate or withdraw consent at any time during the survey.

No contact details or personal identification data are collected in the survey and all responses collected will be kept confidential and will not be shared out of the institution board. Respondents were also given directions to contact the researcher if they have any questions or concerns regarding the study or their participation.
4.5.5. Limitations:

The scope of the study is limited by the accessible sample and the actual response level to the survey. It is imperative to note, the purpose of undertaking the research will be to demonstrate the researcher’s capability of understanding marketing and research concepts and applying them to a practical study. Peer review of the results and publication of the study in the public domain is not under consideration and the dissertation report is purely done as part of the course requirement.

While care has been taken to design the questionnaire as simple as possible, it is possible for the respondents may misinterpret or misinformed on the subject matter.

The brief timeframe of 12 weeks also limits the scope for a large scale data collection and having different control groups for further expanded statistical analysis.
5. DATA ANALYSIS:

5.1. Survey administration:

The online questionnaire was designed in Google form and 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 are residing in the European Region or from Non-EU so that they can 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.

The survey 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.

1. Frequency and Familiarity with cookie pop-ups.

The first question related to research topic was to ascertain how familiar were the respondents with regards to cookie consent pop-ups which will give a better insight of how often they were browsing general websites instead of their private work websites.

Majority of the respondents (over 90%) stated that they often interacted with cookie pop-ups, with about 70% of the respondents marking very often, followed by 20%
marking often. This strengthens the validity of the responses to the survey, as the respondents are not just regular internet users, but also familiar with cookie consent banners and likely to have answered the survey questions based on their personal experience.

2. **Awareness of cookies**

The 2\textsuperscript{nd} question was to ascertain the awareness levels of different aspects of website cookies covered under 4 factors, which were the functionality of cookies, purpose of cookies, benefits of cookies and privacy risks of cookies.

![Chart 2 Awareness of Cookies](image)

- **a) The functionality of cookies:**
  
  About 30\% of the respondents were moderately aware of the functionality of cookies. Around 40\% of the respondents were well aware and about 23\% were slightly aware of the functionality of cookies. Only 7\% stated they were not aware of how website cookies worked.

- **b) Purpose of cookies:**
  
  More respondents were aware of the purposes of cookies than its functionality. Almost half of the respondents (48\%) of the respondents said they were very or extremely aware of the purposes cookies are used for. Only about 5\% of the users said they were not aware of purposes for which cookies are used.
c) **Benefits of cookies to the user:**

While the majority of the users (44%) were still well aware of the benefits, a sharp decline can be seen in the moderately aware and an increase in slightly aware. This suggests that users who had moderately aware of functionality and purposes of cookies were not exactly aware of the benefits of cookies to the user.

d) **Privacy Risks of the cookies:**

Again 40% of the respondents were very or extremely aware of the privacy risks associated with cookies. Interestingly, the two extremes in the awareness scale had their highest scores in the privacy factor when compared to the other aspects of the cookies. 21% of the users said they were extremely aware of the privacy risk which is considerably more users relative to extreme awareness of other aspects.

At the same time, 9% of users said they were not at all aware of the privacy risks which is almost twice the number of responses who were not aware of the functionality of cookies. This suggests, users who knew about the functionality of cookies, its purposes and benefits, may not be aware of the privacy risks.

3. **Benefits of Cookie acceptance.**

The next question was a multiple choice question where users can choose the various benefits of using cookies, which is likely to convince them to accept cookies. These responses were based on factors like Design, User Experience, Security which were derived from the previous research studies related to technology acceptance models discussed in the literature review, especially TAM (Davis, 1989), TAM2 (Venkatesh and Davis, 2000) and Stimulus Theory Framework (Help University, Malaysia and Lai, 2017) and other cookie-related studies which outlined the benefits (Bayan, 2001) (Miyazaki, 2008).
Remembering user’s website preferences was the most voted factor (41%) which is likely to convince the user to accept cookies. This was followed by auto sign-in of existing users and improving website user experience. While 13.6% voted none of the reasons will convince them to accept cookies, Personalized ads were the least popular benefit among the respondents.

This highlights that users are ok with essential cookies which are necessary for the website to function properly and improve their browsing experience, but not third party cookies which are used to serve personalized ads which are considered the most invasive.
4. Reasons for Accepting Cookies

The next question was also a multiple choice question which was used to ascertain the user motivations or scenarios in which they are likely to accept cookies.

![Chart 4 Reasons for Accepting Cookies](image)

The response set was derived from factors like Brand Trust, Quick access, Task Completion, Regular user or Repeat user and Content Quality. The need to quickly access the website, followed by the need for information to complete the task were the most popular factors which made users accept the cookies. Brand trust and repeat usage of a website got only about 40% of votes each, which suggests, just because a website is popular among users or trust the brand, doesn’t mean users will be accepting the cookies.

Accepting cookies seems to be motivated by time and intent more than anything. That means the same user who is visiting the same website can accept or decline the cookies, depending on whether they are trying to access the site in a hurry to complete a task in hand or if they are just casually browsing without any particular purpose in mind.
5. Cookie acceptance across categories

This question was presented in a Likert scale grid item and covered 7 major categories of online activities which are Shopping, News Media, Corporate Info, Social Media, Banking & Finance, Healthcare and Education. This was used to ascertain if various user intents are likely to affect user behaviour of accepting or rejecting the cookies. The results have been presented as category wise as follows.

A. Shopping

When it comes to shopping, the majority of the respondents (42%) were likely to accept the cookies which might be because more users perceive it helps in improving their user website user experience. Almost 1/3\textsuperscript{rd} of the users appeared neutral if they will accept or reject cookies, which means they are not entirely sure if it would make any difference in their user experience.

This might also depend on whether they are online shopping in a hurry like food or groceries or they are just browsing for items which are likely in the case of apparel or accessories. However, 26% of users are unlikely to accept the cookies, which might suggest a considerable section of users are still not comfortable accepting cookies.
B. News Media

Similar to shopping, majority of users said they are likely (45%) to accept cookies when they access news media, which based on the previous responses, the users want quick access to the news item and hence likely to accept the cookies. With the current 24-hour news cycle and breaking news several times a day, users are often prone to articles with clickbait headlines and the impulse is to get the news as quickly as possible. A cookie pop-up in blocking the content will be intrusive and the user is more likely to accept the cookies for faster access.

C. Corporate Info

Unlike the previous categories, 44% of respondents marked they are unlikely to accept cookies when browsing for corporate information. This might be because people may not be familiar with the website or brand are looking up for information about the company to know more. Also, they may be looking up
information on the site but no necessarily carrying out a task in the website and hence may not feel motivated to accept cookies.

D. Social Media

When it comes to Social Media, 42% of respondents said they are more likely to accept the cookies, which is not very surprising as users share more personal data on social media more than the scope of what cookies can capture. At the same time, more than 1/3rd of the respondents are not likely to accept cookies, which means a considerable set of users are concerned about privacy and social media. It is also important to consider that 99% of social media is consumed through native mobile apps which do not ask for cookie consent. (KEMP, 2020).

E. Banking & Finance
Unlike the previous categories, when it comes to banking and finance, the respondents are almost evenly split, 39% of users marked they are unlikely to accept the cookies, and almost equally 38% of users marked they are likely to accept the cookies. Only 23% of users offered a neutral response which suggests, the users were highly clear in their stance regardless of their awareness on cost/benefit analysis of accepting the cookies when it comes to banking and financial activity online.

F. Healthcare

When it comes to healthcare, majority of the respondents (47%) were likely to accept the cookies, which may be because users will be getting healthcare information from the sources they trust, so they are comfortable to accept cookies so that they can have a personalised user experience. However, 1/3rd of the users were unlikely to accept the cookies. This might denote, users are concerned with privacy when sharing their health-related data or medical records.
A clear majority of 54%, said they are likely to accept cookies when browsing websites related to education which is the highest among the categories listed in the question. However similar to other categories still about 1/3rd of the users were unlikely to accept the cookies. Neutral responses were also the lowest among the categories with only 18% who were unsure if they will accept the cookies from an educational website.

While there can be many reasons for accepting or rejecting cookies from a website, it is clear from the responses, users behave differently in different categories of web activity. Hence, it can be said that user intent does influence user behaviour when it comes to accepting or rejecting website cookies.
6. Concerns about Accepting Cookies

This question was also a multiple-choice to ascertain which of the concerns regarding cookies were preventing users from accepting cookies.

An overwhelming majority of the users (70%) voted that sharing user data with 3\textsuperscript{rd} party vendors is their primary concern which prevented them from accepting website cookies. This clearly shows users do not like web publishers sharing their user data to their marketing partners and advertising vendors who are the majority of 3\textsuperscript{rd} party who use the data to serve targeted ads to users which are highly personalized.

The 2\textsuperscript{nd} biggest concern among users (64%) is their data being used for purposes they are not aware of. This speaks directly to the lack of transparency from website owners on how they treat user data and for what purposes. While website owners can argue that these are listed in their privacy policy, the finer details are often presented in complex legalese or technical terminology. This contradicts GDPR principles of transparency and fair usage. It is also interesting to note that the response level for concerns regarding cookies is objectively much higher than the responses for accepting cookies.
7. Cookies and website usage

The next question was a simple yes or no question to check if users have refused or exited a website without using since the website required users to accept the cookies to get access to the content.

![Chart 13 Exiting websites for Requiring cookies]

More than 60% of the users said that they have exited a website instead of accepting cookies which indicate, users would rather not use a website that accepts cookies, which also suggests they do not trust the website and the brand associated with it. They are likely to use an alternative website which does not force them to accept cookies to access the site. This indicates that users do take cookie consent seriously and forcing them to give consent is likely to result is going to increase the bounce rate of users.
8. User perception on Cookie Consent Banner effectiveness on data control

This question was to directly capture the user perception towards cookie consent banner and if they feel in their opinion that they are empowering them in managing their data choices.

There was no clear consensus among respondents if cookie consent banners empower them on giving them control over the data collection and usage. Around 38% agree to a certain level cookie banners are effective and around 35% disagree, cookie consent banners give them any control over data usage. 27.3% neither agree nor disagree, which indicates a considerable portion of the users are not clear how cookie banners affect user data control and not sure if they are effective enough in managing their data choices.

Website owners should demonstrate the usefulness of their cookie consent banners and assure that their data choices are being honoured without any ambiguity which will motivate users to make more informed data choices with confidence.
9. Impact of Cookie Consent Banner on user perception on the website’s data policy

This question presented a mirror statement of the previous question, to check if the respondents were firm in their attitude towards cookie banners

Mirroring the previous question’s results, this question also did not provide any consensus if users feel cookie banners are ineffective. About 1/3rd of the users (36%) users disagree cookie banners do not have any impact on their perception of the website’s data handling, which effectively means, users do think that cookie banners do affect their perception of the website’s handling of their data.

Around 34% remained neutral, which might either mean they are not sure about their effectiveness or if their attitude differs between websites and other factors. Around 30% were likely to agree that cookie banners do not affect their perception of how the website’s handling their data.

10. Choice of Cookie Banner Design

To understand user preference on the cookie banner design, the respondents were presented different cookie consent banner designs which were based on the classification used in a 2019 study of cookie consent dialogues. (Utz et al., 2019)
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 88% of users wanted some level of choice in the cookie consent banner, to better manage their data choices.

This also suggests users are very much in favour of websites to collect active consent rather than operating with implied consent.
6. Findings and Discussion

6.1. **Objective A: To evaluate the awareness level of online users about cookies.**

Based on the responses from the sample population, the majority of the users were only moderately aware of the functionality of cookies, its purposes, benefits as well as the risks. More respondents were extremely aware of the risks associated with cookies (21%) than the benefits of cookies for users (14%).

This raises some questions like what is the ideal level of awareness, where 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 very much problematic ethically and even legally in some cases.

Website owners should be held responsible for making sure users have presented enough information in simple and clear language on their data choices, before asking for their consent for cookie usage.

6.2. **Objective B: To examine if the usefulness of cookies motivates the user to give cookie consent.**

To find out if the user’s awareness of benefits of cookies motivates users to give cookie consent, crosstab analysis was generated in SPSS between Awareness of Benefits of Cookies and likeliness of accepting cookies under various categories of online activity as mentioned in the survey which was shopping, news media, corporate info, social media, banking & finance, healthcare and education.

The rightmost bar graphs of each category, represent the acceptance rates of users who are extremely aware of the benefits. None of the awareness levels shows any consistency in acceptance rates of cookies across the categories.
This clearly shows awareness of benefits alone does not increase or decrease the acceptance rates of cookies. There are likely to be other factors like user intent which are likely to influence the users’ cookie acceptance behaviour.
6.3. **Objective C: To examine if user intent motivates the user to give cookie consent.**

When the acceptance level for cookies across categories is plotted together in one single chart, it can be seen that there is no consistent level of cookie acceptance across different categories of online activities, which leads to suggest that depending on the purpose of usage, the acceptance level changes.

![Chart 17 Cookie Acceptance across categories based on User Intent](chart.png)

More than 50% (Q4) of respondents’ state that they were willing to accept cookies if it is needed to complete the task in hand. This suggests that 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.
6.4. Objective: To investigate the influence of brand reputation in getting cookie consent from users.

The familiarity of the brand was voted as the 3rd factor by users which impacts their decision in accepting cookies. Being a regular user of the website came in 4th influences 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.

6.5. Objective: To examine if the perceived risk of accepting cookies influences users in giving consent.

Websites which deal with healthcare, finance, banking, education are often called YMYL (Your Money or Your Life). Based on the responses, there seems to 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.

![Chart 18 Cookie Acceptance across YMYL categories based on Perceived Risk](image-url)
Interestingly, more users were unlikely to accept cookies, when accessing a website to get some corporate info, even the risk of privacy or security breach is very low.

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.

6.6. Objective: To investigate if the user-friendly consent mechanisms motivate the user to give cookie consent.

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.
Even though users had previously cited the quick access to the website as one of the key factors in accepting cookies, 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.

This indicates that users are likely to prefer a design which will help them opt out quicker and whenever given choice users would rather opt-out from accepting cookies than accept cookies.

When the design preferences for the cookie banner are plotted in a radar map, there is a clear skew towards opt-out option and managing data choices.

This suggests that while a better design of a cookie consent banner, have 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.
6.7. Summary of Findings and Analysis

Based on the survey results and their corresponding graphs, different factors had different influences on the cookie acceptance level of the users. Further analysis using cross-tabulation analysis, the various factors which were considered in the research objectives were linked with the survey results to ascertain the influence or lack thereof on the cookie acceptance levels were established and the findings were discussed in the previous section.

For better clarity and understanding, the below table summarizes the answers to the research question of what are the factors likely to influence acceptance rates of cookies.

<table>
<thead>
<tr>
<th>Objective Parameter</th>
<th>Influence on Cookie Acceptance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Usefulness of Cookies</td>
<td>No Significant Influence</td>
<td>Awareness of cookie benefits did not produce consistent acceptance levels</td>
</tr>
<tr>
<td>Perceived Ease of Use in setting Cookie Preferences</td>
<td>Negative Influence</td>
<td>A user-friendly cookie banner design is likely to increase the rate of opting out from cookies by users.</td>
</tr>
<tr>
<td>User Intent when visiting the website</td>
<td>Strong Influence</td>
<td>The purpose of visiting a website seems to play a significant role in acceptance rates which differs across different website categories</td>
</tr>
<tr>
<td>Perceived risk in accepting cookies</td>
<td>No Significant Influence</td>
<td>No consensus among users in acceptance of high risk (e.g. financial) and low risk (e.g. Corporate info)</td>
</tr>
<tr>
<td>Brand trust (Trust of the website owner)</td>
<td>No Significant Influence</td>
<td>Not ranked among the important factors for cookie acceptance.</td>
</tr>
</tbody>
</table>

It is clear that user intent is the prime motivating factor for the user to accept website cookies and given a choice, users are most likely to opt-out non-essential cookies, especially 3rd party marketing cookies, which are the most invasive type of cookies often used for serving targeted advertisements to the users.
7. Conclusion and Recommendations

7.1. 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 have had an impact on organisations taking the data privacy and security more seriously.

However, there is also enough evidence, that organisations are treating their GDPR efforts as a compliance issue, as 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 3rd 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 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 which helps in tracking, measurement 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 which are much more invasive and much harder to opt-out when compared to cookies.
7.2. Future of Consent:

While on the surface, making 3rd part website cookies seem to resolve the issue of obtaining explicit cookie consent and related complications, 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.

7.3. 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 which has benefitted 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 consumer develops a negative perception towards the brand on how the brand handles their user data or become aware of them engaging in invasive practices, then all the personalized ads will not be able to help them to recover from that. Advertisers and web technology providers should develop technologies, process and protocols with the consumer’s right to data privacy at their core so that the industry is sustainable in the long-run.
7.4. Recommendations for Managing User Consent

The European Commission has been discussing stringent cookie consent laws, including standardizing the language, consent banner design and accountability for managing data choices (legroju, 2017). These changes were expected to come into effect in 2020, but due to various delays such as BREXIT and Covid-19 crisis have further delayed their implementation. It might take another year at least for these changes to come into effect and an additional couple of years for it to be fully implemented by organisations, during which time advertisers would have already moved to advanced technologies for tracking and advertising, 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 on the survey, users simply are not interested in cookies or managing their cookie settings and 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 which can 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 in mind the foundation principle of GDPR. Such a framework will help develop directives to regulate organisations for getting consent from users to use their data for advertising and marketing purposes regardless of the technologies they might employ to serve targeted ads. Organisations must maintain high levels of transparency what data is being collected and the purposes they are used for and how users can opt-out of getting targeted ads, where possible.

To that effect, this study proposes a Consent for Advertising Directive (CAD) which can be incorporated with the current ePrivacy regulations (ePR). The below chart illustrates the proposed factors which will form the Consent for Advertising Directive (CAD) which will increase transparency and effective consent from users.
Benefits to Businesses

CAD will not only strengthen the effectiveness of GDPR compliance but also helps brands 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 by removing any ambiguity of what the customers are giving their consent for. By engaging in a more transparent way brands will be strengthening their consumer trust by championing the data protection rights of their customers.
7.5. Limitations and Future Research opportunities

The study was based on a limited set of responses of 132. Even though a majority of the respondents had a good level of awareness on the subject matter results which helped in developing interesting insights, the smaller sample size makes it harder to justify generalizing those conclusions for the entire population.

Demographics of the users apart from the current region of residence were not collected in this survey and any correlation between factors like age, income, education and their attitude towards cookie consent was not explored. The findings of the study are based on the existing cookie laws and cookie consent banner mechanisms used at the time of the survey and consumer attitudes are likely to change over time.

Based on the findings of this research, there are further opportunities to explore consumer attitude towards personalized ads and what are the boundaries consumers expect brands to maintain when employing targeted advertising. There are opportunities to explore if there are various degrees of consent for various types of data usage and if they can be deployed at various stages of a customer journey so that customer can choose at what stage they are comfortable sharing what type of data.

Since the 3rd party cookies are being phased out, studies can be undertaken, to see what kind of impact they might be having in targeted advertising from both from an advertiser perspective as well as a consumer perspective.
8. BIBLIOGRAPHY


9. Appendix

Appendix 1: Questionnaire

Cookie Consent Survey July 2020

Hi there! My name is MJ and I am currently pursuing my Masters in Dublin Business School and I would like to survey you as part of my Thesis. Thank you for your time and consideration to take this survey.

*Required

About the Research:
The purpose of this research project is to survey internet users to study their motivations towards website cookies consent which is mandated by ePrivacy Directive (known as the "cookie law") under General Data Protection Regulation (GDPR).

This is a research project being conducted as part of a Master thesis at Dublin Business School. You are invited to participate in this research project because you are recognized as an internet user from the EU region. Your participation in this research study is voluntary. You may choose not to participate. If you decide to participate in this research survey, you may withdraw at any time. If you decide not to participate in this study or if you withdraw from participating at any time, you will not be penalized.

The procedure involves filling an online survey that will take less than 10 minutes. We will do our best to keep your information confidential. All data is stored in a password protected electronic format. To help protect your confidentiality, the surveys will not contain information that will personally identify you. The results of this study will be used for scholarly purposes only and may be shared with Dublin Business School representatives.

If you have any questions about the research study, please contact me at mj-digital@outlook.com. This research has been reviewed according to Dublin Business School for research involving human subjects.

ELECTRONIC CONSENT FORM: Please select your choice below. Clicking on the "agree" button below indicates that: a) you have read the above information b) you voluntarily agree to participate c) you are at least 18 years of age.

If you do not wish to participate in the research study, please decline participation by clicking on the 'disagree' button.

☐ Agree
☐ Disagree
Current Region of Residence *

- European Union Region (includes EEA)
- Non-EU Region
- Other:

How often do you interact with cookie banners similar to the one below *

This website uses cookies
In order to offer you the most effective service possible, our site makes use of necessary cookies and similar technologies. With your permission we use statistic cookies to test and optimize the website. If you accept marketing cookies we share information with our partners for social media, advertising and analysis. Please let us know underneath which cookies we can use.

Manage cookies   Accept all cookies

1  2  3  4  5
Not Very often

How aware are you about Website Cookies? *

<table>
<thead>
<tr>
<th></th>
<th>Not at all Aware</th>
<th>Slightly Aware</th>
<th>Moderately Aware</th>
<th>Very Aware</th>
<th>Extremely Aware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality of Cookies</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Purposes of Cookies</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Benefits of Cookies to User</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Privacy Risks of Cookies to User</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
Which of the below reasons will convince you to accept all cookies? (you can choose multiple answers) *

- [ ] It will improve website user experience
- [ ] Automatically sign-in if existing user
- [ ] Personalized ads
- [ ] Remember my website preferences
- [ ] Free Content
- [ ] None of the above (leave other boxes unchecked)

Complete the following "I am more likely to accept cookies if ________________" (you can choose multiple answers) *

- [ ] I need the information from the website to complete a task.
- [ ] I am very familiar with the brand/business of the website and its reputation
- [ ] I am a regular user of the website
- [ ] I find the content interesting and would like to know more
- [ ] I need to access the content quickly
- [ ] None of the above (leave all other boxes unchecked)
- [ ] Other:

How likely will you accept all cookies in the below online activities *

<table>
<thead>
<tr>
<th>Activity</th>
<th>Very Unlikely</th>
<th>Moderately unlikely</th>
<th>Neither likely nor unlikely</th>
<th>Moderately likely</th>
<th>Very Likely</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shopping</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>News Media</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>Corporate info</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>Social Media</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>Banking &amp; Finance</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>Healthcare</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>Education</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>
Which of the below concerns will stop you from accepting all cookies? *

- Loosing my Online Anonymity
- More of my data being collected than needed to access the website
- My data used for purposes which I was not aware of
- My data being shared with other 3rd party vendors
- Tracking my online behavior after I have left the website
- None of the above. (leave other boxes unchecked)
- Other:

Have you ever not used a website for requiring to accept cookies? *

- Yes
- No

How do you feel about below statement “Cookie Consent Banners give me control over how my data is collected and used” *

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely Disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How do you feel about below statement “Cookie Consent Banners do not have any impact on how I feel about the website’s handling of my data” *

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely Disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Which cookie consent banner do you prefer?

- Notification (no choice)
- Confirmation (without opt-out option)
- Confirmation with opt-out option
- Option to choose how your data can be used.
- None of the above
- Option to choose who can use your data.
Appendix 2: SPSS OUTPUT

1. Awareness Benefits of Cookies * Categories Cross tabulation

### AwarenessBenefitsofCookies * Shopping

<table>
<thead>
<tr>
<th>AwarenessBenefitsofCookies</th>
<th>Shopping</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Moderately</td>
<td>Moderately</td>
<td>Neither</td>
<td>Likely</td>
<td>Unlikely</td>
</tr>
<tr>
<td>Extremely Aware</td>
<td></td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>Moderately Aware</td>
<td></td>
<td>9</td>
<td>0</td>
<td>9</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Not at all Aware</td>
<td></td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Slightly Aware</td>
<td></td>
<td>6</td>
<td>9</td>
<td>15</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Very Aware</td>
<td></td>
<td>21</td>
<td>9</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>36</td>
<td>18</td>
<td>42</td>
<td>20</td>
<td>16</td>
</tr>
</tbody>
</table>

### AwarenessBenefitsofCookies * NewsMedia

<table>
<thead>
<tr>
<th>AwarenessBenefitsofCookies</th>
<th>NewsMedia</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Moderately</td>
<td>Moderately</td>
<td>Neither</td>
<td>Likely</td>
<td>Unlikely</td>
</tr>
<tr>
<td>Extremely Aware</td>
<td></td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Moderately Aware</td>
<td></td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Not at all Aware</td>
<td></td>
<td>6</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Slightly Aware</td>
<td></td>
<td>9</td>
<td>6</td>
<td>9</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Very Aware</td>
<td></td>
<td>9</td>
<td>6</td>
<td>12</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>39</td>
<td>21</td>
<td>33</td>
<td>20</td>
<td>19</td>
</tr>
</tbody>
</table>

### AwarenessBenefitsofCookies * Corporateinfo

<table>
<thead>
<tr>
<th>AwarenessBenefitsofCookies</th>
<th>Corporateinfo</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Moderately</td>
<td>Moderately</td>
<td>Neither</td>
<td>Likely</td>
<td>Unlikely</td>
</tr>
<tr>
<td>Extremely Aware</td>
<td></td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>Moderately Aware</td>
<td></td>
<td>6</td>
<td>6</td>
<td>9</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Not at all Aware</td>
<td></td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Slightly Aware</td>
<td></td>
<td>9</td>
<td>12</td>
<td>9</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Very Aware</td>
<td></td>
<td>9</td>
<td>18</td>
<td>6</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>25</td>
<td>39</td>
<td>30</td>
<td>19</td>
<td>19</td>
</tr>
</tbody>
</table>
# Awareness Benefits of Cookies by Domain

## Social Media

<table>
<thead>
<tr>
<th>Awareness Benefits of Cookies</th>
<th>Extremely Aware</th>
<th>Moderately Likely</th>
<th>Moderately Unlikely</th>
<th>Neither Likely nor Unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>9</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>3</td>
<td>6</td>
<td>3</td>
<td>9</td>
<td>9</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>15</td>
<td>6</td>
<td>12</td>
<td>0</td>
<td>3</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>Very Aware</td>
<td>9</td>
<td>6</td>
<td>12</td>
<td>8</td>
<td>4</td>
<td>39</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>31</strong></td>
<td><strong>18</strong></td>
<td><strong>33</strong></td>
<td><strong>25</strong></td>
<td><strong>25</strong></td>
<td><strong>132</strong></td>
<td></td>
</tr>
</tbody>
</table>

## Banking and Finance

<table>
<thead>
<tr>
<th>Awareness Benefits of Cookies</th>
<th>Extremely Aware</th>
<th>Moderately Likely</th>
<th>Moderately Unlikely</th>
<th>Neither Likely nor Unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>9</td>
<td>3</td>
<td>9</td>
<td>3</td>
<td>6</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>12</td>
<td>9</td>
<td>9</td>
<td>12</td>
<td>0</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Very Aware</td>
<td>6</td>
<td>21</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>39</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>37</strong></td>
<td><strong>33</strong></td>
<td><strong>30</strong></td>
<td><strong>13</strong></td>
<td><strong>19</strong></td>
<td><strong>132</strong></td>
<td></td>
</tr>
</tbody>
</table>

## Healthcare

<table>
<thead>
<tr>
<th>Awareness Benefits of Cookies</th>
<th>Extremely Aware</th>
<th>Moderately Likely</th>
<th>Moderately Unlikely</th>
<th>Neither Likely nor Unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>11</td>
<td>3</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>9</td>
<td>3</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>3</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>9</td>
<td>15</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>Very Aware</td>
<td>15</td>
<td>9</td>
<td>3</td>
<td>11</td>
<td>1</td>
<td>39</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>34</strong></td>
<td><strong>27</strong></td>
<td><strong>30</strong></td>
<td><strong>28</strong></td>
<td><strong>13</strong></td>
<td><strong>132</strong></td>
<td></td>
</tr>
</tbody>
</table>
### 2. Awareness Privacy Risks of Cookies * Categories

#### AwarenessPrivacyRisksofCookies * Shopping Crosstabulation

<table>
<thead>
<tr>
<th>AwarenessPrivacyRisksofCookies</th>
<th>Extremely Aware</th>
<th>Moderately likely</th>
<th>Moderately unlikely</th>
<th>Neither likely nor unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Aware</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>3</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>6</td>
<td>8</td>
<td>9</td>
<td>3</td>
<td>4</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>6</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>12</td>
<td>15</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>Very Aware</td>
<td>17</td>
<td>6</td>
<td>3</td>
<td>12</td>
<td>1</td>
<td>39</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>45</td>
<td>29</td>
<td>24</td>
<td>26</td>
<td>8</td>
<td>132</td>
<td></td>
</tr>
</tbody>
</table>

#### AwarenessPrivacyRisksofCookies * NewsMedia Crosstabulation

<table>
<thead>
<tr>
<th>AwarenessPrivacyRisksofCookies</th>
<th>Extremely Aware</th>
<th>Moderately likely</th>
<th>Moderately unlikely</th>
<th>Neither likely nor unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Aware</td>
<td>6</td>
<td>0</td>
<td>9</td>
<td>3</td>
<td>10</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>9</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Very Aware</td>
<td>6</td>
<td>12</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>39</td>
<td>21</td>
<td>13</td>
<td>20</td>
<td>20</td>
<td>132</td>
<td></td>
</tr>
</tbody>
</table>

#### AwarenessPrivacyRisksofCookies * CorporateInfo Crosstabulation

<table>
<thead>
<tr>
<th>AwarenessPrivacyRisksofCookies</th>
<th>Extremely Aware</th>
<th>Moderately likely</th>
<th>Moderately unlikely</th>
<th>Neither likely nor unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Aware</td>
<td>1</td>
<td>0</td>
<td>12</td>
<td>5</td>
<td>10</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>12</td>
<td>9</td>
<td>3</td>
<td>6</td>
<td>7</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>0</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>5</td>
<td>6</td>
<td>9</td>
<td>5</td>
<td>0</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>Very Aware</td>
<td>3</td>
<td>18</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>25</td>
<td>39</td>
<td>30</td>
<td>19</td>
<td>19</td>
<td>132</td>
<td></td>
</tr>
</tbody>
</table>
### AwarenessPrivacyRisksofCookies * SocialMedia Crosstabulation

<table>
<thead>
<tr>
<th>AwarenessPrivacyRisksofCookies</th>
<th>Moderately likely</th>
<th>Moderately unlikely</th>
<th>Neither likely nor unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Aware</td>
<td>4</td>
<td>0</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>28</td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>6</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>4</td>
<td>37</td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>9</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>9</td>
<td>29</td>
</tr>
<tr>
<td>Very Aware</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>3</td>
<td>3</td>
<td>26</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>31</strong></td>
<td><strong>18</strong></td>
<td><strong>33</strong></td>
<td><strong>25</strong></td>
<td><strong>25</strong></td>
<td><strong>132</strong></td>
</tr>
</tbody>
</table>

### AwarenessPrivacyRisksofCookies * BankingFinance Crosstabulation

<table>
<thead>
<tr>
<th>AwarenessPrivacyRisksofCookies</th>
<th>Moderately likely</th>
<th>Moderately unlikely</th>
<th>Neither likely nor unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Aware</td>
<td>10</td>
<td>1</td>
<td>9</td>
<td>5</td>
<td>3</td>
<td>28</td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>3</td>
<td>7</td>
<td>37</td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>12</td>
<td>9</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>29</td>
</tr>
<tr>
<td>Very Aware</td>
<td>3</td>
<td>14</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>26</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>37</strong></td>
<td><strong>33</strong></td>
<td><strong>30</strong></td>
<td><strong>13</strong></td>
<td><strong>19</strong></td>
<td><strong>132</strong></td>
</tr>
</tbody>
</table>

### AwarenessPrivacyRisksofCookies * Healthcare Crosstabulation

<table>
<thead>
<tr>
<th>AwarenessPrivacyRisksofCookies</th>
<th>Moderately likely</th>
<th>Moderately unlikely</th>
<th>Neither likely nor unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Aware</td>
<td>4</td>
<td>1</td>
<td>9</td>
<td>11</td>
<td>3</td>
<td>28</td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>9</td>
<td>9</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>37</td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>0</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>29</td>
</tr>
<tr>
<td>Very Aware</td>
<td>9</td>
<td>8</td>
<td>0</td>
<td>6</td>
<td>3</td>
<td>26</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>34</strong></td>
<td><strong>27</strong></td>
<td><strong>30</strong></td>
<td><strong>28</strong></td>
<td><strong>13</strong></td>
<td><strong>132</strong></td>
</tr>
</tbody>
</table>

### AwarenessPrivacyRisksofCookies * Education Crosstabulation

<table>
<thead>
<tr>
<th>AwarenessPrivacyRisksofCookies</th>
<th>Moderately likely</th>
<th>Moderately unlikely</th>
<th>Neither likely nor unlikely</th>
<th>Very Likely</th>
<th>Very Unlikely</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Aware</td>
<td>7</td>
<td>1</td>
<td>6</td>
<td>11</td>
<td>3</td>
<td>28</td>
</tr>
<tr>
<td>Moderately Aware</td>
<td>8</td>
<td>11</td>
<td>9</td>
<td>7</td>
<td>2</td>
<td>37</td>
</tr>
<tr>
<td>Not at all Aware</td>
<td>9</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>Slightly Aware</td>
<td>12</td>
<td>9</td>
<td>3</td>
<td>5</td>
<td>0</td>
<td>29</td>
</tr>
<tr>
<td>Very Aware</td>
<td>9</td>
<td>8</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>26</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>45</strong></td>
<td><strong>29</strong></td>
<td><strong>24</strong></td>
<td><strong>20</strong></td>
<td><strong>8</strong></td>
<td><strong>132</strong></td>
</tr>
</tbody>
</table>