



Thesis: May 3rd,2022

An awareness study of the EU Privacy and Electronic Communication(ePrivacy) directive (S.I. No. 336/211).

Thesis presented by

Pat Rowland

This dissertation was submitted in fulfilment of the requirements for the Master of Science in Digital Media and Marketing, Atlantic Technological University, Mayo Campus.

Supervisors: Dr. Janine McGinn and Dr. Eoin Cullina.

May 2022

DECLARATION

I hereby declare that this dissertation is my own work, and it has never been presented to any institution or university for the award of a Degree or Diploma.

Pat Rowland

Patrick Rowland

Candidate Name

Date: April 30, 2022

Dr. Janine McGinn

Supervisor

Date: April 30, 2022

Dr. Eoin Cullina

Supervisor

Date: April 30, 2022

ACKNOWLEDGEMENTS

Thanks, and acknowledgments are due to many people who have given their time, support, encouragement, advice, and expertise over the last two years.

Firstly, I would like to thank my primary supervisor, Dr. Janine McGinn, for her endless help and support, in the preparation and completion of this thesis. Her willingness to help and review countless transcripts is a testament to her tremendous dedication and work ethic. Thanks also to Dr. Eoin Cullina for his expert guidance and advice which proved very useful in completing this dissertation. I was also like to thank Laura Hegarty, Sharon Boyle, and Noreen Henry, also of GMIT, who guided me through the completion of my Post-Graduate Certificate

I would also like to thank my family for their help and support throughout the Post-Graduate Certificate and thesis modules. Without their unfailing support, none of this would be possible. Special thanks, to my wife Karen and children, Anthony, Kevin, Paul, and Anna.

I would finally like to thank all those that gave their time to complete surveys or interviews, my work colleagues and classmates who often referred me to material relevant to my subject matter and were always willing to help with advice and words of encouragement.

Abstract

Background: In today's increasingly information and digital age there is widespread use of search engines and social network sites. The use of this media form seems to be ubiquitous as it cuts across all age groups, social classes, and cultures. Online Behavioural Advertising (OBA) through the tracking of users has allowed for the development of user-targeted campaigns which traditional legal principles have struggled to come to terms with. It has fallen to the European Union and subsequently governmental organisations such as the Data Protection Commission (DPC) in Ireland to implement guidelines by which users must actively consent before cookies can be set up. The EU Privacy and Electronic Communication (e-privacy) directive (EU Cookie Law), (S.I. No. 336/211) outlines the regulations by which consent must be given by consumers prior to placing cookies on their devices. Cookies are small text files that record internet users' online activity. The regulators moved to update its guidance in 2020 having identified widespread failings of compliance during a sweep of websites in 2019. Given the widespread noncompliance as identified in the DPC cookie sweep and review of literature, there is, however, a lack of research into awareness of the directive by the various stakeholders.

Aim: The aim of this analysis is to measure the awareness and effectiveness on a regulatory, business, and consumer level of the EU Privacy and Electronic Communication (e-privacy) directive (EU Cookie Law), (S.I. No. 336/211) one year after the updated guidance from the DPC and how this may affect future policy.

Methods: A two-phased sequential mixed methods study across three key stakeholders was conducted consisting of an online survey administered to consumers and one-to-one interviews with representatives of the business community and with the Regulator who has responsibility for enforcing these regulations.

Results: The results identified a significant lack of awareness of the directive amongst the consumer and business cohorts with widespread noncompliance and limited enforcement

by the Regulator and large-scale indifference by consumers to protect their online privacy despite their stated concerns for their online data.

Conclusion: There is a very low level of awareness of the directive. The reasons for this range from the way the legislation is drafted, limited, and shared powers of enforcement by the DPC, deliberate non-compliance and largely missing the same enforcement powers as GDPR. Awareness campaigns, standardized CMP's and automated auditing tools will all help increase awareness and effectiveness of the directive.

Keywords: Privacy, Awareness, Cookies, Enforcement, DPC, Privacy Paradox, Cookie Fatigue, Awareness Campaigns, Dark Patterns.

Table of Contents

DECLARATION	ii
ACKNOWLEDGEMENTS	iii
Abstract	iv
<i>List of Figures</i>	<i>ix</i>
<i>List of Tables</i>	<i>x</i>
<i>List of acronyms and definitions</i>	<i>x</i>
Chapter 1: Introduction	1
1.1 <i>Growth of Online Business:</i>	<i>1</i>
1.2 <i>Online behavioural advertising and cookies</i>	<i>1</i>
1.3 <i>Background to legislation.</i>	<i>2</i>
1.4 <i>Data protection Commission (DPC) enforcement</i>	<i>3</i>
1.5 <i>Research aims and objectives.</i>	<i>5</i>
1.6 <i>Dissertation Structure Overview.</i>	<i>5</i>
1.7 <i>Positionality of Researcher</i>	<i>6</i>
1.8 <i>Limitations</i>	<i>6</i>
Chapter 2: Literature Review.	7
2.1. <i>Introduction</i>	<i>7</i>
2.2 <i>Background on Privacy Concerns</i>	<i>7</i>
2.2.1 <i>Privacy Paradox</i>	<i>8</i>
2.2.2 <i>Privacy Regulation and consumers concerns over privacy.</i>	<i>9</i>
2.2.3 <i>Cookie Fatigue</i>	<i>10</i>
2.2.4 <i>Future Research</i>	<i>11</i>
2.3 <i>Background on Privacy law.</i>	<i>11</i>
2.3.1 <i>Statutory Control-Privacy</i>	<i>12</i>
2.3.2 <i>ePrivacy Regulation</i>	<i>13</i>
2.3.3 <i>Dark Patterns</i>	<i>13</i>
2.3.4 <i>Common Law</i>	<i>14</i>
2.3.5 <i>Future Research</i>	<i>15</i>
2.4 <i>Background on Awareness Concerns.</i>	<i>16</i>

2.4.1 Awareness Studies	16
2.4.2 Awareness Campaigns.....	16
2.4.3 Factors to increase the effectiveness of an awareness campaign	18
2.4.4 Future Research	19
2.5 Conclusion on Literature Review.....	20
Chapter 3 Methodology.....	23
3.1 Introduction.....	23
3.2 Context of the Study.	23
3.3 Research Design, Sampling, and Data Collection	24
3.3.1 Pilot Study	24
3.3.2 Study Design.....	25
3.3.3 Quantitative Research	25
3.3.4 Qualitative Research.....	26
3.3.5 Mixed-methods Research	26
3.3.6 Review of literature around research approach.....	27
3.3.7 Chosen Research Method	28
3.4 Survey	28
3.4.1 Survey Design.....	29
3.5 Data Analysis.....	34
3.5.1 Survey analysis. Online Survey.....	35
3.5.2 Qualitative analysis.	39
3.5.3 Data Integration	39
3.5.4 Ethics.....	42
3.6 Limitations.....	43
Chapter 4 Findings/Discussion.	44
4.1 Research Question	44
4.2 Survey Strand – Consumer Survey Results.....	44
4.2.1 Level of awareness of Directive amongst consumers.....	45
4.2.2 Data Privacy.....	45
4.2.3 Trust.....	47

4.2.4 Patterns nudging people to consent to cookies.....	48
4.2.5 The majority of respondents felt that Internet providers should have primary responsibility to protect their data.	49
4.3.1 Level of awareness of Directive amongst businesses.	51
4.3.2 Companies care about data privacy but are more concerned about GDPR than the directive.	52
4.3.3 Most businesses see it as a mere compliance issue and nothing more, compliance amongst our respondents was patchy.	53
4.3.4 The majority of consumers are just accepting their cookie policies without reading it.....	54
4.3.5 All businesses thought that there should be more media campaigns to increase awareness.	54
4.4 Triangulation.....	56
4.4.1 Complementary results.....	56
4.4.2 Divergent results.....	56
4.5 Regulator	56
4.5.1 Reasons for low level of awareness around ePrivacy directive.	57
4.6 Discussion.....	60
Chapter 5: Conclusion and Recommendations.....	63
5.1 Introduction.	63
5.2 Research purpose and Methodology.	63
5.3 Findings.....	64
5.4 Recommendations.	66
5.4.1 Awareness.....	66
5.4.2 Enforcement.....	67
5.4.3 Challenges.....	67
5.4.4 Google’s dominance.	68
5.4.5 Trust.....	69
5.5 Future research.....	69
5.6 Conclusions	70
Bibliography	72

Appendices	78
Appendix A: Ethics Approval Form	79
Appendix B: Consumer Questionnaire	107
Appendix C: Questions to Business Cohort.	117
Appendix D: Questions for Regulator.	124

List of Figures

Figure 1 Overview of Results from DPC Cookie Sweep (Deloitte, 2020)	4
Figure 2 Main Factors which influence human behaviour and change (Dolan et al., 2010).	18
Figure 3: Online survey participants	30
Figure 4: Business Cohort.....	32
Figure 5 the Conceptual framework for a mixed-methods approach (Othman et. al, 2020).....	35
Figure 6: Analytics Tool, Microsoft forms	36
Figure 7 Picture of transcribed interviews.....	40
Figure 8 : Key findings consumer survey.....	44
Figure 9: Consumers' trust concerns and their reluctance to change providers to protect their privacy.....	47
Figure 10: Respondents trust in organisations to protect their data.	47
Figure 11: Respondents' responses as to who should protect their data.	50
Figure 12: Key findings business sector	50
Figure 13: Quote from Manager, large digital agency	52
Figure 14: Level of compliance with directive per our survey	54
Figure 15: Word cloud of respondents' suggestions to increase awareness of the Directive.....	55
Figure 16: Key findings Regulator	57
Figure 17: Quote from Regulator with reference to the ePrivacy Directive.....	58
Figure 18: Different phases involved in an ESMMR approach.....	61
Figure 19: Aggregated research findings	66

List of Tables

Table 1: Themes from review of literature.....	22
Table 2: Business Segment Interviewees.....	32
Table 3: Breakdown of survey responses	38
Table 4: Breakdown on interview responses.....	41
Table 5: Comparison of main themes from literature review to themes from findings.	62
Table 6 : A Summary of our findings and proposed solutions.....	71

List of acronyms and definitions

C.C.C. P.	Competition and Consumer Protection Commission.
C.E.O	Chief Executive Officer.
C.F.I.P.	Concerns for Information Privacy.
C.M.A.(UK)	Consumer and Markets Authority (UK).
C.J.E.U.	Court of Justice of the European Union.
COMREG	Commission for Communications Regulation.
C.P.M	Communication Privacy Management.
C.M.P.	Consent Management Platform.
C.T.O.	Chief Technology Officer.
D.P.C.	Data Protection Commission.
D.P.O	Data Protection Officer.
ePD	ePrivacy Directive (S.I. No, 336 of 2011).
G.D.P.R.	General Data and Protection Regulation (2018).
I.D.	Unique Identifier.
I.P.	Internet Protocol Address.
O.E.C.D.	The Organisation for Economic Co-Operation and Development
R.E.F.I.T.	European Commission’s Regulatory Fitness and Performance Programme.

Chapter 1: Introduction

1.1 Growth of Online Business:

A 2014 White House Report on 'big data' concludes that with reference to the technological trajectory 'that more and more data will be generated about individuals and will persist under the control of others' (Executive office of the President, 2014). Individual needs have driven the growth of the Internet with 79% of people in 26 countries considering Internet access to be a fundamental human right (BBC, 2010). In addition, the use of social media is growing at such a rapid pace that the 21st century could well be described as the boom period for social media use. The numbers of social media users represent 49% of the global population and according to a recent Smart Insight Report the use of social media was growing by 9% annually with over 3.8 billion social media users as at January 2020 (Dave Chaffey, 2020). In Ireland 91% of households have access to the Internet with almost all houses with dependent children having internet access (CSO, 2019) .

1.2 Online behavioural advertising and cookies.

This ready access to and availability of social media together with the vast engagement as detailed above has generated a wealth of data that the big data companies, social media platforms and marketing professionals are leveraging for strategic insight and digital marketing. All these entities are using this vast data as a target of commercialisation strategies. Cookies are an important way for businesses to monitor user behaviour and can provide a detailed profile based on user behaviour, which can be easily exploited for marketing purposes. Capturing online users and converting them into paying customers is how you succeed in the digital world. When browsing the internet, you leave behind digital traces that websites can legally use to keep track of your activities and identify you.

Cookies are small text files stored on a device that record internet users' online activity. Using a visitor's IP (Internet protocol address) address as a unique ID (unique identifier), cookies contain information like browsing history, user ID, session ID, and several other pieces of information (Bocetta, 2020).

1.3 Background to legislation.

Regulation 5 of the European Communities (Electronic Communications networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. No, 336 of 2011) ('the ePrivacy regulations or Cookie law) protects the confidentiality of electronic communications. This legislation is separate to, but complements, the General data protection Regulation ('GDPR). Organisations must comply with both laws, but the rules under the ePrivacy legislation apply first when you are considering your organisation's use of cookies and other tracking technologies (DPC, 2020).

EU rules as set out in the Privacy and Electronic Communications (e-Privacy) Directive subsequently transposed into Irish law via Statutory Instrument No. 336 of 2011 state that storing and accessing information on users' computers is, generally, only lawful "on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information about the purposes of the processing". An exception to the consent requirements exists where the cookie is "strictly necessary" for the provision of a service "explicitly requested" by the user.

Cookies placed on user's machines by the website controllers are known as first- party cookies and these are commonly used to store information such as user preferences, login names and shopping cart information. Because these are deemed strictly necessary for the website to work these cookies are generally exempted from the regulations unless they are used for tracking or profiling purposes.

The regulations are mostly concerned with what are known as third party cookies which are cookies that originate from sources generally unconnected with the first-party cookie website and are often used as a tracking mechanism for advertising or profiling purposes. They are generally delivered by tracking pixels or JavaScript code. Because third-party cookies originate from sites, companies, or services that users have not directly interacted with, they have long been seen as an invasion of privacy - or outright means to enforce internet censorship (Bocetta, 2020).

1.4 Data protection Commission (DPC) enforcement.

In August 2019, the Data protection Commission (DPC) commenced an examination of the use of cookies and similar technologies on a selection of websites across a range of sectors, including media and publishing, the retail sector, restaurants and food ordering services, sport and leisure and the public sector (DPC,2020) They surveyed the websites and practices of 38 well known organizations seeking to establish whether, and to what extent, organizations were complying with the ePrivacy regulations in respect of the use of Cookies , and the general data protection Regulation (EU) (2026/679) (;GDPR') in respect of the processing of personal data via the cookies. Although the law was in place since 2011 Mr. Tony Delaney, Deputy Commissioner for enforcement at the DPC in a One Trust Webinar in July 2020 (OneTrust, 2020), stated that enforcement did not become a priority until 2019. He stated that several factors prompted them to increase enforcement in 2019. Firstly, the regulation adopts the provisions for consent laid out in the GDPR, consent must be freely given, specified, informed, and allowed to be withdrawn at any time.

Secondly, he indicated that the DPC office had received additional funding to commence enforcement, had received complaints from members of the public and from their observations as users of websites. Additionally, they stated that they were aware of recent judgments in the Fashion ID case and the Planet 49 judgments by the European Court (CJEU). The Planet 49 case related to consent and transparency requirements regarding the use of cookies and similar technologies. (C.J.E.U., 2019). In this case the CJEU judged that pre checked boxes are not sufficient in order to obtain valid consent for placing cookies on a user's device, as it does not constitute an unambiguous indication of the wishes of the data subject. In the Fashion ID case the CJEU held that Fashion ID and Facebook are joint controllers facing equal requirements regarding the personal data which is processed (C.J.E.U., 2019).

Based on the results of its sweep, the DPC concluded that many organisations may misunderstand what is of required of them. Twenty of the targeted organisations were given an “amber grading,” indicating a good response and approach to compliance but signaling at least one serious concern. Twelve organisations were given a “red grading” due to poor quality responses, bad practices with cookie banners, setting cookies without consent, poor policies on cookies and privacy, and an overall failure to grasp the objectives of ePrivacy law. Only two organisations were given a “green

grading,” meaning that the DPC found them to be substantially compliant. Fig 1 below gives a graphical overview of the results of the sweep.

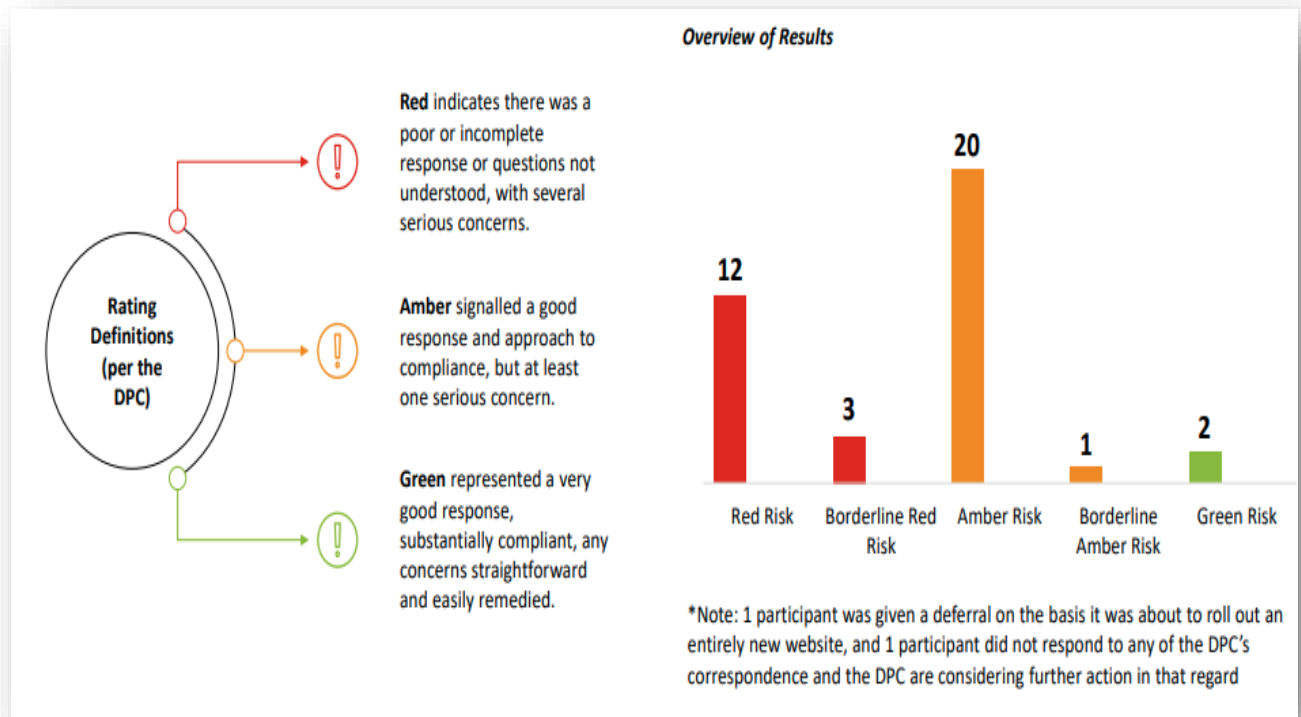


Figure 1 Overview of Results from DPC Cookie Sweep (Deloitte, 2020)

In concluding that “*bad practices were widespread even among companies and controllers that are household names,*” the DPC has acknowledged that there are systemic issues that require its guidance, “*followed by possible enforcement action where controllers fail to voluntarily bring themselves into compliance* (DPC 2020, Pg.19). Subsequent to this the DPC moved to update its guidance in 2020 after the widespread failings identified in the Cookie Sweep and gave organizations a six-month grace period and indicated that changes are on the horizon for businesses who are not meeting compliance, resulting in an increase in enforcement globally after the October 5, 2020, compliance grace-period ended.

1.5 Research aims and objectives.

The main aims of this research are to determine the level of awareness of the directive amongst the public at large one year after updated guidance from the DPC. I sought to measure this by surveying the level of awareness amongst consumers, the business community, and the regulator. I also sought to determine if there was a relationship between the level of awareness of and compliance with the directive and ultimately whether further policy changes are warranted to increase the level of awareness of this important directive.

1.6 Dissertation Structure Overview.

This thesis is divided into six chapters. Chapter One *Introduction* gives a brief outline of the growth of online business and cookies. It also gives some background to the legislative and enforcement regime and sets out the main research aims and objectives. A short description of the research methodology is provided as is a brief overview of the structure of the dissertation.

Chapter two *Literature Review*. The literature review examines academic work related to this study. It examines the research from three different perspectives, namely the background on privacy concerns, privacy law and finally on awareness. It identifies themes and areas for further research throughout the document.

Chapter three discusses the *methodology* chosen to best optimize answers to the questions posed in our research whilst Chapter four presents our *findings and discusses* these findings with a view to meeting the research objectives.

Chapter 5 presents in summary form our methodology and findings and recommends several policy changes that may improve awareness and enforce compliance of this privacy legislation. It concludes how the study achieves its aims and objectives in the end.

1.7 Positionality of Researcher

My background as a CEO of a national Irish retailer with a significant digital presence and a qualified lawyer has given me an acute awareness of the benefit of, but also the sensitive nature of consumer data and how we must incorporate consumers privacy concerns into our Digital Marketing and privacy policies for a mutually beneficial relationship. In addition, our company was part of the DPC initiated Cookie sweep of websites in 2019 and noted that, only that we were part of this sweep we would not have been aware of the directive and at the time would not have been in compliance with the current ePrivacy regulations.

1.8 Limitations

Certain restrictions regarding the scope of the dissertation should be acknowledged from the outset. Firstly, it will be restricted to an examination of the awareness and effectiveness of the ePrivacy law one year after the updated guidance from the DPC and to what can be done to improve compliance with this law from a policy perspective. It does not examine emerging use of technologies such as browser fingerprinting, deep packet inspection, history sniffing or Google FLOC or Apple IOS.5

Having narrowed the scope of the research it is now worth outlining the focus of the research through the literature review.

Chapter 2: Literature Review.

2.1. Introduction

This chapter reviews the relevant literature on the awareness of the ePrivacy directive and explores previous research on this and related topics of privacy, legislation, and awareness. The researcher reviewed a wide range of academic journals, government publications, books, advisory briefings, and other relevant literature to inform him of the background to the research topic and help lay a foundation on how to best answer the research question by reviewing how other researchers approached the relevant topics.

The review is broken down into three stages. The first stage 2.2 reviews the literature around privacy concerns, the second stage 2.3 reviews the legal position and the final stage 2.4 examines in detail past research on awareness and awareness studies.

2.2 Background on Privacy Concerns.

Social media and the information/digital age have redefined privacy. The growth of social media has made it easier than ever for consumer information to be collected, sold, and shared leading to rising customer concerns about privacy. In recent years however, privacy issues associated with Internet use have become increasingly important while the public have become more concerned about online privacy. YouGov research reveals 72 percent of British consumers are concerned about their private information online, and the UK Commissioner's Office (ICO) urges businesses to invest in data privacy (YouGov, 2015).

A 2019 SmarterHQ survey found that 86% of those polled were concerned about their data privacy with 79% of consumers believing companies know too much about them. (SmarterHQ, 2020). 74% of the consumers surveyed say that push notifications are the most invasive channel because they view their phone as an everyday tool that's part of their personal space and accordingly 63% say they would stop purchasing products and services from companies that take "creepy" marketing too far. In line with these trends the theory of **surveillance capitalism** has been proffered by (Zuboff, 2015) which effectively proposes a theory of mass surveillance and commercialisation of data by Google and the main social media sites that will result in a new form of capitalism ruled by the invisible hand of the keeper of the data. Zuboff proffers the theory of surveillance capitalism

as an accumulation of data by the big internet and social media players that aims to predict and modify human behaviour as a means to produce revenue and market control. Many of the practices associated with capitalizing on these opportunities challenge social norms associated with privacy and are contested as violations of rights and laws. She further states that as a result, Google and other actors learned to obscure their operations, choosing to invade undefended individual and social territory until opposition is encountered, at which point they can use their substantial resources to defend at a low cost what had already been taken.

2.2.1 Privacy Paradox

Although all the articles reviewed identify privacy as a major concern for consumers using these media platforms there is conflicting evidence of how much it actually affects their usage on the Internet. Martin (Martin, 2020) ,referred to the **privacy paradox** as referenced by academics and practitioners as the tension between consumers 'stated privacy preferences, as measured in surveys, and their actual behaviour, as measured by consumers 'continued online activity. The Privacy Paradox argues that there is effectively a gap between privacy attitudes and social behaviour and that whilst individuals might be concerned about their privacy it does not prevent them sharing their information online without protecting their online behaviour possibly with the purpose of achieving greater benefits from the online transaction. Indeed, in an online shopping experiment that compared self-reporting privacy preferences of people with their actual self-disclosing behaviour, found out that a majority of the test participants- regardless of their previously stated privacy attitudes – disclosed a large amount of personal information (Spiekermann, et al., 2001).

Potzsch (2008) advocated greater privacy awareness tools to counteract the privacy paradox and stated that people can make informed decisions when not only the benefits of disclosing personal data are pointed out to them, but when they are also reminded about their intentions toward privacy and the existence of possible data recipients. It is important to note that whilst this paper provided valuable information on privacy awareness, it predated the ePrivacy directive which implemented the type of transparency enhancing tools advocated by Potzsch as a technological solution to the privacy paradox.

More recent literature explores theories explaining the privacy paradox and mainly considers general internet activities with a focus on e-commerce and social networking activities (Barth, et

al., 2019). In this paper the authors reviewed the emergence of the privacy paradox through affected lenses, differentiating decision making according to a rational risk-benefit calculation, a biased risk-benefit calculation, and a decision-making process that involves no or only negligible risk considerations. They concluded that concrete proposals to tackle the problem of paradoxical behaviour remain scarce and advocated that designs of mobile applications should be adapted to different cognitive styles. Similarly, in a 2017 review of current research on the privacy paradox phenomenon, (Kokolakis, 2017) contented that a narrow definition of the privacy paradox could encourage online controllers to increase the collection and use of personal information based on consumers' often careless online behaviours despite their self-reported concerns about privacy.

He concludes that people still expect their privacy to be protected despite their behaviour and pointed out that privacy behaviour, awareness campaigns, and the availability of privacy-enhancing technologies have been under-researched. One solution to the privacy paradox is to be more transparent about how organisations collect, store, and use data. Being transparent on how data is collected and stored by following proper privacy regulations will lead to organisations collecting less meaningless data and encourage them to collect more targeted data, and the more targeted the data, the more efficient our data use must become. For most consumers, it is about how the data is collected and used, and not necessarily what data attribute is being collected (Harriot, 2021).

2.2.2 Privacy Regulation and consumers concerns over privacy.

The EU have since 2002 in an effort to protect people's privacy online attempted to protect people's data via the ePrivacy directive as revised, as traditional legal principles have struggled to come to terms with the rapid proliferation of internet technologies. The rigidity of the legal framework contrasts strongly with the fluid and ever-changing online sector. Our review of the literature indicates that despite every organisation stated concerns over privacy, apart from their legal obligations around GDPR they may be missing the bigger picture of allaying consumers concerns by being up front with them about how they use their data resulting in a better mutually rewarding relationship. Evidence of this can be gleamed from the (SmarterHQ, 2020) report in which 50% of consumers trust Amazon over brands to use their data responsibly outperforming Apple, Google, and banks. Amazon's policy of product recommendations, openness, peer reviews

and loyalty help customers feel safe and understood, this I feel could be the starting position for all organisations developing an online policy. Openness and transparency appear to be lacking in a lot of the policies as they blindly follow the gold rush to collect data no matter what the cost. Further, some of the research also suggested that notices that are perceived by consumers to be obfuscated or excessively legalistic can contribute to skepticism (Milne & Culnan, 2004). If consumers are not comfortable with what and how marketers use their online data, consumers may develop negative attitudes which may in turn impact consumers purchasing intention and lead to a loss of trust and damaged relationship between the parties. Recent research finds that consumers perceptions of using social media have a relationship with their comfort with marketers using their public available social media data (Jacobson, 2020) The research extends the applicability of communication privacy management (CPM) theory to social media and introduced a new construct of *marketing comfort* which refers to an individual's comfort with the use of online information for targeted advertising, customer relations, and opinion mining.

This follows from the conclusion of (Slyke&J.T.Shim&Richard, 2006) in relation to their construct of concerns for information privacy (CFIP) where they found evidence that consumers concern for information privacy affect willingness to conduct transactions with an online merchant under certain conditions. They concluded that organisations might be better served by putting their efforts into other means of reducing risk and increasing trust and familiarity rather than by focussing on reducing consumers' privacy concerns alone. It could be argued however that one of the pillars of increasing trust and reducing risk is to develop and open and transparent privacy policy, indeed in the same article consumers had higher CFIP whilst using Amazon as against a lesser-known web merchant as they had lesser concerns about security risk and trust with them and thus placed more emphasis in CFIP which may be why Amazon have developed a more open policy than some of their peers.

2.2.3 Cookie Fatigue

A Deloitte survey across a sample of both consumers and organisations to gain insights into attitudes towards privacy since GDPR became enforceable on the 25 May 2018 found that, even though more transparent cookie notifications have been in place since 2011, 65% of the respondents agreed that excessive use of cookies is a concern for them (Deloitte, 2020). Regarding this, the EU body Regulatory Fitness and Performance (REFIT), which is in charge of verifying

effectiveness of directives, states the current rules end being counter-productive as “the constant stream of cookie pop-up-boxes that users are faced with completely eclipses the general goal of privacy protection as the result is that users blindly accept cookies” (REFIT, 2016). This is commonly known as ‘**cookie fatigue**’ and demonstrated the challenges that both organizations and consumers face given the apparent apathy or reluctance to understand more about them. Rather than giving power to consumers, the current model seems to blind consumers as to what data privacy even means, it seems to be easier to just click “accept’ and move on.

2.2.4 Future Research

Although a solid backdrop on consumers’ privacy concerns and how companies develop policies to alleviate these exists, there is need for additional research into how much Companies consider privacy concerns in developing their digital marketing practices and conversely how much consumers consider this in their online activity.

Although there is a lot of international research on privacy and consent notices and pop ups in this field there is limited research in Ireland apart from the usual online usage and privacy surveys, there is a gap in the research about how organisations are moulding their policies to reflect the public’s growing unease with how they use their data. By becoming more transparent about data collection and use and reassuring the public about the ethical integrity of how they are using their data, Companies can help build the much sought after trusted relationship with their consumers which should be to their mutual benefit into the future. Part of our research will inquire how companies are complying with the ePrivacy directive in Ireland and reasons for their noncompliance. I intend to also research what value they place on consumer privacy as vehicle for growth or do they just regard all these regulations as just more legislation which has to be complied with. Secondly as I develop the thesis, I may want to look at consumers attitudes towards Companies using their online data, how companies can harvest this concern for mutual benefit might however be a more fertile platform for growth rather than minimal compliance with privacy protecting legislation.

2.3 Background on Privacy law.

There are two main legal concerns in relation to online privacy, firstly in relation to the common law tort of breach of privacy and secondly through the statutory control by the legislature. This thesis will concern itself mainly with statutory control.

2.3.1 Statutory Control-Privacy

Current regulatory requirements for cookie consent notices on websites are derived from the ePrivacy Directive (ePD) which was transposed into Irish law in the 2011 ePrivacy regulations and personal data collected from Cookies and tracking technologies must be processed in line with the General Data Protection Regulation (GDPR). In May 2019, the General Data Protection Regulation (GDPR) outlined that it is unlawful to process personal data without the consent of the individual concerned. By virtue of this law privacy notices must be given to individuals to indicate how their personal data will be processed and in order to make that consent valid, it must be “freely given”, it must be “specific and informed”, it must be “explicit and unambiguous” and for Under 13’s consent must be provided by parents.

Any breach of GDPR may result in fines or prosecution and organisations have devoted many resources to comply with GDPR, aware of the threat any breach brings. There are however some pitfalls that threaten the individual control envisaged by this legislation such as information complexity, literacy, information overload, information asymmetry, data invisibility, and intangibility (Gurkaynak, 2013). There are also concerns about how companies document privacy policies and terms of service with some empirical research to suggest that the vast majority of people (74%) visiting websites ignore the privacy policies and see privacy policies as nothing more than an unwanted impediment to sole purpose to get online (Obar, 2016). What is apparent however from reviewing the articles that there is patchy compliance with the ePrivacy directive across Europe and not just limited to Ireland. A 2019 longitudinal study of the EU Cookie law over a four-year period found that of 10,000 websites tracked by the study on average 74% install cookies from third parties before any user consent (Trevisan, et al., 2019). A 2020 empirical study of Consent management systems (CMP’s) introduced to the web to conform with the GDPR and ePrivacy regulations found that many of them are configured illegally and only 11.8% meet the minimal requirements set by European law (Nouwens, et al., 2020) .

What is becoming clear from reviewing the literature is that for this level of noncompliance to be so prevalent businesses must be either unaware of the legislation or more concerning wilfully ignoring it. By having disregard for the legislation designed to protect consumer privacy is ignoring growing concerns over Internet privacy and the role of the Big Data companies in harvesting, using, and selling this data.

2.3.2 ePrivacy Regulation

The ePrivacy directive is in the process of being replaced by the new ePrivacy Regulation which is currently going through the legislative process in Europe. It is intended to complement, add to, and underpin the requirements of the GDPR. Its territorial reach is the same as the GDPR in that it includes any data gathered from data subjects in EU countries by international organisations, and it applies to all direct marketing through electronic means. Crucially the instrument is a regulation rather than a directive, meaning it will like GDPR, have direct effect in Member States, there will be no discretion in how Member States transpose it into law, and Data Protection Authorities across the EU will be solely responsible for its enforcement. This is important as Comreg in addition to the DPC, currently share the enforcement function for part of the ePrivacy Directive leading to some confusion over who is responsible for regulation and limiting enforcement actions. A directive is a legal act of the European Union that requires member states to achieve a particular result without dictating the means of achieving that result. Directives first must be enacted into national law by member states before the law takes effect and member states have a certain amount of leeway as to how the rules are adopted. Directives can be adopted into national law by means of a variety of legislative procedures the most common of which is Statutory Instruments in Ireland. A "Regulation" is a binding legislative act. It must be applied in its entirety across the EU, and it has direct effect meaning that it automatically becomes part of the laws of the member states with no discretion as to how it is adopted. When an EU regulation enters into force, it becomes directly and immediately applicable within EU countries.

2.3.3 Dark Patterns

Furthermore, there is a lot of debate in the literature about consumer privacy and the right to make informed choices. There is evidence that there is a growing trend to try and influence the consumer into a choice that is most advantageous to the providers of digital services. Interface

designs that try to guide end users into desired behaviour through malicious interaction flows are referred to as '**dark patterns**' (Gray, et al., 2018).

As a phenomenon they are part of a larger agenda around persuasive design and nudging. '**Nudging**' describes undue influence on the user's decision to provide or refuse consent (Klingebiel, 2021).

This area has been extensively reported on by consumer protection organisations most notably by the Norwegian Forbrukerradet (consumer council of Norway) in their influential 2018 document "deceived by design" (Forbrukerradet, 2018). In that report, they analyzed a sample of settings in Facebook, Google, and Windows 10, and showed how default settings and dark patterns, techniques and features of interface design meant to manipulate users, are used to nudge users towards privacy intrusive options. The findings include privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users. (Forbrukerradet 2018). They concluded that the combination of privacy intrusive defaults and the use of dark patterns, nudge users of Facebook and Google, and to a lesser degree Windows 10, toward the least privacy friendly options to a degree that they considered unethical. The infamy of this report led the European Union and data protection officers to specifically highlight common dark patterns as non-compliant with the DPC in their 2019 cookie sweep concluding that a so called 'nudging' approach to the web design by the participants of the sweep was common, with users effectively forced into accepting all cookies. (DPC 2020, pg7). They also noted that badly designed or even potentially deliberately deceptive cookie banners and consent management tools were also a feature on some sites (DPC 2020, pg., 8)

2.3.4 Common Law

In relation to the common law regulation of the Online Industry the courts worldwide have been lax in regulating privacy concerns to the same extent as they have in more traditional contracts or traditional media channels and have struggled to keep up with technological advancements in the Online sphere.

The worldwide legal cases to date indicate a growing consensus on the extent of search engine liability. Because a search engine operator or social media platform does not create, change, and

upload the content on the Internet, it cannot be held liable for infringement nor does it have any obligation to monitor content and is not accountable for infringing the protected content rights of third parties (Gurkaynak, 2013) . In addition because they aggregate, analyse and anonymise data it is difficult to argue clearly that they are breaching an individuals' right to privacy although it has been argued by (Zuboff, 2015) that Google develops a declarative model that it repeats into other ventures , namely that of incursion into undefended private territory until resistance is encountered. In Street View Google does not ask if it can photograph homes for databases, it simply takes what it wants. Google then exhausts its adversaries in court or eventually agrees to pay fines that represent a negligible investment for a significant return (Zuboff, 2015). Traditional legal principles have struggled to keep up with the rapid proliferation of internet technologies making the ePrivacy directive and proposed ePrivacy Regulation and the GDPR being the most important protection of peoples' data in Europe.

2.3.5 Future Research

Although there is case law to help in this area there is need for additional research into how much marketers consider legal concerns in developing their digital marketing not just concentrating on GDPR but on how they are harvesting data about their customers without their knowledge or at least in the full knowledge that consumers are not heeding cookie or Privacy Policies or Terms of service.

Organisations may benefit from embracing rather than hide behind this, passive surveillance and basic protections may well not protect against the tort of Appropriation that of stealing someone's' identity (name, likeness) to gain advantage without the full permission of the individual. To claim that they have a full Privacy Policy in place with the knowledge that the vast majority of users do not check these may not give them the legal protection they may think they have. The old maxim in equity law of " He who comes to law must do so with clean hands" may be pertinent here, saying that you comply in the full knowledge that people disregard the notices may not give people the legal protection they think they have.

Defining a User-Centric Cookie Experience may support organisations in creating a cookie compliant, yet user friendly and branded privacy experience for online customers. I would posit from reviewing the literature that organisation's envisioned functionality and use of cookies could

be molded to a more customer-centric approach to help give companies a competitive edge particularly regarding consumers stated concerns for privacy.

2.4 Background on Awareness Concerns.

Awareness is based on an individual's attention, perception, and cognition of physical as well as non-physical objects (Potzch, 2009). The state of being aware of something fades away as soon as there is no longer any stimulus present. Awareness in this study refers to awareness of the legislation in place, reasons for its existence and penalties for non-compliance. I would like to explore the correlation between awareness of legislation and compliance.

2.4.1 Awareness Studies

Studies of the awareness of the ePrivacy directive amongst consumers and controllers are limited. For the purpose of this review, I had to rely on awareness studies in other areas for guidance on the constructs and methodology to prepare for this study. Other fields reviewed included computer supported co-operative work, privacy awareness studies, environmental awareness studies and road safety awareness which provided a fertile ground for research in this area. Importantly a 2015 study on Cyber security awareness campaigns provided pertinent information on awareness campaigns and people's behaviour (Bada, et al., 2015).

The concept of privacy awareness as perpetuated by (Potzch, 2009) in an article on the privacy paradox was helpful in that it explored privacy awareness which is very relevant in the context of the ePrivacy directive. In addition, the concept that raising awareness is essential for ensuring compliance with legislation (Wynveen & Sutton, 2017) is significant for this research. According to the (OECD, 2010) promoting environmental awareness seems to work best in situations in which farmers have a high awareness of consequences of failing to adhere to the regulations regarding farming systems and public health.

2.4.2 Awareness Campaigns

Perhaps the most relevant study for our dissertation which most closely relates to our subject matter relates to an article on Cyber security Awareness Campaigns and why they fail to change behaviour. (Bada, et al., 2015). This article sets out the reasons for the failure of cyber security awareness campaigns, findings which may help in researching the effectiveness of awareness

campaigns around the ePrivacy directive as in both cases it seems that past and current efforts have not had the desired impact.

This article very helpfully sets out what they believe are the essential components for an awareness campaign as well as the important factors which can lead to a campaign's success or failure namely communication, the fact that fear invocations have often proved insufficient to change behaviour, education, and perceived control. In relation to cyber security awareness campaigns, they found that an awareness and training program was crucial, in that, it is the vehicle for disseminating information that all users (employees, consumers and citizens, including managers) need. In the case of an Information Technology (IT) security program, it is the typical means used to communicate security requirements and appropriate behaviour. An awareness and training program can be effective, if the material is interesting, current, and simple enough to be followed. Any presentation that 'feels' impersonal and too general as to apply to the intended audience, will be treated by users as just another obligatory session (Bada, et al., 2015). Arising from this it should be noted that according to (Dolan, et al., 2010) the main factors which influence human behaviour and behaviour change are set out in Figure 2 below. In this paper on how to influence behaviour through public policy they outlined nine robust influences on human behaviour and change. These principles are underpinned by considerable research from the fields of social psychology and behavioural economics. They are therefore presented as the most robust effects that policymakers should understand and, if appropriate, use.

Messenger	we are heavily influenced by who communicates information
Incentives	our responses to incentives are shaped by predictable mental shortcuts such as strongly avoiding losses
Norms	we are strongly influenced by what others do
Defaults	we 'go with the flow' of pre-set options
Saliency	our attention is drawn to what is novel and seems relevant to us
Priming	our acts are often influenced by sub-conscious cues
Affect	our emotional associations can powerfully shape our actions
Commitments	we seek to be consistent with our public promises, and reciprocate acts
Ego	we act in ways that make us feel better about ourselves

Figure 2 Main Factors which influence human behaviour and change (Dolan et al., 2010).

These factors can influence the user's motivation to adopt the knowledge offered by an awareness campaign and are important as psychological tools in maximising the benefit of awareness campaigns.

2.4.3 Factors to increase the effectiveness of an awareness campaign.

In addition, this paper gave a succinct review of the psychological theories of awareness and behaviour and considered them to gain insights as to why awareness campaigns often fail. In summary Dolan et al (2010) state that simple transfer of knowledge about good practices is far from enough. Knowledge and awareness are a prerequisite to change behaviour but is not necessarily sufficient, and therefore it must be implemented with other influencing strategies such as training and enforcement. Additionally I researched a study on to how to measure awareness in a lead based paint survey commissioned by the Department of Housing and Urban Development(HUD) in the US in an effort to evaluate the impact of legislation containing changes pertaining to the control of lead based paint hazards and the reduction of lead exposure (Ciochetto & Haley, 1995). This paper focussed on the process used to design a series of questions that could

produce baseline measures of awareness and knowledge about lead based paint hazards and was most helpful in framing our research questionnaires around awareness. This study found that measuring awareness or knowledge can create some challenges. It is important to measure what respondents know as well as what they do not know. This paper found that there is a risk that people respond by guessing rather than admitting that they do not know and questions regarding awareness and knowledge must be structured so that respondents feel comfortable reporting a “don’t know”. This was a landmark study in structuring and influencing our consumer and business sector questionnaires to get as accurate picture as possible of their actual awareness.

2.4.4 Future Research

Research in this field seems to be largely concentrated on awareness studies in healthcare, environmental regulations, computer supported cooperative work, cloud computing, road safety and cyber security awareness. These articles whilst not specific to the ePrivacy directive provided excellent data on the essential components of an awareness campaign and which factors which can lead to a campaign’s success or failure.

Based on our review of the literature and analysis of several awareness campaigns I would suggest that the following factors as advanced by Cartwright in a 2020 paper on why cyber security awareness campaigns fail can be helpful in enhancing the effectiveness of an awareness campaign and guide us in our examination in studying the awareness of this directive (Cartwright, 2020). He set out several factors that could be helpful in enhancing the effectiveness of current and future awareness campaigns.

(1) Try and find the optimal balance of awareness on a subject, too little awareness may lead to noncompliance or delayed implementation whilst too much awareness may lead to fatigue as the requirements are perceived by the user as merely an obstacle preventing them from their primary task.

(2) Invoking fear in people is not an effective tactic as it could encourage people who least can afford it to take risks (Bada et al., 2015).

(3) Awareness campaigns need to be targeted, actionable and doable.

(4) The perception of co-responsibility is important for an effective awareness campaign making the targets key stakeholders in the process.

(5) The Regulator's willingness to enforce legislation influences the awareness of legislation.

(6) Knowledge of the penalties for noncompliance may be an important factor in the success or otherwise of an awareness campaign.

2.5 Conclusion on Literature Review.

Despite of the aforementioned privacy paradox which refers to the gap between privacy attitudes and social behaviour, the research shows that consumers retain privacy expectations after disclosing information and judge the sharing of information with third parties and the secondary use of this information to be a violation of trust. As consumers become more careful about sharing data, and regulators step up privacy requirements leading companies are learning that data protection and privacy can create a business advantage. As consumers increasingly adopt digital technology, the data they generate create both an opportunity for enterprises to improve their consumer engagement and a responsibility to keep consumer data safe. These data, including location-tracking and other kinds of personally identifiable information, are immensely valuable to companies: many organizations, for example, use data to better understand the consumer's pain points and unmet needs. These insights help to develop new products and services, as well as to personalize advertising and marketing (the total global value of digital advertising is now estimated at \$300 billion) (McKinsey, 2020). By embracing people's privacy concerns will help business grow and thrive, as Microsoft's Brad Smith opines 'Had Microsoft continued its assaults on regulators and the competition, we wouldn't be the most valuable company in the world today. We wouldn't have been given the opportunity. We had to persuade people that we deserved the trust,' (Rathesar/Redmond, 2019). Awareness is a key component in the success of any legislation and together with other influencing strategies such as enforcement can influence the rate of compliance with a law. Awareness campaigns are important factors in increasing awareness about a particular issue and the literature shows that awareness campaigns are important in educating people about different topics which in turn may influence their behaviour in a positive fashion.

Table 1 below sets out the key findings in summary form from the review of the literature.

The main knowledge gap that is addressed in this thesis is the level of awareness of the directive amongst the public at large. Based on our research it was found that there is a gap in knowledge on the level of awareness of the directive and whether this has contributed towards the low level of compliance and the following questions were developed to support the pursuit of our research objective and address the knowledge deficit in this area.

- 1.** What is the level of awareness of the directive amongst the public at large one year after updated guidance from the DPC? We sought to measure this by surveying the level of awareness amongst consumers, the business community, and the regulator.
- 2.** Whether there was a relationship between the level of awareness of and compliance with the directive?
- 3.** How can increasing the level of awareness of legislation influence public policy in a positive way?

Table 1: Themes from review of literature.

Authors	Origin	Purpose	Type of Source	Major Themes from Literature
DPC (DPC,2020).	Ireland	Examination of the use of cookies and similar technologies across a range of sectors.	Report	Bad Practices were widespread, controllers were not in compliance with directive, increase in enforcement coming.
Zuboff (Zuboff, 2015).	USA	An examination of the nature and consequences of computer mediated transactions.	Journal	A theory of mass surveillance and commercialisation of data by Google and the main social media sites that will result in a new form of capitalism ruled by the keeper of the data.
Martin (Martin, 2020)	UK	To examine the conceptualisation of privacy post disclosure assumed in the privacy paradox.	Journal	Privacy paradox, the tension between consumers stated privacy preferences as measured in surveys and their actual behaviour.
Refit (Refit, 2016)	Europe	Regulatory overview of fitness and performance of directives.	Report	Talks about cookie fatigue demonstrating the challenges that both organisations and consumers face given the apparent apathy or reluctance to understand more about cookies.
Forbrukerradet (Forbrukerradt, 2018)	Norway	To sample settings in Facebook, Google and Windows 10 to show how default settings and dark patterns, techniques and features of interface design are meant to manipulate users or nudge them to privacy intrusive options.	Report	Combination of privacy intrusive defaults and the use of dark patterns, nudge users to the least privacy friendly options.
Bada et Al (Bada et.al, 2015)	UK	To identify key factors regarding cyber security awareness campaigns which may lead them to fail to appropriately change peoples behaviour.	Report	Essential components of awareness campaigns as well as the factors which can lead to a campaign success or failure. Among the factors identified include communication, awareness and training.

Chapter 3 Methodology.

3.1 Introduction.

Raising awareness is essential for ensuring compliance with legislation. (Wynveen and Sutton, 2017). This chapter discusses the methodological choice of research chosen to measure the awareness and effectiveness on a regulatory, business, and consumer level of the updated E.U. privacy and Electronic Communication(ePrivacy) directive (S.I.No. 336/211), one year after updated guidance from the DPC. Our review of the literature would indicate that both awareness of and compliance with the directive is low and after extensive research on the optimal research approach, detailed extensively later in this chapter, I chose a mixed-methods approach, in two phases. Firstly, an anonymous survey was administered to a consumer segment followed up by one-to-one interviews with the business cohort and Regulator to follow up on issues that required deeper exploration. The data collection instruments consisted of consumer surveys as well as semi-structured interview data with the business and regulatory cohorts.

In terms of the order of the data collection, I sought to measure the awareness of the directive amongst the consumer and business cohort firstly to be in a position to present these results to the Regulator for comment and further insights from their perspective. The timing of the research was coordinated as best we could to measure awareness of the directive one year on from the updated guidance from the DPC in April 2020 following on from their Cookie Sweep of various websites in 2019. This chapter consists of five main sections with the first 3.2 giving some context to the study. Section 3.3 focuses on the research design, sampling, and instruments of data collection, section 3.4 is largely concerned with survey design whilst section 3.5 sets out the data analysis methodology and ethics. Finally, section 3.6 sets out the limitations of the methodology.

3.2 Context of the Study.

Subsequent to the cookie sweep in August 2019 the DPC issued a guidance note on cookies and other tracking technologies accompanying the release of the report outlining the results of the sweep. It is the most significant and detailed guidance that the DPC has issued to date on the processing of cookies and similar tracking technologies. Based on the results of its sweep, the DPC identified widespread failures and concluded that many organisations may misunderstand what is required of them, with only two of the 38 organisations surveyed being given a “green grading,”

meaning that the DPC found them to be substantially compliant. Importantly, a six-month grace period was allowed for controllers to bring their cookie processing practices into alignment with the legislation at which point, the DPC has indicated that further action including enforcement will be considered. The DPC had through its Cookie sweep identified widespread non-compliance amongst website controllers and this study aims to measure firstly awareness of the directive and whether the awareness or lack thereof contributed to this phenomenon and whether a more robust awareness campaign could have increased awareness and compliance with the directive and suggests some policy changes.

3.3 Research Design, Sampling, and Data Collection

3.3.1 Pilot Study

Post ethics approval pilot studies were carried out in May and June 2020 to pretest questions for both our interviews and consumer questionnaires.

A total of four social contacts were used as participants in the consumer segment of our study which was conducted in June 2020 and further refined in October before the detailed questionnaire was sent out. Feedback from these contacts was mainly in relation to the understanding of two questions which presented a difficulty for all respondents and one suggested explanation boxes would be helpful on two questions for further elaboration. In one question I had asked what the single most important device for getting online was but allowed for multiple answers. In addition, my supervisors warned of the dangers of dichotomous questions and helped in advising on how questions and scales should be structured to give a clear understanding of the meaning of each point on the scale and to structure the questionnaires from the general to the specific. As preparation for our interview with the business cohort, the researcher interviewed one Omni channel retailer and discussed the interview template and questions with my supervisor prior to the interview, and further refined the questions post-interview. This allowed me to hone my interview technique and refine the questions to eliminate overlap and try and ensure we got more relevant information in a short timeframe.

Finally, I interviewed a partner on one of the big six law firms who specialize in data protection to learn more about the directive and possible enforcement and penalties to try and frame a more specific interview for the Regulator who had obvious awareness of the directive but whom I

intended to probe on why other cohorts lacked such awareness. Feedback from the pilot questionnaires and interviews proved very helpful and enabled us to prepare relevant questions, hone our interview technique and ensure that I am gathering relevant information in our limited timeframe.

3.3.2 Study Design

Early on in our study, the researcher carried out extensive research to find an optimal design that would help answer the research questions posed.

1. What is the level of awareness of the directive amongst the public at large one year after updated guidance from the DPC? We sought to measure this by surveying the level of awareness amongst consumers, the business community, and the regulator.
2. Whether there was a relationship between the level of awareness of and compliance with the directive?
3. How can increasing the level of awareness of legislation influence public policy in a positive way?

As part of our studies on the optimal research approach to adopt I reviewed qualitative, quantitative, and mixed methods approach to best deal with our research problem. According to (Creswell, 2014) research approaches are plans and the procedures for research that span the steps from broad assumptions to detailed methods of data collection, analysis, and interpretation.

3.3.3 Quantitative Research

Quantitative research encompasses a range of methods concerned with the systematic investigation of social phenomena, using statistical or numerical data (Watson, 2015). Quantitative research involves measurement, and it is essential that what is being researched can be measured and then analysed for trends and relationships and verify the measurements made. According to (Holton, et al., 2005) quantitative techniques are particularly strong at studying large groups of people and generalizing from the sample being studied to broader groups beyond that sample. There are some limitations and weaknesses of this research method that the researcher needed to be mindful of in the research process. The main limitations and weaknesses of this research method are an improper representation of the target population, inability to control the

environment, limited outcomes due to mainly close-ended questions, and the fact that this research is difficult, expensive, and requires a lot of time to perform the analysis (Chetty, 2016)

3.3.4 Qualitative Research

Qualitative research is the systematic inquiry into social phenomena in natural settings. These phenomena can include but are not limited to, how people experience aspects of their lives, how individuals and/or groups behave, how organizations function, and how interactions shape relationships (Teherani, et al., 2015). In qualitative research, the researcher is the main data collection instrument, and this approach gives the researcher a greater ability to explore more detail about the research problem. In qualitative research, however, the subjective nature of the information that can be gleaned from such methods as interviews and case studies mean that they are open to interpretation and observer bias (Johnson, 2018) . In addition, because of its subjective nature and small sample size qualitative findings cannot be generalized to broader groups beyond the sample.

3.3.5 Mixed-methods Research

Creswell (2014) defines mixed methods research as an approach to an inquiry involving collecting both quantitative and qualitative data, integrating the two forms of data, and using distinct designs that may involve philosophical assumptions and theoretical frameworks. The core assumption of this form of inquiry is that the combination of qualitative and quantitative approaches provides a more complete understanding of a research problem than either approach alone. (Creswell & Plano-Clark, 2007) pointed out that conducting mixed methods research is not easy, and (Bryman, 2007) indicated that there are several barriers. Mixed methods studies are a challenge because they require more work and resources and take more time. Increased time demands arise from the time it takes to implement the quantitative and qualitative parts of the study and it also requires that researchers develop a broader set of skills that span both quantitative and qualitative. Mixed methods research has developed rapidly in these last few years, emerging as a research methodology with a recognized name and distinct identity, especially in some fields such as education, health sciences, psychology, and sociology (Denscombe, 2008). Through our research for our literature review, our pilot study, and interaction with my supervisor we attempted to devise the most appropriate method of data collection for this specific research study. The

researcher investigated several scholarly articles in an attempt to choose the best research approach,

3.3.6 Review of literature around research approach

As no study was available examining similar themes to our research topic the researcher relied on literature from studies in other fields where the research methodology helped answer similar research questions, particularly around knowledge, behaviour, compliance, and awareness. Interestingly most of these studies were in the fields of health sciences, psychology, and legislation.

A 2019 German study on nurses' knowledge, behaviour, and compliance concerning hand hygiene in nursing homes influenced the researcher in his approach. A two-phased mixed methods study was adopted surveying 165 nurses and interviewing 27 nursing managers from nursing homes in Germany. The survey results and interview transcripts were analysed independently by several researchers with the findings integrated at the interpretation stage contributing, according to the authors to a more complete, balanced, and insightful portrait of the phenomena under investigation (Hammerschmidt & Manser, 2019).

Additionally, a 2020 paper on how to integrate data in a midwifery research project noted that the mixed methods study design combines the strengths of both quantitative and qualitative approaches to answer research questions (Othman, et al., 2021). This design includes quantitative and qualitative phases, and each phase is undertaken independently, followed by combining quantitative results and qualitative findings for a broader purpose and in-depth understanding of the research questions and phenomena. In this paper, the researchers used a variation of the mixed methods design namely a sequential explanatory mixed methods design. Creswell (2014) defines this design method as involving a two-phase project in which the researcher collects quantitative data in the first phase, analyzes the results, and then uses the results to plan (or build on to) the second, qualitative phase. He states that the overall intent of this design is to have the qualitative data help explain in more detail the initial quantitative results. Similarly, in a 2019 study on how knowledge brokers mobilized health evidence in low income and middle-income countries, the research team used a mixed methods explanatory sequential study design to firstly describe survey characteristics of knowledge brokers and their evidence sharing and user behaviour, and then qualitatively develop insights into the survey data to explain decisions made by the brokers in their intermediary role (Norton, et al., 2021). In this study, implementation began with a

collection of survey data and a limited amount of qualitative data using a self-administered online survey. The survey was followed by semi-structured interviews with a subset of survey respondents,

3.3.7 Chosen Research Method

After our review of the different research methods, an explanatory sequential mixed method design was considered the best approach to analyze the awareness and effectiveness of the implementation of the E-privacy directive (2019) across the three different stakeholder groups as outlined. As no existing survey was available to capture the awareness of the directive amongst consumers, I developed one specifically for the first phase of this study. I had knowledge from the DPC cookie sweep that there was poor compliance with the directive amongst the business sector and I chose to conduct semi-structured interviews to explore the awareness of the directive amongst this cohort. After triangulating the results from the consumer and business sectors I presented our results to the Regulator as part of our interview in an attempt to explain in more detail and probe answers to the initial results from the first two sectors.

One challenge in this strategy is to plan adequately what survey results to follow up on and what participants to gather qualitative data from in the second phase. The key sequence in our study was to take the results from the consumer and business cohort and use this data to follow up with the Regulator and explore the results in more depth. The key idea is that the qualitative data collection builds directly on the survey results.

3.4 Survey

The objective of the survey sampling strategy was to assess the level of awareness of the directive from a consumer perspective to provide data relevant for the interviews with the regulator. A survey design provides a quantitative or numeric description of trends, attitudes, or opinions of a population by studying a sample of that population. (Creswell, 2014). Survey design, subject privacy and confidentiality, sampling and subject solicitation, distribution methods and response rates, and survey piloting are critical methodological components that must be addressed in order to conduct sound online research (Andrews, et al., 2003). An online survey was chosen as opposed to a traditional survey method as it increased productivity by saving time and the data mined was instantly available and could easily be transferred into spreadsheets when a more detailed analysis

was needed. The economy of design and rapid turnaround in data collection was helpful in the sequence of research in that this data proved useful in our further interviews.

3.4.1 Survey Design

3.4.1.1 Consumer Sector.

In conjunction with my supervisors and from the research into best practices for designing and conducting online surveys the researcher designed a detailed consumer questionnaire to assess the level of awareness of the directive from a consumer perspective as set out in appendix B. Given the time pressure involved and cognizant of the resources required to conduct a random sample of the population the researcher selected a group of respondents from a larger population knowing full well that some members of the population had zero chance of being surveyed.

The two prerequisites to completing the study were.

- Participants had to be over 18 years of age
- Be consumers of online content

Whilst this form of non-probability sampling does not support formal statistical inference it is especially useful for identifying issues, defining ranges of alternatives, or collecting other sorts of non-inferential data (Fricker, 2012). **Non-probability sampling** selects a group of respondents from a larger population, knowing full well that some members of the population have zero chance of being surveyed. This is not allowed in **probability sampling**, which requires everyone in the population to have a *non-zero* chance of being selected (SurveyMonkey, 2020). In our case, this survey provided a quick and convenient method to investigate awareness of the ePrivacy directive amongst consumers for further research later in the dissertation. There was also an element of snowball sampling in our survey in that we invited all our respondents to recruit other participants for our study. Snowball sampling is where research participants recruit other participants for a test or study. It is used where potential participants are hard to find. It's called snowball sampling because (in theory) once you have the ball rolling, it picks up more "snow" along the way and becomes larger and larger (Glen, 2020). In keeping with our survey, it is a non-probability sampling method where the researcher used his own judgment to choose participants. A 2020 paper by (Bergman, 2020) proved helpful in survey design, providing overviews and click-by-click instructions for popular survey platforms and participant recruitment platforms. They set out the main considerations for designing an online survey as (1) considering

participants' ability and willingness to answer, (2) responses should be considered relative in that the researcher should assume that participants will be able to accurately report certain coarse facts, (3) Researcher should provide converging evidence, (4) Questions should be clear, concise, and simple and (5) the researcher should avoid leading questions. To achieve the best possible response rate and to investigate the awareness of the directive amongst a group of consumers the survey was sent to a wide range of social contacts, colleagues, and other contacts all of whom are users of online content. Some of these cohorts as known consumers of online content had previously indicated their willingness to participate in research projects for the researcher and had been used for newsletter circulation and testing scenarios as part of the exercises for the post-graduate certificate in 2020. The survey was sent to 61 contacts all of whom were invited if they so wished to pass it on to their peers and other contacts. In total 144 people responded to the survey, and only 1 did not complete it.



Figure 3: Online survey participants

The questions began at a more general level with inquiry about social demographic variables such as sex, gender, and age and questions about time spent online, preferred devices, and browsers and gradually got more specific about awareness of the directive and awareness of the GDPR regulations as a comparative, acceptance of cookie notices and whether consumers find them annoying and whether awareness needed to be improved. We also allowed the respondents the opportunity to expand on their answers to some important questions. Consumers were asked to complete the survey as consumers of online content and the average time to complete was 10

minutes. The survey consisted of 37 questions. In keeping with our research on optimal design for online surveys, questions were kept clear and simple, the responses time at an average of 10 minutes was short enough to keep the respondents engaged, leading questions were avoided, and respondents were asked a variety of questions to keep them engaged.

Confidentiality and anonymity were warranted as promised in the ethics approval form, (see appendix A), and it was explained that the information gained from this study will be used as part of a postgraduate thesis and possible presentation at some digital conferences in 2023. The questionnaire, though different from the interview technique used for the business sector allowed us to quickly survey a significant sample size and get a good barometer of awareness from this cohort which could be used for comparison purposes from the data collated from the business cohort.

3.4.1.2 Business Sector.

In total, I interviewed 8 organisations as a representative group of the business sector. The DPC cookie sweep in 2019 surveyed the websites of 38 well-known organisations across a range of sectors including, media and publishing, the retail sector, insurance, sport and leisure, restaurants and online ordering, and the public sector. The researcher endeavored to use a similar framework as used by the DPC to replicate some of the sectors examined, namely retail, insurance, online, and service sectors. Time constraints however limited us to interviews with 8 businesses across diverse sectors and with multiple turnover thresholds. Semi-structured interviews were conducted with the following individuals from the following business segments over October and November 2021 as set out in Table 2 below.

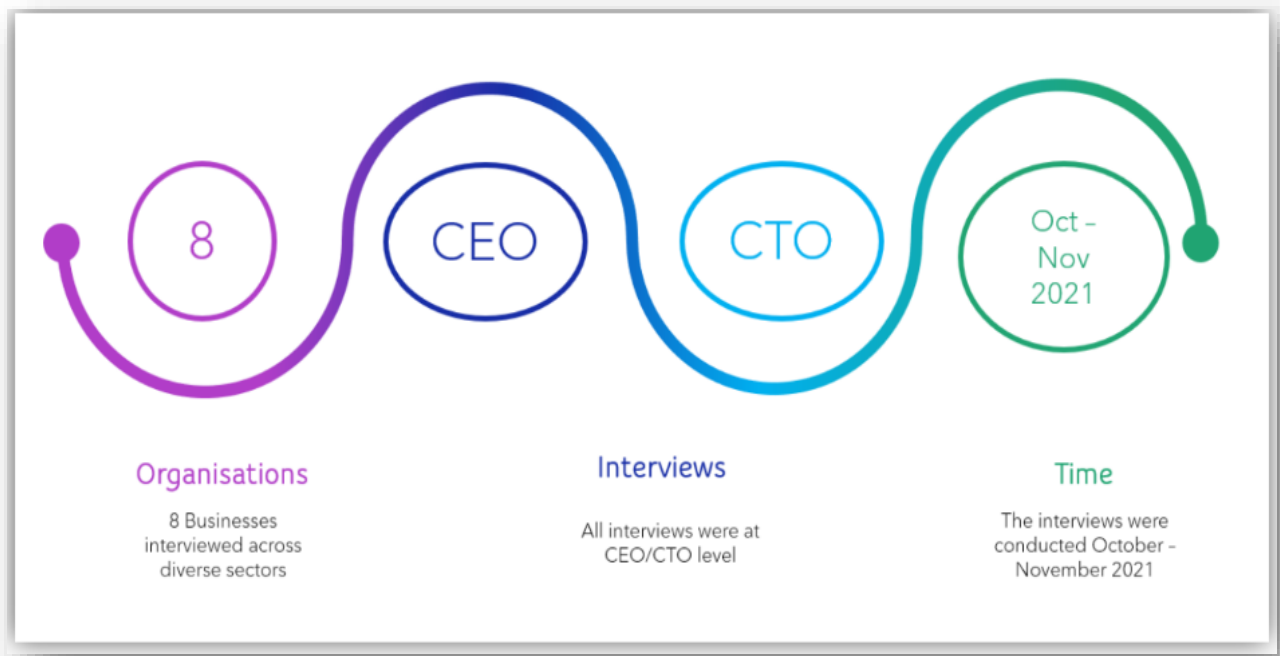


Figure 4: Business Cohort

Table 2: Business Segment Interviewees.

ORGANISATION	TURNOVER
One Small Omni Channel Retailer	Turnover 2m
One large national retailer	Turnover > 100m
One large Manufacturer with a significant DTC business	Turnover > 50m
One large Manufacturer	Turnover > 300m
One Online only player with significant recent investment rounds	Turnover 25m
One Digital agency	Turnover 10m (Estimated)
One leading law firm	Turnover 30m (Estimated)
One Insurance/Investment involved in financial service	Turnover 30m (Estimated)

All the interviews were at CEO (Chief Executive Officer)/CTO (Chief technology officer) level with two of the respondents bringing their DPO (Data protection officers)/Compliance officers on the interviews. All entities were provided with the questions before the interview and in line with the ethics form (see Appendix C); all signed and returned consent forms before the interviews. It was stated in the consent form that the questions were deliberately open-ended thus inviting the respondents to further elaborate on their views and the informal nature of the interviews allowed for an honest assessment of their awareness of the subject and enabled the researcher to look at the phenomena from different perspectives. Indeed, some of the respondents had filled in answers to the questions before the interview, and the interviews then allowed us to probe the validity of answers and encourage the respondents to offer more detail on certain areas. Different sectors were more regulated than others and consequently had a more disciplined approach to compliance but the spread of the business across diverse sectors allowed for a strong representative understanding of the awareness from a business perspective.

3.4.1.3 Regulator

The researcher deliberately scheduled the interview sequencing with the regulator to the end of the data gathering process to permit data collection from the business and consumer sectors to be presented to the regulator for comment.

The questionnaire for the Regulator was designed slightly differently for both the business and consumer segments in that it was populated with summary findings from the other sectors and prompted the Regulator to comment on the findings as set out in Appendix D. Cognisance was also taken in the design of the questionnaire of the advice imparted by a specialist data lawyer as part of the pilot survey. The representative from the DPC was a special investigator in the enforcement section and was the instigator of the cookie sweep in 2019 and involved in the publication of the guidance published in 2020. Like the consumer questionnaire the questions began with a more general focus and moved towards a more specific focus as the interview proceeded.

It took some time for the DPC to consent to an interview and involved a considerable amount of interaction and approval before the interview was granted. In this regard, the ethics approval form as set out in Appendix A form proved very useful in addressing their concerns prior to the interview, particularly regarding confidentiality and anonymity. The ethics form as finally approved after

revision in April 2021 formed part of a rigorous ethical approval process detailing the research summary, methodology, a risk checklist, and the main ethical considerations of the research process.

The interview with the Regulator allowed us to complete our data collection and it is the author's view that the multiple data collection methods across the different cohorts enabled us to increase the credibility and reliability of the data. As referred to above, it took almost two months for the Regulator to consent to an interview, and consent was only granted after four emails and two calls and being sent a detailed list of the questions to be asked at the interview. These questions as set out in Appendix D were populated with initial findings from the consumer and business cohorts. This interview was vital as it provided an opportunity to present the data collected in the preceding survey and interviews and draw inferences from the responses of the regulator. This interview was particularly valuable as it gave us access to the sole supervisory authority for the Irish ePrivacy Regulations and instigator of the aforementioned cookie sweep in 2019. The researcher contends that any awareness study of the ePrivacy directive in Ireland would be incomplete without input from the Regulator and this interview provided the final, but the most vital layer of data collection.

3.5 Data Analysis.

Data analysis is referred to as bringing order, structure, and meaning to the evidence collected (De Vos, et al., 2002). The process of data analysis involved data interpretation, reduction, and further analysis. Data analysis in this study is divided into two processes, namely online survey, and interview analysis both of which were analysed using Microsoft Excel (See Tables 3 and 4). The following diagram set out in Figure (3) below as developed by (Othman et al., 2020) sets out the conceptual framework elements for a sequential explanatory mixed methods design. As evidenced in the framework as set out, data analysis methods for the separate phases are different. Microsoft Excel was used to analyse the survey data for our study; the content analysis for the interviews is the same for both studies.

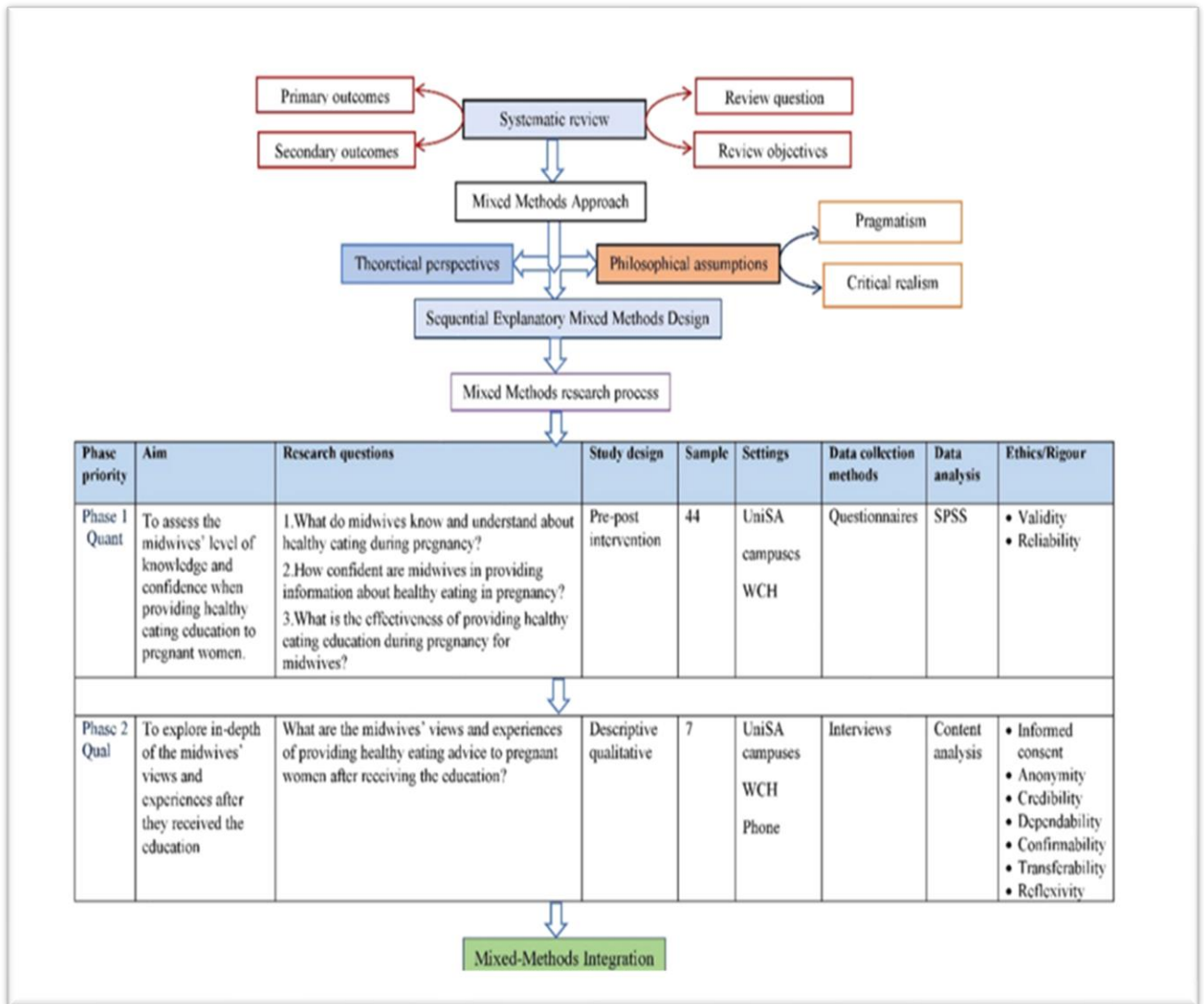


Figure 5 the Conceptual framework for a mixed-methods approach (Othman et. al, 2020)

3.5.1 Survey analysis. Online Survey

Survey data analysis techniques are intended for the examination of measurable features to provide quantitative findings. Such analysis entails the processing of data using organized methods that are quantitative in nature (Toyen, 2021).

The researcher exported the survey data from Microsoft forms to a Microsoft Excel file for further analysis. The aim of the analysis was twofold: firstly, to identify themes and patterns that may be helpful in answering our research questions and to provide a general picture of the research problem which can be further refined, extended, or explained through the qualitative data collection and analysis.

The rationale for this approach is that the survey data and results provide a general picture of the research problem; more analysis, specifically through qualitative data collection is needed to refine, extend, or explain the general picture (Subedi, 2016) . This approach correlates with our explanatory sequential mixed methods approach where the survey data is collected and analysed firstly allowing the results to be further explained in the qualitative phase. As set out in appendix B the survey consisted of 37 questions, 35 of which were closed to allow for easier analysis of the data collected. Closed questions give the respondent a limited number of options to choose from and therefore provide for easier analysis of the data. The 2 open questions which required the respondent to answer in their own words were placed specifically to get some information on a subject to complement the quantitative data polled for the closed questions and were analysed via the analysis tool in Microsoft forms as set out in Figure (6) below with the themes identified and collated as part of our overall content analysis.

37. How can the authorities improve the awareness of laws and regulations governing Cookie use and Online privacy?

77 Responses

ID ↑	Name	Responses
1	anonymous	by having a user/community driven GDPR/privacy rating out of 5 per site, service or app.
2	anonymous	Legislation, information, implementation
3	anonymous	with clearer language and less Jargon.
4	anonymous	Huge Fines
5	anonymous	Approve cookie use by a graded 5 star system. If it is say 4 star and above I will accept but no less than 4 star. Each person can then accept based on their level which satisfy cookie privacy criteria.
6	anonymous	More awareness campaigns needed of what can happen when you provide your data.
7	anonymous	Advertising campaigns. Also standardizing policies.
8	anonymous	
9	anonymous	By making all sites turn off ALL cookies (This should be the default) and not try and trick users into accepting marketing cookies.

Figure 6: Analytics Tool, Microsoft forms

Whilst Microsoft forms provide real-time data and simple charts to visualize the data I needed to export the data to excel for a more in-depth analysis. One issue with Microsoft forms is that when the data is exported to excel it is presented in the resultant spreadsheet in an unstructured form. The initial spreadsheet exported directly from Microsoft Forms was unmanageably large and complex consisting of 146 rows and over 50 columns. The data was therefore split into multiple worksheets to help organize the workbooks and make it easier to find content. I created a separate table for each of the questions and as evidenced in Table 3 below I further broke down the answers into male and female and different age categories. Once I broke it down into separate tabs it became dramatically more searchable, manipulative, and viewable.

By formatting it in this manner it enabled us to analyse the data to identify themes, calculate statistics and percentages and find meaning in the data that may help in making informed recommendations later in the report. Table 3, below sets out the finalized breakdown of the survey data with the separate tabs' representative of a separate worksheet for each survey question which was then used to analyse the data at a more detailed level for each question.

Table 3. Breakdown of survey responses

Question	Are you aware of the recent EU Privacy and Electronic Communication (e-privacy) directive otherwise known as the EU Cookie Law?			Totals
Options	Not aware	Somewhat aware	Very aware	
Female				
18-24	12	4		16
25-34	11	5	2	18
35-44	4	6	3	13
45-54	9	9	3	21
55-64	1			1
Female Total	37		8	69
Male				
18-24	1	2		3
25-34	12	5	1	18
35-44	5	6	3	14
45-54	11	8	3	22
55-64	4	7	2	13
65+	3	1		4
Male Total	36		9	74
Grand Total	73		17	143

3.5.2 Qualitative analysis.

Qualitative methods demonstrate a different approach to scholarly inquiry than methods of quantitative research. (Creswell 2014). I developed the qualitative study by collecting data via in-depth interviews with a purposeful segment and subsequently transcribing those interviews. Because of the vast amount of data collected in the interviews we found I needed to focus on important parts of the data and aggregate it into a small number of themes. Creswell (2014) advised breaking it down into between five and seven themes. Again, I used Excel to code and track themes from the data collected. Because of the work in the research design phase there is duplication of questions in both strands which made it easier for coding and comparison purposes, but the real difference was the qualitative data provided reasons or explanations for the phenomena explored. The object of this research phase was to review all the data, make sense of it, and organize it into categories or themes that cut across all the data sources. The key idea behind qualitative research is to learn about the problem or issue from participants and to address the research to obtain that information.

Fig. 7, below shows the initial coding technique used to analyse the collected data. All the interviews were transcribed from recordings and interview notes. The transcripts were then coded manually with different themes identified in separate colours. The seven main themes from the interviews were entered into an Excel worksheet and were further broken down into multiple worksheets with a separate column for comments in each, see Table 4, below. Again, I found that by breaking it down into separate tabs it became dramatically more searchable, manipulative, and viewable and enabled us to learn from our database. The difference between this and the analysis of our survey database was that there was more work in identifying and coding the themes. In our survey analysis once the data was organized into separate worksheets it was very easy to measure the trends in simple percentages.

3.5.3 Data Integration

According to (Fielding, 2012) data integration is a crucial element in mixed-methods analysis and conceptualization. It combines survey results and qualitative findings, which enables a more in-depth understanding of data. The data from the first two phases were analyzed and integrated to frame the questions for the Regulator. Again, the data was analysed and integrated using Microsoft

excel. Our data had indicated certain trends and I wanted to present these to the Regulator for comment and analysis. The data from the interview with the Regulator was transcribed and coded manually and helped answer many of the questions that arose from the first two phases of data collection and analysis. This transcript also helped in formulating policy suggestions in the conclusions chapter. In hindsight, this research design was very time-consuming for the researcher and possibly involved too many interviews and involved too many questions in the survey. Whilst the work yielded excellent findings the data organization phase was extremely laborious for every phase.

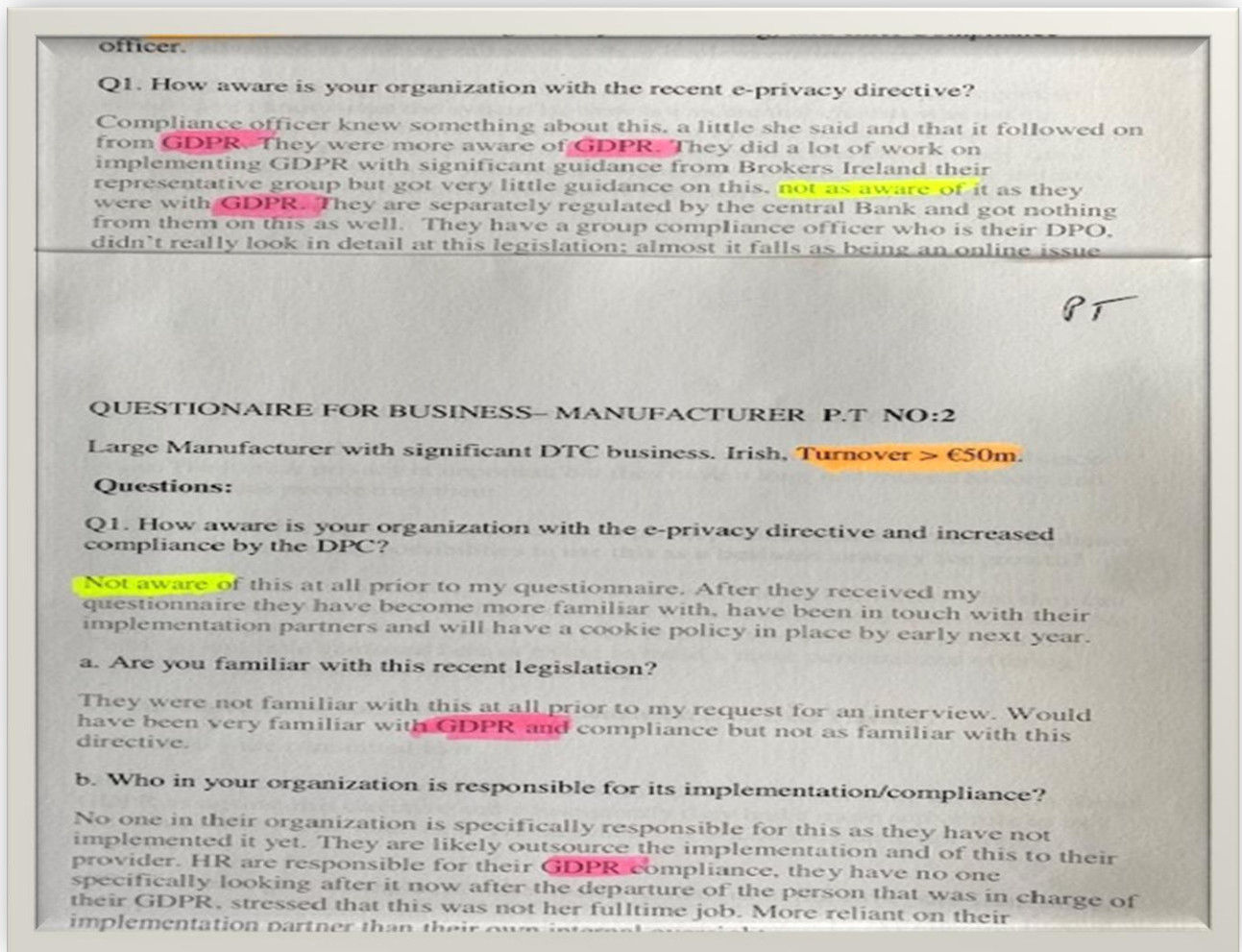


Figure 7 Picture of transcribed interviews.

Table 4: Breakdown on interview responses.

A	B	C	D	E
Interview	Are you aware of ePrivacy directive			Comment
	Not aware	Somewhat aware	Very aware	
Interview No.1		1		Not overly familiar, website hosting outsourced, heard about changes from their Hosting company, heard nothing on public forum or from Regulator.
Interview No.2	1			Not aware, knew very little about this, more aware of GDPR. Had to research about how they are using cookies. Have DPO but thought this was more for Online.
Interview No.3	1			Not aware, researched it after they received questionnaire, not compliant but have been in touch with their hosting provider and will be compliant in a year.
Interview No.4		1		Somewhat aware, know it followed on from GDPR. Has a lot of guidance on GDPR but very little on this, have DPO but she saw this as more of an issue for Online.
Interview No.5			1	Very aware of this, Analytics a big part of their business, they have awareness but their customer's have very little awareness.
Interview No.6		1		Not aware as they should be, No direction from senior management, some knowlegde from their provider.
Interview No.7			1	Very aware now because organisation part of DPC cookie sweep, also Digital agency informed them, CMP in place
Total	2	3	2	
Interview Code				
<p>Interview No.1: One Small Omni Channel retailer, turnover €2m.</p> <p>Interview No.2: One large manufacturer with a turnover >€300m.</p> <p>Interview No.3: One large Manufacturer with a significant DTC business, turnover > €50m.</p> <p>Interview No.4: One Financial/Insurance Turnover >€15m.</p> <p>Interview No.5: One Digital Agency, Google approved partner.</p> <p>Interview No.6: One Online only player with significant recent investment rounds.</p> <p>Interview No.7: One large national retailer, turnover > €100m.</p>				

3.5.4 Ethics

The Ethics approval form was prepared and submitted via the GMIT Taught Programme Research Ethics Approval Application Form in February 2021 and after some feedback and resubmission, approval was granted in April 2021. Please see appendix A for copy of approved application form. We have set out the ethical considerations below in line with the different phases of our research design.

3.5.4.1 Ethics Online survey data.

Consumers for this survey were chosen from a wide range of social contacts, colleagues, and other contacts all of whom are users of online content. Some of these cohorts as known consumers of online content had previously indicated their willingness to participate in research projects for the researcher and had been used for newsletter circulation and testing scenarios as part of the exercises for the post-graduate certificate in 2020. All participants were voluntary, were asked for consent prior to the commencement of research and all were over 18 years of age and were an even mix across the genders. We warranted to all participants that their responses and data would be treated with full confidentiality that all information was completely anonymous, and that information would be stored online in a secure password-protected space. The participants could withdraw from the study at any point before the final submission of the questionnaire and their responses would be automatically deleted. Once they submitted the questionnaire, they were no longer able to withdraw as their response

3.5.4.2 Ethics Interview survey data.

In the case of the business suite, I contacted potential interviewees via their Marketing Departments directly in some instances or indirectly via some key executives in the business that the researcher would know in a professional capacity. The research was carried out by means of in-depth interviews. All participants were required to sign a consent form prior to the commencement of the research and were provided with a copy of the questions prior to the interview. This list was intended as a guide to the questions asked and all participants were encouraged to expand their answers and talk about other areas of interest. As all the interviews were conducted during a time of pandemic restrictions all interviews were carried out via Microsoft Teams and participants were asked for permission to record the interview at the outset.

Permission was sought to use any of the information gathered for the purposes of a dissertation and possible presentation at a Digital West Event or similar and the individuals and organisations will be anonymised to protect their identities. Confidentiality and anonymity were warranted and there was no reward for participation. It was explained to all participants from the outset that they could withdraw from the project at any time by contacting me prior to publication and they were given details of the project timeline to enable them to do so if they wished. The process of trying to set up an interview with the DPC was more time-consuming and took a consistent email exchange to finally get approval for the interview. The representative from the DPC was a special investigator in the enforcement section and was the instigator of the cookie sweep in 2019 and involved in the publication of the guidance in 2020. There was a separate set of questions sent on to the Regulator prior to the interview comprised of findings from our previous research and questions that emanated from this data that I felt needed further explanation.

3.6 Limitations

The sample size is a small representation of the general population. Whilst every effort was made to avoid bias in the survey all participants are over 18 thereby excluding a proportion of the population who are active consumers of online content. The biggest limitation of the research was time constraints which limited the number of participants from the business cohort and prevented the researcher from researching more feedback on the regulatory side aside from the office of the Regulator. Finally, the perception of participants may change over time as the DPC increases its enforcement of the directive and our study is limited to a point in time several months after the updated guidance from the DPC. The age profile is a little more weighted towards the 45-50 cohorts and lack some representation in the 18-24 age group of which we have only 19 respondents.

Chapter 4 Findings/Discussion.

4.1 Research Question

Prior to stating our findings, it may be helpful to restate the questions I wanted answered prior to detailing our findings. The researcher wished to inquire on the level of awareness of the directive amongst the public at large one year after updated guidance from the DPC? I sought to measure this by surveying the level of awareness amongst consumers, the business community, and the regulator. I also sought to determine if there was a relationship between the level of awareness of and compliance with the directive and if increasing the level of awareness of legislation influence public policy in a positive way? The findings as set out below for the three cohorts surveyed have in the researcher's view met the research objectives in that I have established the level of awareness of the directive amongst the three sectors and identified reasons why this may not be at the required level. I have set out the key research findings for each sector in summary form below and have then discussed each of the findings in more detail in the body of the chapter. I identified five main findings from our research in each sector as set out in summary in Figs, 6, 7 and 8 below.

4.2 Survey Strand – Consumer Survey Results

As detailed in the methodology chapter the questionnaire was sent to 61 contacts all of whom were invited if they so wished, to pass it on to their peers and other contacts. In total 144 people responded to the survey, only 1 did not complete. The survey took an average time of 9 minutes and 40 seconds to complete. Fig. 6 below sets out the key finding from the consumer survey.

RESEARCH FINDINGS - CONSUMER SURVEY

1. There is a low level of **awareness** of the Directive amongst consumers.
2. People are concerned about **data privacy** but are not as diligent in protecting it.
3. Consumers do not **trust** organisations with their data.
4. Many organisations are perceived to be **nudging** people to consent to cookies.
5. The majority of respondents felt that Internet providers should have **primary responsibility** to protect their data.

Figure 8 : Key findings consumer survey

4.2.1 Level of awareness of Directive amongst consumers.

In our survey it was noteworthy that slightly over half the respondents at 51%, were not aware of the ePrivacy directive, 37% somewhat aware and only 12% were fully aware of the regulations. This contrasts sharply with the awareness of the GDPR where only 13% of those surveyed have no awareness of these regulations. This is despite almost 70% of those surveyed noticing an increase in cookie banners when accessing online content. The highest level of awareness was amongst the male and female cohort between ages 35-44. Sixty eight percent of the respondents between 18-25 stated that they had no awareness of the directive. Interestingly these are also the respondents who spend most time online from our survey participants with 63% of this cohort spending more than three hours daily online. Eighty eight percent of the respondents know what the purpose of cookies are but despite this, the majority (51%) think that cookie acceptance or banners only minimally improve their privacy with 42% of the respondents classifying them as very annoying. I would posit, based on this research that user's consciousness of their online privacy and subsequent knowledge of the ePrivacy directive and how it seeks to protect them is too low.

In contrast the DPC implemented a very detailed awareness campaign around GDPR in 2018, establishing a dedicated website, www.GDPRandyou.ie and conducting an extensive media campaign in their efforts to help people prepare for GDPR.

4.2.2 Data Privacy

Most of our respondents believe that online players know too much about them and that organizations are not able to effectively protect their data. Ninety percent of those surveyed believe that online players know too much about them with just under half saying it not possible for their online data to be effectively protected. Our results match a 2019 SmarterHQ survey which found that 86% of those polled were concerned about their data privacy with 79% of consumers believing companies know too much about them. (Smarter HQ, 2020).

Still however, a large share of those surveyed (59%) stated that they are not concerned about their privacy when buying online and interestingly 64% of those surveyed were willing to decide to automatically consent to cookies if refusing them meant a more difficult or lesser experience online.

Indeed 55% of respondents do not pay any more attention to cookie policies from companies they are not familiar with.

Despite their express worry about various aspects of their digital privacy, many of those surveyed are not as diligent as they state they are when online. Almost a third of those surveyed who feel that they were unable to protect their privacy felt that if they wanted to avail of the service, they must accept how their data is being used.

This data very much evidences the Privacy Paradox as referred to in the literature review. The Privacy paradox argues that there is effectively a gap between privacy attitudes and social behaviour and that whilst individuals might be concerned about their privacy it does not prevent them sharing their information online without protecting their online behaviour possibly with the purpose of achieving greater benefits from the online transaction.

Half of the respondents said they would consider changing their search engine to a provider that prioritizes searchers privacy yet only 6% had changed their browser in light of privacy concerns. Google unsurprisingly was the most popular search engine amongst our respondents with 85% preferring Google as their search engine of choice followed by Safari at 14%. Interestingly search engines like DuckDuckGo and Brave that prioritize user's privacy did not feature at all amongst our respondents with only Google, Safari and Yahoo making the list out of a choice of 10 providers and an option for the respondent to enter any other search engine they use to get online. This Data correlates with recent statistics from StatCounter which places Google's market share in Ireland at 95% (Statcounter, 2022).

Finally considering the Covid pandemic 24% of respondents were much more willing to share data more than they would normally if this helped in providing information to public health with almost half at 47% somewhat more willing to share data but the majority (45%) unwilling however to support any privacy laws being suspended as a tool to help deal with the pandemic.

Despite the ongoing pandemic, most consumers want little or no reduction in privacy protections, while still supporting public health and safety efforts



Figure 9: Consumers' trust concerns and their reluctance to change providers to protect their privacy.

Based on our research questionnaire I would posit that although people are concerned about data privacy they are not as diligent as they should be in protecting it.

4.2.3 Trust

Only 10% of those surveyed trust organizations to protect their online data.

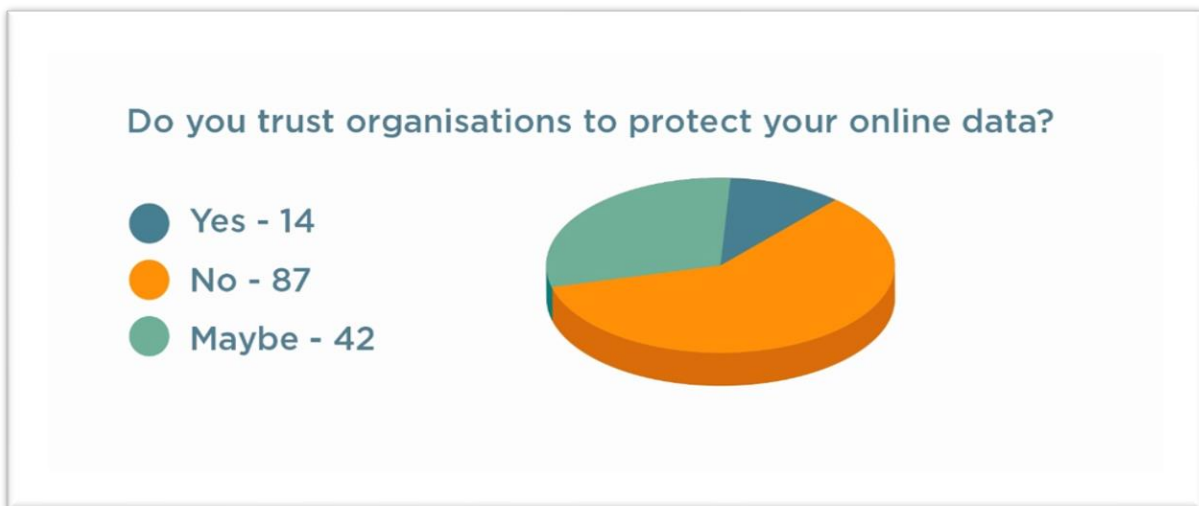


Figure 10: Respondents trust in organisations to protect their data.

A significant 61% of respondents do not trust that their online data is being protected yet continue to share information as evidenced above despite the trust deficit. These percentages are evenly spread out over gender and age groups signaling broad concerns about data collection by various entities. The survey also finds that 65% are more likely to trust organizations that are fully transparent about how they use their data. Building trust should be key component of the customer dynamic, two thirds of those surveyed are more likely to consent to being tracked if there is some consideration for the transaction such as discounts or special offers. Customers expect providers to keep their data protected and secure, this is a fundamental requirement of trust in the digital world. Beyond that, customers want to be informed about how their data is collected, used, and managed, and ultimately, customers want control of their data. This desire for visibility and control goes across any data relationship. Increasingly, consumers will make decisions about their providers with privacy and transparency in mind.

In today's digital economy, an objective benchmark for assessing trust is vital. As seen above it requires full transparency. If sensitive information gets into the wrong hands, consequences can include privacy breaches, loss of intellectual property, interruptions to operations and revenue and reputational damage.

4.2.4 Patterns nudging people to consent to cookies.

Considering the increased prevalence of Cookie banners and CMPs on websites our respondents have found that Cookie policies are difficult to read and are purposely complicated to ensure they are accepted. 78% of our survey population feels that organizations are continually nudging consumers towards consent. A bigger majority (84%) feel that cookie policies are purposely difficult to navigate so as to entice users towards accepting the cookies and continuing their online journey and 77% feel that cookie policies are couched in legalistic language making it difficult to understand.

This data very much evidences the prevalence of dark patterns as referred to in the literature review.

Dark patterns refer to illegal configuration of cookie banners or CMP's, with vendors of CMPs turning a blind eye to — or worse, incentivizing — clearly illegal configurations of their systems. Enforcement in this area seems to be lacking and our consumer survey would indicate that they do not trust cookie polices to be configured for the mutual benefit of the customer and business.

There is no standardized CMP and even customers using the same CMP can configure it differently to promote acceptance.

4.2.5 The majority of respondents felt that Internet providers should have primary responsibility to protect their data.

The second last question on our survey asked who should have primary responsibility for protecting data privacy. Interestingly most of the respondents felt that the Internet service providers should bear primary responsibility for protecting their data privacy followed closely by the Government at 29%, individuals at 21% and social media providers at 18%. Given that it has fallen to the European Union and subsequently governmental organisations such as the Data Protection Commission (DPC) in Ireland to implement guidelines by which users must actively consent before cookies can be set up and the reluctance or out respondent s to trust organizations to protect their data it is unusual that the majority felt that it should fall to the service providers to protect their privacy.

I would posit that it is the activities of these organizations that has prompted a lot of the current regulation and would refer to Zuboff as quoted in the literature review where she proffered the theory of mass surveillance and commercialisation of data by Google and the main social media sites that will result in a new form of capitalism ruled by the invisible hand of the keeper of the data.

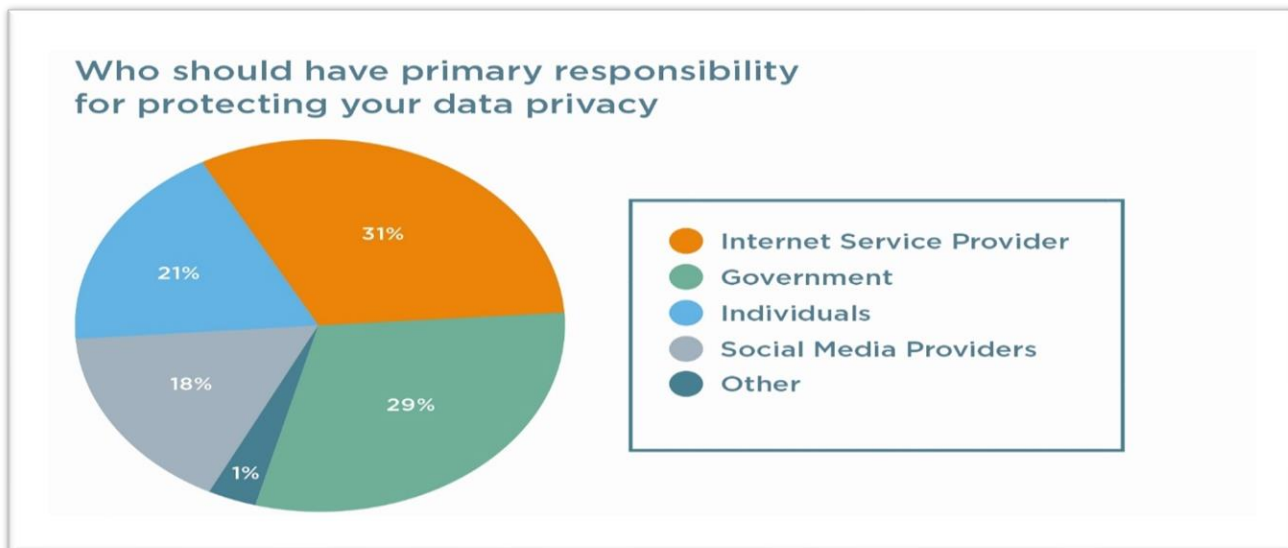


Figure 11: Respondents' responses as to who should protect their data.

4.3 Qualitative Strand – Business Interview Results

In total I interviewed 8 organisations as a representative group of the business sector. I tried as much as I good to replicate the sectors as examined as part of the DPC Cookie sweep in 2019. Time constraints however limited us to interviews with 8 businesses across diverse sectors and with multiple turnover thresholds. Semi structured interviews were conducted with seven business segments over October and November 2021 as identified in Table 2 above. All the interviews were at CEO/CTO level with two of the respondents bringing their DPO/Compliance officers on the interviews. All entities have sight of the questions before the interview and in line with the ethics form; all signed and returned consent forms before the interviews.

RESEARCH FINDINGS – BUSINESS

1. There is a low level of **awareness** of the Directive amongst the Business framework.
2. Companies care about **data privacy** but are more concerned about GDPR than the directive.
3. Most businesses see it as a mere **compliance** issue and nothing more, compliance amongst our respondents was patchy.
4. The majority of their customers are just **accepting** their cookie policies without reading it.
5. All businesses thought that there should be more **media campaigns** to increase awareness.

Figure 12: Key findings business sector

4.3.1 Level of awareness of Directive amongst businesses.

In our survey 29% of respondents were not aware of the ePrivacy directive, 42% somewhat aware and only 29% were fully aware of the regulations. Of the 29% or the two respondents who were very aware of the regulations, one entity was part of the DPC Cookie sweep in 2019 and the other is a digital agency who stated that it was critical to them to educate themselves on developments in this area as they were worried that reduced viability on analytics would have a detrimental impact on their business. Interestingly whilst they have obvious awareness of the directive, they stated that the level of awareness of their customers was low and advised all their 112 clients as to the importance of the legislation and the requirements to comply. Most of those interviewed excluding those that had knowledge for very specific reasons, were either not aware or only somewhat aware of the directive. Two of those interviewed only became aware of the directive through their hosting providers. One business with a significant online business had no awareness of the directive until they received the pre-interview questionnaire and subsequently contacted their provider to put a CMP in place.

All respondents stated that they were very aware of GDPR and allocated a lot of time and resource to ensure they were compliant. There is a very stark difference between the overall awareness of GDPR and the ePrivacy directive amongst our interviewees.

Most of the interviewees learned about the directive from either their hosting providers or digital agencies and most were shocked to hear that their organisation could record a criminal conviction for noncompliance. Most cited lack of awareness campaigns as the reason for their limited knowledge and suggested media campaigns, targeted information events and two suggested putting the onus on the Online providers. Four of the organizations interviewed have DPO's in place but their DPO's felt that this specific issue was an issue for online and should have been dealt with by the online department.

This was best summed up in a quote from the manager of the digital agency who felt that awareness and implementation of this directive falls within the horrible middle ground between regulatory/legal and marketing/online.



Figure 13: Quote from Manager, large digital agency

4.3.2 Companies care about data privacy but are more concerned about GDPR than the directive.

Our results show that all the organizations surveyed have stated they care about data privacy with all indicating that they have made significant investment in their GDPR compliance capabilities and are continuing to invest to embed privacy practices into their business processes. All the respondents feel that they are compliant with the GDPR which they see as their main privacy requirement.

One interviewee likened GDPR as akin to Brexit in that he would never get to the end of it. Conversely only 2 of the respondents gave the same level of attention to the ePrivacy directive with all seeing it as a compliance burden rather than something that will help them nurture customer's privacy.

Only one of the interviewees saw the legislation and the whole privacy discussion as a business strategy for growth, with this respondent stating that the directive will help in increasing trust in how they use customers data, He saw this as a vital component for future growth online particularly if there is a value exchange for using people's data. He felt that transparency in how they use people's data was key, and that by building this trust they will build a loyal customer who will consent to being tracked rather than spending resources on acquiring new customers via Google ads or similar.

As I have noted from our consumer survey, I would recommend that building trust should be a key component of the customer dynamic, two thirds of the consumers surveyed are more likely to consent to being tracked if there is some consideration for the transaction such as discounts or special offers, yet the majority of the business cohort see it mainly as a compliance issue.

4.3.3 Most businesses see it as a mere compliance issue and nothing more, compliance amongst our respondents was patchy.

Our results show that only three of the 7 respondents are fully compliant with the ePrivacy directive. Again, of the organisations that feel they are fully compliant, one was part of the cookie sweep, one is a digital marketing company that is promoting compliance and one thinks they are compliant but is reliant on his hosting provider for confirmation. One respondent was not in compliance because he was not aware of the directive, another online start up stated that they were growing so quick they were hoping to fully catch up on compliance after whilst the other two had noticed prior to the interview that there were significant aspects of their CMP's that were not compliant. Interestingly whilst the digital agency has stated that they are compliant with the directive, they stated that only 60 or 53% of their 112 clients are complying. The main reason for the lack of compliance was the low evidence of enforcement of the directive and they also said their client's focus during the pandemic was on survival and not compliance.

This figure of 53% noncompliance correlates with our survey where 43% of the respondents are not in compliance. Interestingly most respondents are relying on their hosting providers to ensure compliance.

Our survey indicates that the majority of our interviewees that some organisations still see this as more of a compliance burden than a way to change how they handle personal data more broadly.



Figure 14: Level of compliance with directive per our survey

4.3.4 The majority of consumers are just accepting their cookie policies without reading it.

Based on data gathered from our interviews on average, only 8% of consumers actively managed cookies when visiting the respondent's websites. This is lower than in our consumer survey where 23% of the respondents claimed to read cookie policies before accepting them. The reason for the difference may be down to timing, as the digital agency interviewee stated that the figure for managing cookies was initially 40% but has subsequently settled at around 10%. From our business survey, 92% of the respondent's consumers just accept cookies with the sole purpose of getting online as quickly as they can. As stated in the literature review, people can sometimes get tired of security procedures and processes, especially if they perceive security as an obstacle, preventing them from their primary task. These feelings describe the so called 'cookie fatigue', and they can be detrimental to the continued awareness and compliance with the directive. This correlates with the EU body Regulatory Fitness and Performance (REFIT), which oversees verifying effectiveness of directives, states in relation to the ePrivacy directive the current rules end being counter-productive as "the constant stream of cookie pop-up-boxes that users are faced with completely eclipses the general goal of privacy protection as the result is that users blindly accept cookies" (Refit 2016).

4.3.5 All businesses thought that there should be more media campaigns to increase awareness.

All respondents felt that needed to be increased awareness campaigns around the directive.

Most cited lack of awareness campaigns as the reason for their limited knowledge and suggested media campaigns, targeted information events and two suggested putting the onus on the Online

4.4 Triangulation

Convergent results

When triangulating data sources, data converged around similar themes expressed by consumers and the business cohort. Both groups shared the perception that awareness of the directive was low and that more media and educational campaigns were needed to increase knowledge. We also found shared views on greater awareness of GDPR than the directive, low compliance rates and the majority of users not heeding cookie policies.

4.4.1 Complementary results

It was relevant for the consumer and business cohort that awareness was low and both groups shared similar perceptions as to how improve this. Both groups had higher awareness of GDPR than the directive and both referenced that people even though they are concerned for their privacy is still quick to share information with businesses.

4.4.2 Divergent results

I found divergent views of consumers and businesses concerning privacy, trust, and perceived behaviour around cookie policies. While most businesses state they are very concerned about people's data the consumer group doesn't feel they can be trusted to keep their data safe online. Furthermore, whilst most of the business cohort says they intend to comply with the directive most consumers say that they are not really adhering to compliance standards most of the time and that business was continuously trying to nudge consumers towards cookie acceptance by making policies difficult to navigate or couching them in legalistic language.

4.5 Regulator

In line with our sequential mixed method design as set out in our methodology chapter, the researcher purposefully left the interview with the regulator until all the data was collected and triangulated from the business and consumer sectors. The questionnaire for the regulator (see appendix D), was designed slightly differently to both the business and consumer segment in that it was populated with summary findings from the other sectors and prompted the regulator to comment on the findings. Cognizance was also taken in the design of the questionnaire of the

advice imparted by a specialist data lawyer as part of the pilot survey. The interview with this respondent helped in setting out the legal basis of the directive, why it might not be as effective as it should be and why the level of awareness of the directive is so low particularly since it has been around since 2002. The representative from the DPC was a special investigator in the enforcement section and was the instigator of the cookie sweep in 2019 and involved in the publication of the guidance in 2020.

RESEARCH FINDINGS — REGULATOR

1. They accept there is a low level of **awareness** of the Directive amongst the Business framework.
2. They had legal powers and budget to **promote awareness** of GDPR, none under the ePrivacy regulations.
3. Their **enforcement** powers are hindered by the way the legislation is framed.
4. They are concerned about the increasing prevalence of **dark patterns** pertaining to the implementation of CRM's.
5. Powers of enforcement and awareness will increase once this legislation is replaced by the **ePrivacy regulation** coming into force within the next three years

Figure 16: Key findings Regulator

4.5.1 Reasons for low level of awareness around ePrivacy directive.

In response to the question as to why there was such a low level of compliance with the directive the respondent pointed out firstly that the cookie law had existed since 2002 and was amended in 2009. There were guidelines set out in 2002 but these were never updated, and their focus was more on unsolicited direct marketing. The ePrivacy directive transposed in Ireland as the ePrivacy regulations 2011 also gave the DPC the power to prosecute unsolicited direct marketing. She said there was a deficit in the way the regulations were written in that they had more powers of enforcement around direct marketing rather than cookies. The interviewee also indicated that there was a lack of technical expertise in the DPC office, and it is only in recent years with the evolution of AdTech and CMP's that they have got the staff to start enforcing this directive.

She accepted that there was a low level of awareness generally around the whole ePrivacy element and gave several reasons for this.

Firstly, the ePrivacy law is a privacy law as opposed to a data protection law and the DPC don't have the same powers of enforcement as they do with GDPR.

Secondly because the regulations also cover unsolicited direct marketing their enforcement powers are jointly held with COMREG which she stated is far from ideal.

There is a deficit in how the legislation is drafted in that they cannot directly investigate a complaint. This is because they would have to prove that a cookie was stored on a particular device on a given day which would prove almost impossible. Instead, all their investigations must be of their own volition so they can satisfy themselves that there was a breach. Since the cookie sweep, they have written to several hundred organizations. They have no budget to promote awareness of the directive in contrast to the GDPR where they spent €200k on an awareness campaign in 2018. Also, the DPC had a role under the GDPR to promote awareness of the regulations, this does not exist in the ePrivacy regulations which she stated is really the poor relation, interestingly they feel that a public awareness campaign could be counterproductive as they may get a huge number of complaints which they don't have the resources to investigate and they cannot enforce a breach without going to court for noncompliance with an enforcement notice. The court then decides on the level of fines.

“

The ePrivacy directive is really the poor relation in comparison to GDPR

”

Figure 17: Quote from Regulator with reference to the ePrivacy Directive.

They get considerably more complaints annually about unsolicited direct marketing than they do around cookies. Most of the implementation of Cookie banners was done by third party providers and is seen as technical issue for the website to work, people never really “ got into the weeds of it” as opposed to GDPR where most organizations spend huge resources on complying. She stated that it was such an arcane piece of legislation that it was difficult to promote awareness of it, that it bored people and it was a challenge to promote awareness of it. Because of the complexities in successfully enforcing the directive they have adopted an approach where they try and nudge people to comply but are ready to enforce if they meet resistance.

They are very aware of “dark patterns ” in relation to the design of CRM’s and have seen huge inconsistency in how they are configured. Some organizations classify analytic cookies and chat bots as strictly necessary which they are not under the legislation. She indicated that if they would probably revise their guidelines in relation to this based on information coming from The European Data Protection Board, but this was one area she saw as an area they needed to concentrate their resources on. They await the new regulation which will have a two-tier regime of fines like GDPR and will give the DPC direct powers to impose these and will have extraterritorial effect. It is hard for them to keep up with technological advances particularly in relation to big service providers but couldn’t go into more detail on this. They are aware of and are monitoring Google’s privacy sandbox and Apples IOS.3. Both are attempts by these providers to bar companies from gathering users’ browsing interests through cookies (Agarwal, 2021).

4.6 Discussion

In our study, the researcher aimed to improve understanding of the individual and organisational factors relating to awareness of and compliance with the ePrivacy directive by consumers and businesses, with the focus on awareness, compliance, and enforcement by applying a mixed-methods approach.

I collected survey data on consumers' awareness, knowledge, behaviour, and compliance regarding the legislation as well as interview data on businesses' perspectives of similar factors. Applying a sequential triangulation approach, I integrated the main results from the consumer survey with business interviews.

Those data described their multiple perspectives concerning relevant awareness, behaviour and compliance and were analysed to identify and clarify parallels and discrepancies in the views expressed by both parties.

When triangulating data sources, data converged around similar themes expressed by consumers and the business cohort. Both groups shared the perception that awareness of the directive was low and that more media and educational campaigns were needed to increase knowledge. I also found shared views on greater awareness of GDPR than the directive, low compliance rates and the majority of users not heeding cookie policies. In line with our sequential mixed method design as set out in our methodology chapter, the researcher used the data was collected and triangulated from the business and consumer sectors and used this in our interview with the Regulator to inquire as to why there was such a low level of awareness.

The Regulator gave varying explanations for the low level of awareness and compliance ranging from the way the legislation is drafted, limited, and shared powers of enforcement, deliberate noncompliance and largely missing the same enforcement powers as GDPR. This will change when the ePrivacy Regulation is adopted but given their inability to keep up with technological advances it may already be too late given that the big data providers may already have blocked cookies on their browsers and replaced them with their own infrastructure which may be another regulatory challenge. Table 5 below sets out a comparison of the themes from our literature reviews with the main themes from our research.

This table shows similar findings to what was unearthed in the literature review. The main area of divergence was around the different views of trust and privacy between business and consumers.

Whilst the research yielded very credible original findings the amount of work involved in this study proved extremely time consuming as it involved several different research methods and involved multiple phases of data analysis and triangulation consistent with our chosen research approach. Increased time demands were required to effectively implement the survey and qualitative parts of the study and required the researcher to develop a broader set of skills across both approaches to analyse and triangulate the data in a sequential manner. Fig 18 below gives an indication of the different phases required in this research approach.



Figure 18: Different phases involved in an ESMMR approach.

Table 5: Comparison of main themes from literature review to themes from findings.

Authors	Origin	Purpose	Type of Source	Major Themes from Literature	Convergent themes from Findings
DPC (DPC,2020).	Ireland	Examination of the use of cookies and similar technologies across a range of sectors.	Report	Bad Practices were widespread, controllers were not in compliance with directive, increase in enforcement coming.	43% of our business respondents not compliant with directive. Digital Marketing agency indicated that only 53% of their clients were compliant. This is over 1year after the end of the grace period offered by the DPC within which to comply. Non compliance still a major issue.
Zuboff (Zuboff, 2015).	USA	An examination of the nature and consequences of computer mediated transactions.	Journal	A theory of mass surveillance and commercialisation of data by Google and the main social media sites that will result in a new form of capitalism ruled by the keeper of the data.	90% of our consumer respondent's believe that online players know too much about them and only 10% of them trust organisations to protect their online data.
Martin (Martin, 2020)	UK	To examine the conceptualisation of privacy post disclosure assumed in the privacy paradox.	Journal	Privacy paradox, the tension between consumers stated privacy preferences as measured in surveys and their actual behaviour.	Despite their express worry about various aspects of their digital privacy, many of those surveyed are not as diligent as they state they are when online. Half of the respondents said they would consider changing their search engine to a provider that prioritizes searchers privacy yet only 6% had actually changed their browser in light of privacy concerns. This data very much evidences the Privacy paradox as where there is a gap between consumers stated regard for privacy and their actual behaviour online.
Refit (Refit, 2016)	Europe	Regulatory overview of fitness and performance of directives.	Report	Talks about cookie fatigue demonstrating the challenges that both organisations and consumers face given the apparent apathy or reluctance to understand more about cookies.	From our business survey, 92% of the respondent's consumers just accept cookies with the sole purpose of getting online as quickly as they can. People are getting tired of security procedures and processes, especially if they perceive security as an obstacle, preventing them from their primary task. These feelings are evidence of 'cookie fatigue' to understand more about cookies'
Forbrukerradet (Forbrukerradt, 2018)	Norway	To sample settings in Facebook, Google and Windows 10 to show how default settings and dark patterns, techniques and features of interface design are meant to manipulate users or nudge them to privacy intrusive options.	Report	Combination of privacy intrusive defaults and the use of dark patterns, nudge users to the least privacy friendly options.	78% of our survey population feels that organizations are continually nudging consumers towards consent. A bigger majority (84%) feel that cookie policies are purposely difficult to navigate so as to entice users to accept and 77% feel that cookie policies are couched in legalistic language making them difficult to understand. Evidence of dark patterns.
Bada et Al (Bada et.al, 2015)	UK	To identify key factors regarding cyber security awareness campaigns which may lead them to fail to appropriately change peoples behaviour.	Report	Essential components of awareness campaigns as well as the factors which can lead to a campaign success or failure. Among the factors identified include communication, awareness and training.	Implementing the directive without accompanying awareness campaigns has in the researchers' view limited the effectiveness of the legislation. Raising awareness is essential for ensuring compliance with legislation

Chapter 5: Conclusion and Recommendations

5.1 Introduction.

In this paper I ran a large-scale measurement campaign on the awareness and effectiveness on a regulatory, business and consumer level of the ePrivacy directive one year after updated guidance from the DPC and testify that despite the best efforts of the Regulator awareness of and compliance with the directive remains low. In this chapter the researcher will present in summary form our methodology and findings and recommend several policy changes that may improve awareness and enforce compliance of this privacy legislation. I will also address continuous technological changes and make an argument against the stringent rules requiring consent to analyse cookies particularly where the data collected is being anonymised. I would posit that this thesis has met the objectives of the study in establishing the level of awareness of the directive and exploring reasons as to why the level of awareness is so low. In addition, I found a high rate of noncompliance linked to low levels of awareness and suggested a number of initiatives to address the issues emergent from the research.

5.2 Research purpose and Methodology.

Our aim in this dissertation was to measure the awareness and effectiveness on a regulatory, business and consumer level of the updated E.U. privacy and Electronic Communication(ePrivacy) directive (S.I.No. 336/211) one year after updated guidance from the DPC.

Our review of literature indicated that both awareness of and compliance with the directive is low and I chose a mixed methods approach, collecting data on consumer's awareness of the directive as well as interview data with the business and regulatory cohort to explore multiple perspectives in relation to our research questions.

As part of a comprehensive data collection exercise, I gauged the level of awareness and effectiveness of the Directive across three different sub-sets

- Consumers of Online Content.
- The Business framework more specifically at an executive level.
- The Regulatory framework more specifically the Data Protection Commission

In terms of the order of the interviews I sought to measure the awareness of the directive amongst the consumer and business cohort firstly and then presented these results to the Regulator for comment and further insights from their perspective as part of our sequential mixed methods approach to the research questions. Through our research for our literature review, our pilot study and interaction with my supervisor I attempted to devise the most appropriate method of data collection for this specific research study.

An explanatory sequential mixed method design was considered the best approach to analyze the awareness and effectiveness of the implementation of the E-privacy directive (2019) across the three different stakeholder groups as outlined.

In the first, survey phase of the study, survey data was collected from 144 people to gauge their awareness. The second, qualitative phase was conducted as a follow up to the quantitative results to help explain the survey results. In this exploratory follow-up, I explored the level of awareness amongst the business cohort and controllers of websites and further probed why there was such a low-level awareness amongst their customers and why there is such a low rate of compliance. These results were then aggregated and brought to the Regulator for further analysis and explanation.

Data wrangling referred to as the process of cleaning and unifying messy and complex data sets for easy access and analysis (Altair, 2022) proved to be a very difficult and time-consuming task and on reflection the researcher probably collected too much data. Whilst the work yielded excellent findings the data organization phase was extremely time consuming for every phase as detailed in Fig.18 above.

5.3 Findings

In our study, I aimed to improve understanding of the individual and organisational factors relating to awareness of and compliance with the ePrivacy directive by consumers and businesses, with the focus on awareness, compliance, and enforcement by applying a mixed-methods approach.

I collected survey data on consumers' awareness, knowledge, behaviour, and compliance regarding the legislation as well as interview data on businesses' perspectives of similar factors.

Applying a concurrent triangulation approach, I integrated the main results from the consumer survey with business interviews. Those data described their multiple perspectives concerning relevant awareness, behaviour and compliance and were analyzed to identify and clarify parallels and discrepancies in the views expressed by both parties.

When triangulating data sources, data converged around similar themes expressed by consumers and the business cohort.

Both groups shared the perception that awareness of the directive was low and that more media and educational campaigns were needed to increase knowledge. We also found shared views on greater awareness of GDPR than the directive, low compliance rates and the majority of users not heeding cookie policies. It was relevant for the consumer and business cohort that awareness was low and both groups shared similar perceptions as to how improve this. Both groups had higher awareness of GDPR than the directive and both referenced that people, even though they are concerned for their privacy are still quick to share information with businesses. I found divergent views of consumers and businesses concerning privacy, trust, and perceived behaviour around cookie policies. While most businesses state they are very concerned about people's data the consumer group doesn't feel they can be trusted to keep their data safe online. Furthermore, whilst most of the business cohort says they intend to comply with the directive most consumers say that they are not really adhering to compliance standards most of the time and that business was continuously trying to nudge consumers towards cookie acceptance by making policies difficult to navigate or couching them in legalistic language. The Regulator gave varying explanations for the low level of awareness and compliance ranging from the way the legislation is drafted, limited, and shared powers of enforcement, deliberate noncompliance and largely missing the same enforcement powers as GDPR. This will change when the ePrivacy regulation is adopted but given their inability to keep up with technological advances it may already be too late given that the big data providers may already have blocked cookies on their browsers and replaced

them with their own infrastructure which may be another regulatory nightmare. Figure 19. Below sets out the main findings from the consumer, business and regulatory cohorts highlighting the common themes.

AGGREGATED RESEARCH FINDINGS CONSUMER, BUSINESS AND REGULATORY

1. There is a low level of **awareness** of the Directive amongst consumers and business and this fact was accepted by the Regulator..
2. People are concerned about **data privacy** but are not as diligent in protecting it.
3. Business say they care about **data privacy** but consumers do not trust organisations with their data. Privacy directive is a privacy rather than a data protection law.
4. Many organisations are perceived to be nudging people to consent to cookies and are not in compliance with the regulations. Regulator notes evidence of **dark patterns** in many CMP's.
5. The majority of respondents felt that Internet providers should have primary **responsibility** to protect their data.
6. Both the consumer and business cohorts agree on increased media, awareness and educational **campaigns** to increase awareness. Regulator had no budget to promote awareness of this directive, also very technical legislation, hard to interest people.
7. Both cohorts had much more awareness of **GDPR** than of the ePrivacy directive. Regulator had both budget and statutory duty to promote awareness of these regulations.

Figure 19: Aggregated research findings

5.4 Recommendations.

Several recommendations have arisen from this research in relation to all three participants of the study.

5.4.1 Awareness.

Raising awareness is essential for ensuring compliance with legislation. (Wynveen and Sutton 2017: Valentine, 2015). We have noticed a direct correlation between low levels of awareness and compliance with the directive. If the regulators are serious about increasing compliance with this directive there should be a proper informative awareness campaign around the directive

regardless of the limitations of the regulations or budget. I would posit that awareness of privacy laws may have several benefits beyond compliance in that it builds consumer confidence and knowledge customers take a more active role in protecting their data. Research in behavioural science as set out by (Dolan et. al, 2010) shows that people who are more aware of and care more deeply about an issue are more likely to change their behaviour and awareness campaigns should accompany all important privacy legislation.

5.4.2 Enforcement

Enforcement of legislation around the directive, which has been in place since 2002, has been limited up until the cookie sweep in 2019. A bigger issue however is the complexity that exists around the Regulator's power to effectively enforce the legislation as detailed in the findings chapter. I am of the view that a significant reason for the low levels of compliance as set out directly relate to low or ineffective enforcement by the regulator. I would suggest a similar regime of enforcement as set out in the GDPR and whilst this may be in the pipeline in the new ePrivacy Regulation, currently this legislation is not fit for purpose and needs considerable amendments to improve effectiveness. I would posit that an awareness campaign combined with consistent enforcement activities like road safety campaigns carried out by the RSA would have significant positive effects on compliance.

5.4.3 Challenges

I would posit that even with increased powers of enforcement that it may be a futile exercise as Regulators are not able keep up with technological advancements and users' awareness of their online privacy is still too low. This is evident in the inability of the regulatory bodies to minimize the "dark patterns" used by providers to nudge users to select privacy-unfriendly options in attempt to push consumers towards choices that benefit the service provider. The DPC's complicated investigation mechanism by virtue of regulations drafted more for direct marketing than cookies make enforcement in this area sorely lacking. The DPC indicated they only tend to audit cases where they have received a complaint and that widespread audits do not currently take place.

The DPC did not indicate they have any automated tools to expedite discovery and enforcement and I would posit without some type of automated audit tool that enables regulators perform

systematic and regular audits, enforcement will always be patchy. I would also suggest that the designers and suppliers of CMP's be pre-approved by the DPC to only allow compliant designs to be used. This may well be legally possible per the Fashion ID case referred to earlier in this document where the CJEU held that Fashion ID and Facebook are joint controllers facing equal requirements regarding the personal data which is processed. It would allow for less latitude in how CMPs are configured which one area of major concern to the Regulator.

Even with improved tools or powers of enforcement consumers may still choose to ignore cookie policies looking on them as merely informational statements rather than privacy enhancing instruments and I feel that the Regulator should continue to propagate the privacy message regardless of user's preferences.

5.4.4 Google's dominance.

I referred earlier in our findings chapter to the fact that Google was the most popular search engine amongst our respondents with 85% preferring Google as their search engine of choice. This Data correlates with recent statistics from StatCounter which places Google's market share in Ireland at 95%. Google promised in early 2021 that they were intending to phase out third party cookies on its chrome browser (Slattery, 2021) . Rather than allowing other companies track an individual's activity, it proposes putting users into groups, or cohorts, based on common interests. The cohort would not be specific enough to allow marketers to personally identify subjects. On the face of it given our research above, this may be a positive development, but I would posit that this is a more dangerous development than the proliferation of tracking cookies in recent years; given their dominant position in the marketplace they are likely to hoard all the precious data for themselves whilst cutting off access to competitors. They will collect data from customer's website and sell it back to them albeit in an anonymised form under the pretence of phasing out their party cookies to enhance privacy. The Competition and Markets authority (CMA) in the UK has been investigating whether Google's intentions are anticompetitive as they may prohibit competition in digital markets. Indeed, Google has agreed not to kill off third party cookies without getting authorization from the UK's Competition and Markets authority (Lapowsky, 2022). Given that Google's European headquarters are based in Dublin I would recommend a multiagency approach to any developments in this area between the DPC and CCPC in Ireland, the constant regulation

and demonization of third-party cookies may well lead to a different regulatory nightmare, people propagating for the demise of cookies need to be careful what they wish for, the alternative might cede control to the dominant players.

Again, I refer to Shoshana Zuboff as quoted in the literature review where she proffered the theory of mass surveillance and commercialisation of data by Google and the main social media sites that will result in a new form of capitalism ruled by the invisible hand of the keeper of the data.

5.4.5 Trust.

Through clearer, transparent and more user centric cookie policies Companies may foster trust with their customers which may result in a more mutually beneficial relationship between the parties. We noted in our research that 67% of users are willing to share more data in exchange for discounts and special offers with the possibility to elevate the whole privacy strategy as a business opportunity rather than a compliance issue. Consumers who trust how their data is being used may well consent to share more data about themselves ensuring that businesses become less reliant on information gathered from third parties, trust is the new currency.

5.5 Future research

There are ample areas of future research arising out of this dissertation. The opportunity to examine and develop standardised CMP's and automated auditing tools to help regulator's perform systematic audits on websites is one area that could be explored further.

There is need for additional research into how much Companies consider privacy concerns in developing their digital marketing practices and conversely how much consumers consider this in their online activity. By becoming more transparent about data collection and use and reassuring the public about the ethical integrity of how they are using their data, Companies can help build the much sought after trusted relationship with their consumers which should be to their mutual benefit into the future. In addition, there is need for additional research into how much marketers consider legal concerns in developing their digital marketing not just concentrating on GDPR but on how they are harvesting data about their customers without their knowledge or at least in the full knowledge that consumers are not heeding Cookie or Privacy Policies or Terms of service. Additionally, there are further studies required on why the ePrivacy directive has not been as

effective as envisaged and whether so much regulation is warranted given that most of the data being collected is anonymised.

5.6 Conclusions

In our study, the researcher aimed to improve understanding of the individual and organisational factors relating to awareness of and compliance with the ePrivacy directive by consumers and businesses, with the focus on awareness, compliance, and enforcement by applying a mixed-methods approach. It was established that there was a shared perception amongst all respondents that awareness of the directive was low and that more media and educational campaigns were needed to increase knowledge. I also found shared views on greater awareness of GDPR than the directive, low compliance rates and the majority of users not heeding cookie policies. I explored reasons for the low level of awareness and compliance ranging from the way the legislation is drafted, limited, and shared powers of enforcement, deliberate noncompliance and largely missing the same enforcement powers as GDPR. I made several recommendations into increasing awareness of and compliance with the directive and suggested a number of policy initiatives that may help improve enforcement and compliance particularly around standardized CMP's and automated auditing tools. Table 6 below sets out in summary our main findings and proposed solutions.

In conclusion this research provided a fascinating insight for the author into the struggle to control the data gold rush. Regulation alone cannot effectively control this area but partnered with traditional legal principals of privacy and competition law and enhanced technologies there is an opportunity to increase compliance for everyone's benefit. It may be in everyone's long term interest to comply, as Microsoft's Brad Smith opines 'Had Microsoft continued its assaults on regulators and the competition, we wouldn't be the most valuable company in the world today. We wouldn't have been given the opportunity. We had to persuade people that we deserved the trust,' (Rathesar/Redmond, 2019).

Or to put it more colloquially as a previous boss of mine put it'' You cannot fight City Hall'', they will get you in the end.

Table 6 : A Summary of our findings and proposed solutions.

Finding	Proposed solution
Low levels of awareness.	Properly financed, targeted awareness campaigns similar to campaigns around GDPR where Regulator had both budget and statutory duty to promote awareness of the regulations.
Low levels of enforcement.	Increased enforcement pending new regulations passing through the European Parliament suggest developing automated audit tools to facilitate systematic and regular audits. Recommend a multiagency approach to enforcement in this area between the DPC and CCPC in Ireland given the dominant market position of Google.
Dark patterns.	Pre-approve CMP providers and promote standardized designs for CMPs, allowing for little latitude in how they are configured with the aim of configuring to the most privacy-friendly option.
Privacy paradox.	Continue to promote privacy awareness despite people's paradoxical behaviour, and do not let the privacy paradox become an excuse to dilute people's privacy.
Trust.	Consumers who trust how their data is being used may well consent to share more data about themselves ensuring that businesses become less reliant on information gathered from third parties, trust is the new currency.

Bibliography

Agarwal, S., 2021. *Digital Trends*. [Online]

Available at: <https://www.digitaltrends.com/features/google-cookies-alternative-chrome-privacy-sandbox-floc/>

[Accessed 7th March 2021].

Altair, 2022. *What is Data Wrangling?*. [Online]

Available at: <https://www.altair.com/what-is-data-wrangling/>

[Accessed 16 March 2022].

Andrews, D., Nonnecke, B. & Preece, J., 2003. Electronic survey methodology: A case study in reaching hard-to-involve internet users. *Journal of Human-Computer Interaction*, 16(2), pp. 185-210.

Bada, M., Sasse, A. & Nurse, J., 2015. *cyber security awarebess canpaigns, why do they fail to change behaviour..* [Online]

Available at:

https://www.researchgate.net/publication/274663655_Cyber_Security_Awareness_Campaigns_Why_do_they_fail_to_change_behaviour

[Accessed 13th December 2020].

Barth, S. et al., 2019. Putting the privacy paradox to the test. : Online privacy and security behaviors among users with technical knowledge, privacy. *Telematics and Informatics,,* 41(10), pp. 55-69..

BBC, 2010. *BBC News*. [Online]

Available at: <http://news.bbc.co.uk/2/hi/8548190.stm>

[Accessed 31st May 2020].

Bergman, A., 2020. *Survey Curious? Start-Up Guide and best practices for running survey and experiments online*, Chigago: University of Chicago, Booth School of Business..

Bocetta, S., 2020. *Globalsign Blog*. [Online]

Available at: <https://www.globalsign.com/en/blog/death-cookie>

[Accessed 15th March 2021].

Bryman, 2007. Barriers to integrating quantitative and qualitative research. *Journal of mixed methods research*, 1(1), pp. 8-22.

C.J.E.U., 2019. *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*. [Online]

Available at: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099en.pdf>

[Accessed 14 February 2021].

C.J.E.U., 2019. *InfoCuria Case Law*. [Online]

Available at:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=EN&>

[mode=lst&dir=&occ=first&part=1&cid=2706076](#)

[Accessed 14 February 2021].

Cartwright, E., 2020. *Why cyber security awareness campaigns fail?*. [Online]

Available at: <https://cyberprotect.our.dmu.ac.uk/2020/01/03/why-cyber-security-awareness-campaigns-fail/>

[Accessed 30 April 2021].

Chetty, P., 2016. *Limitations and weaknesses in quantitative research methods*. [Online]

Available at: <https://www.projectguru.in/limitations-quantitative-research/>

[Accessed 30th March 2022].

Ciochetto, S. & Haley, B. A., 1995. *HOW DO YOU MEASURE "AWARENESS"? EXPERIENCES WITH THE LEAD-BASED PAINT SURVEY*, Washington D.C.: Bureau of the Census, Center for Survey Methods Research, Washington, D.C..

Creswell, J. & Plano-Clark, V. L., 2007. *Designing and conducting mixed methods research*. 1st ed. Thousand Oaks, California: Sage.

Creswell, J. W., 2014. *Research Design, Qualitative, Quantitative and Mixed methods Approaches*. 4th ed. California: Sage.

CSO, 2019. *Central Statistic Office*. [Online]

Available at: <https://www.cso.ie/en/releasesandpublications/ep/p-isshh/informationstistics-households2019/householdinternetconnectivity/>

[Accessed 31st May 2020].

Daniel J. Solove & Neil M. Richards, 2010. Daniel J. Solove & Neil M. Richards, Prosser's Privacy Law: A Mixed Legacy, 98 Cal. L. Rev. 1887 (2010). *California Law Review*, 98(2010), p. 1887.

Dave Chaffey, 2020. *Smart Insights*. [Online]

Available at: <https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/>

[Accessed 31st MAY 2020].

De Vos, A., Strydom, H., Fouche, C. & Delport, C., 2002. *Research at Grass Roots: For the Social Sciences and Human Service Professions*. 1st ed. Pretoria: Van Schaik Publishers.

Deloitte, 2020. *Cookie Benchmark Study*. [Online]

Available at: <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-cookie-benchmark-study.pdf>

[Accessed 27th February 2021].

Deloitte, 2020. *Cookies & Website Tracking Technologies*. [Online]

Available at: <https://www2.deloitte.com/ie/en/pages/risk/articles/cookies-website-tracking-technologies.html>

[Accessed 6th April 2021].

- Denscombe, 2008. Communities of Practice: A research paradigm for the mixed methods approach.. *Journal of mixed methods research*, 2(1), pp. 270-283.
- Dolan, P. et al., 2010. *MindSpace: Influencing behaviour through public policy.*, London: Cabinet office: Institute for Government.
- DPC, 2020. *Guidance Note: Cookies and other tracking technologies*, Dublin: DPC.
- Executive office of the President, 2014. *Big data: seizing opportunities, preserving values.*, Washington D.C.: Executive office of the President.
- Fielding, N. F., 2012. Triangulation and mixed methods research. *Journal of mixed methods research*, 6(2), pp. 124-136.
- Forbrukerradet, 2018. *Deceived by design*. [Online]
Available at: <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/>
[Accessed 25 November 2021].
- Fricker, R. J., 2012. Sampling methods for online surveys.. In: J.Hughes, ed. *Sage handbook of online research methods*. London: Sage Publications, pp. 195-216.
- Glen, S., 2020. *Statistics How To, Snowball Sampling: Definition, Advantages and Disadvantages.* [Online]
Available at: <https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/snowball-sampling/>
[Accessed 16 March 2021].
- Gray, C. M. et al., 2018. *The (dark) patterns side of UX design*. Montreal, ACM.
- Gurkaynak, G., 2013. Understanding search engines: A legal perspective on liability in the internet law vista. *Computer law and security review*, 29(1), pp. 40-47.
- Hammerschmidt, J. & Manser, T., 2019. Nurses knowledge, behaviour and compliance concerns had hygiene in nursing homes.. *BMC Health Services Research*, Volume 547, pp. 1-10.
- Harriot, D., 2021. *Digital Marketing Institute, How the Privacy Paradox affects Business Growth*. [Online]
Available at: <https://digitalmarketinginstitute.com/blog/how-the-privacy-paradox-affects-business-growth>
[Accessed 6th June 2022].
- Holton, R., Swanson, A. & Elwood, F., 2005. *Research in Organisations: Foundations and methods in inquiry*. First ed. San Francisco: Berrett Koehler.
- Jacobson, J., 2020. Social media marketing: Who is watching the watchers. *Journal of Retailing and Consumer Services*, 53(101774), pp. 1-12.
- Johnson, L., 2018. *Problems in Research: Quantitative and Qualitative Methods*. [Online]
Available at: <https://classroom.synonym.com/problems-research-quantitative-qualitative-methods-4418.html>
[Accessed 30th March 2021].

Klingebiel, D. M., 2021. *Consent management – is it okay to “nudge” users?*. [Online]
Available at: <https://blog.eprivacy.eu/?p=1065>
[Accessed 5th October 2021].

Kokolakis, S., 2017. Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *computers & security*, 64(10), pp. 122-134.

Lapowsky, i., 2022. *Protocol*. [Online]
Available at: <https://www.protocol.com/bulletins/google-cookies-cma-deal#:~:text=Google%20has%20agreed%20not%20to,Sandbox%20plans%20are%20actually%20anticompetitive>.
[Accessed 16 March 2022].

Lexico.com, 2020. *lexico.com*. [Online]
Available at: <https://www.lexico.com/definition/privacy>
[Accessed 31st May 2020].

Martin, K., 2020. Breaking the Privacy Paradox: The value of privacy and associated duty of firms.. *Business Ethics Quarterly*, 30(1), pp. 65-96.

McKinsey, 2020. *The consumer-data opportunity and the privacy imperative*. [Online]
Available at: <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative>
[Accessed 27th April 2021].

Milne, G. R. & Culnan, M. J., 2004. STRATEGIES FOR REDUCING ONLINE PRIVACY RISKS WHY CONSUMERS READ OR DONT READ PRIVACY NOTICES.. *Journal of Interactive Marketing*, 18(3 CULNAN, GEORGE R. MILNE AND MARY J.), pp. 15-29.

Norton, T. C., Rodriguez, D. C., Howell, C. & Williams, S., 2021. *‘Maybe we can turn the tide’: an explanatory mixed methods study to understand knowledge brokers*. [Online]
Available at:
<https://www.ingentaconnect.com/content/tpp/ep/2021/00000017/00000001/art00002;jsessionid=1nm7r2u5jd7hj.x-ic-live-01>
[Accessed 19th January 2022].

Nouwens, M. et al., 2020. *Dark patterns after the GDPR*. Honolulu, ACM.

Obar, J. A., 2016. *Biggest lie on the Internet: Ignoring the Privacy policies and Terms of service policies of social networkingservices*, Toronto: Working Paper - York University.

OECD, 2010. *Guidelines for Cost-effective Agri-environmental Policy Measures*. [Online]
Available at: https://www.oecd-ilibrary.org/agriculture-and-food/guidelines-for-cost-effective-agri-environmental-policy-measures_9789264086845-en
[Accessed 15 March 2021].

- OneTrust, 2020. *Cookie Enforcement: What the DPC Wants You to Know*. [Online]
Available at: <https://www.onetrust.com/resources/cookie-enforcement-dpc/?v=video&ref=form>
[Accessed 12th November 2021].
- Othman, S. M., Steen, M. & Fleet, J.-A., 2021. A sequential explanatory mixed methods study design. *Journal of nursing education and practice*, 11(2), pp. 75-89.
- Potzch, S., 2009. *Privacy Awareness: A means to solve the privacy paradox.*, Dresden: Technische Universität Dresden.
- Rathesar/Redmond, R., 2019. *Hoe Microsoft's Brad Smith is trying to restore your trust in Big tech.*. [Online]
Available at: <https://time.com/5669537/brad-smith-microsoft-big-tech/>
[Accessed 31st May 2020].
- REFIT, 2016. *REFIT Platform Opinion on the submission by the Danish Business Forum on eprivacy directive*, Brussels: REFIT.
- Slattery, L., 2021. *www.irishtimes.com*. [Online]
Available at: <https://www.irishtimes.com/business/media-and-marketing/demise-of-cookies-expected-to-put-further-pressure-on-irish-media-1.4661229>
[Accessed 20th October 2021].
- Slyke&J.T.Shim&Richard, C. V., 2006. Concern for Information privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems*, 7(6), pp. 415- 444.
- SmarterHQ, 2020. *SmarterHQ.com*. [Online]
Available at: <https://smarterhq.com/privacy-report>
[Accessed 31st May 2020].
- Spiekermann, S., Grossklags, J. & Berendatt, B., 2001. *Research Gate*. [Online]
Available at:
https://www.researchgate.net/publication/242093728_Stated_Privacy_Preferences_versus_Actual_Behaviour_in_EC_Environments_a_Reality_Check
[Accessed 16 March 2021].
- Statcounter, 2022. *Search Engine Market Share Ireland*. [Online]
Available at: <https://gs.statcounter.com/search-engine-market-share/all/ireland>
[Accessed 19th April 2022].
- Subedi, D., 2016. Explanatory sequential mixed methods design. *American Journal of Educational Research*, 4(7), pp. 570-577.
- SurveyMonkey, 2020. *Non probability sampling*. [Online]
Available at: <https://www.surveymonkey.com/mp/non-probability-sampling/>
[Accessed 30 March 2021].

Teherani, A. et al., 2015. Choosing a qualitative research approach. *Journal of Graduate Medical Education*, 7(4), pp. 668-670.

Toyen, M. A. S., 2021. Explanatory sequential design of mixed methods research: Phases and Challenges.. *International Journal of Research In Business and Social Science*, 10(5), pp. 253-260.

Trevisan, M., Traverso, S., Bassi, E. & Mellia, M., 2019. 4 Years of EU Cookie Law: Results and Lessons learned. *Proceedings on Privacy Enhancing Technologies*, Volume 2, pp. 126-145.

Watson, 2015. Quantitative Research. *Nursing Standard*, 29(31), pp. 31-44.

Wynveen, C. J. & Sutton, S. G., 2017. Engaging great barrier reef stakeholders.. *Human Dimensions of Wildlife*, 22(2), pp. 126-141.

YouGov, 2015. *Advn.com*. [Online]

Available at: <https://www.advn.com/stock-market/stock-news/66296774/concerns-about-data-privacy-online-force-british-c>

[Accessed 31st May 2020].

Zuboff, S., 2015. Big Other: surveillance capitalism and the prospects of an information civilization. *Journal of Information technology*, 30(3962/15), pp. 75-89.

Appendices

Appendix A: Ethics Approval Form



Taught Programme Research Ethics Approval Application Form

Research undertaken by taught students must receive ethical approval unless deemed exempt. This application form may be completed by an individual student or by a Programme Board/Lecturer for a group of similar research projects.

This application is completed by:

Student: OR Lecturer on behalf of Programme Board:

PART A

Applicant Details	
Name:	Pat Rowland
Student ID: (If relevant)	G00388175
Programme Title:	MSc. Digital Media and Marketing
Programme Stage:	Final research module before Thesis Commencement.
Research Supervisor's Name: (If relevant)	Dr. Janine McGinn/Dr. Eoin Cullina

Project Details	
Research Study Title:	A study of the societal awareness and effectiveness of the EU Privacy and Electronic communication directive (EU Cookie law) in Ireland one year after implementation.
Research Study Summary (max 100 words):	
In today's increasingly information and digital age there is widespread use of search engines and social networks sites. The use of this media form seems to be ubiquitous as it cuts	

across all age groups, social classes, and cultures. Online Behavioural Advertising (OBA) through the tracking of users has allowed for the development of user targeted campaigns which traditional legal principles have struggled to come to terms with. It has fallen to the European Union and subsequently governmental organisations such as the Data Protection Commission (DPC) in Ireland to implement guidelines by which users must actively consent before cookies can be set up.

The aim of this analysis is to measure the awareness and effectiveness on a regulatory, business and consumer level of the recent EU Privacy and Electronic Communication (e-privacy) directive (EU Cookie Law), (S.I. No. 336/211) and how this may affect future policy.

Although there is some European research in this field there is limited research in Ireland apart from helpful guidance notes from the Data Protection Commission and numerous Legal publications outlining the requirement to comply and penalties for noncompliance with the directive. The regulators moved to update its guidance in 2020 after identifying widespread failings of compliance during a sweep of websites in 2019. Given the widespread noncompliance there is, however, a lack of research into awareness of the directive by the various stakeholders.

Awareness is an essential tool in the understanding and evaluation of the success of any legislation (DeLavega, 2004) and this study will attempt to gauge the awareness of the directive across the three key stakeholders.

Risk Checklist			
Please answer ALL the questions in each of the sections below – Tick YES or NO			
	Will the research study....?	YES	NO
1	Involve direct and/or indirect contact with human participants?	✓	
2	Involve analysis of pre-existing data which contains personal or sensitive information not in the public domain?	✓	
3	Require permission or consent to conduct?	✓	
4	Require permission or consent to publish?	✓	
5	Have a risk of compromising confidentiality?	✓	
6	Have a risk of compromising anonymity?	✓	
7	Collect/contain personal data i.e., any information that relates to an identified or identifiable individual?		✓
8	Collect/contain sensitive personal data e.g., health data, sexual orientation, race religion?		✓
9	Contain elements which you OR your supervisor is NOT trained to conduct?		✓

Risk Checklist			
Please answer ALL the questions in each of the sections below – Tick YES or NO			
	Will the research study....?	YES	NO
10	Use any information OTHER than that which is freely available in the public domain?	✓	
11	Involve respondents to the internet or other visual/vocal methods where participants may be identified?		✓
12	Include a financial incentive to participate in the research?		✓
13	Involve our own students or staff?		✓
14	Take place outside Ireland?		✓
15	Involve participants who are vulnerable or at risk?		✓
16	Involve any participants who are unable to give informed consent?		✓
17	Involve data collection taking place BEFORE informed consent is given?		✓
18	Involve any deliberate deception or covert data collection?		✓
19	Involve a risk to the researcher or participants beyond that experienced in everyday life?		✓
20	Cause (or could cause) physical or psychological harm or negative consequences?		✓
21	Use intrusive or invasive procedures?		✓
22	Involve a clinical trial?		✓
23	Involve the possibility of incidental findings related to participant health status?		✓
24	Involve the remuneration of research participants?		✓

If, as a student, you answered **NO** to all the above questions your research supervisor will review, and if in agreement sign below to indicate that this form does not have to be submitted to the Taught Programme Research Ethics Committee.

<i>Name</i>		<i>Signature</i>		<i>Date</i>	
	Research Supervisor				

If you answered **YES** to any of the above questions, you need to complete part B below.

PART B

1	Project Overview
<p>Please give a brief overview of the study, including a summary of the aims and objectives.</p> <p><u>Help:</u> Describe the purpose of the research and what question(s) the project should answer.</p>	
<p>The main purpose of the research is to determine the societal awareness of the aforementioned E-privacy directive in Ireland and ultimately whether further policy changes are warranted to increase the level of awareness of this important directive.</p> <p>From our literature review we have established that privacy protection is of clear importance to consumers and a strong privacy framework is paramount. There is some evidence however consumers visiting websites ignore the privacy policies and see them as nothing more than an unwanted impediment to the sole purpose of getting online (Obar, 2016), thereby diluting the effectiveness of the E-privacy directive.</p> <p>Masden (1996) emphasized the concept that awareness is the ultimate driving force that stimulates knowledge and awareness is an essential tool in the understanding and evaluation of the success of any legislation (DeLavega, 2004).</p> <p>We intend to gauge the level of awareness and effectiveness of the Directive across three different sub-sets</p> <ul style="list-style-type: none">• The Regulatory framework more specifically the Data Protection Commission• The Business framework more specifically at an executive level.• Consumers of Online Content <p>We would hypothesize that whilst there is an acceptable level of awareness about the Directive across all three sectors it still may not be at the required level given the Commissions own findings of widespread noncompliance in 2019.</p> <p>We would also posit that the Directive is counterproductive in that consumers faced with a constant stream of cookie notices blindly accept these notices with the sole intention of getting online as quickly as possible (EU REFIT Platform 2016). In addition, Companies have spent significant revenue on compliance with the Directive and may be better served concentrating on elevating the privacy discussion from a mere compliance need to a business strategy for growth.</p>	

From a consumer standpoint despite what people say about privacy and cookie awareness there seems to be disparity between what they say and what they do with preliminary research showing a 95% acceptance rate as of November 2020. (Teads 2020)

Finally, we will need to examine whether all this work is in vain as Apple and now Google are developing browser technologies that will replace cookies within the next two years casting doubt on the regulators ability to keep up with advanced technological development.

The paper will conclude by recommending methods which can be used to increase awareness of the directive if required.

2	Methodology
<p>Please give a description of the methodology, including any data collection and analysis methods.</p> <p><u>Help:</u> Give an outline of the study here. If the project is complex, you can also submit the research proposal/protocol (no more than 2-3 A4 sides) if this would help the reviewer's understanding of the project. Include details of your (or the Research Supervisor's) appropriate skills and qualifications to carry out this research. Consideration of how, and for what duration are stored should be provided under Section 7 below.</p>	
<p>A comparative case study analysis of the awareness and effectiveness of the implementation of the E-privacy directive (2019) across three different stakeholder groups will be carried out to gauge the level of awareness of these new regulations across different stakeholders and contexts.</p> <p>This research will consist of a qualitative research approach with semi structured expert interviews, surveys and possibly a focus group study with some of the industry participants.</p> <p>We hope to conduct interviews with individuals at management level with a minimum of 10 diverse organisations all of whom are active on social media and are involved in Digital marketing Campaigns.</p> <p>There will a broad range of organisations interviewed from retail to wholesale, Sporting Bodies and possibly even some state institutions.</p> <p>There will interviews with the Regulator's as to their perception of awareness and compliance of the directive.</p>	

Finally, we intend to survey up to 20 website users to gauge their awareness of the new legislation.

A pilot study will take place using social contacts as participants in the Consumer segment of our study as well as an interview with one industry representative and one expert in regulation in preparation of our questions with Industry groups and the Regulator. This will enable us to prepare relevant questions, hone our interview technique and ensure that we are gathering relevant information in our limited timeframe. I will be guided in developing my questionnaires and interview technique with my primary supervisor Dr. Janine McGinn who has considerable relevant experience in this area having recently completed her doctoral research thesis.

Participants at CEO/CTO level from up to 10 cross national organisations across industry and society will be contacted and interviewed as part of this research. All these bodies have given a preliminary indication that they are willing to cooperate. The recruitment strategy for this cohort is similar to the strategy employed by the DPC in 2019 in their examination of the use of cookies and similar technologies on a selection of websites across a range of sectors including media and publishing, the retail sector, restaurants and food ordering services, insurance, sport and leisure and the public sector. Their strategy was to get as wide a survey as possible across different sectors and we intend to apply a similar approach to try and gauge awareness levels across diverse sectors. The DPC examined 40 controllers, but our survey will be limited to 10 or less given the limited time and resources available for our study.

The Regulator in this instance is the office of the Data Protection Commissioner and I will contact this organisation through their communications department having initially spoken to an employee of the commission through a Data Sweep carried out by the DPC on 38 cross national organisations in 2019.

Consumers will be from a wide spread of social contacts, colleagues, and other contacts all of whom are users of Online content. Some of this cohort has been previously used for newsletter circulation and well as testing scenarios as part of the exercises for the Post Graduate Certificate in 2020 and are all active consumers of online content. The recruitment strategy for this cohort will target consumers of online content and/or users of social media. The questionnaire will be sent to a minimum of 20 people to mirror a sample population to ascertain their awareness of the directive with the expectation that some of these participants will forward the survey to other members of their social circle.

Timeline: This research will be carried out over a period of three months post Ethics approval.

In light of the Public Health Emergency all interviews will be conducted remotely and subject to consent will be recorded on Microsoft teams as well as via Smartphone.

3	Main Ethical Considerations
<p>Please give a brief description of the main ethical considerations involved in the study. <u>Help:</u> Highlight here the main ethical considerations for the study (which may concern, e.g., the type of participants, the sensitive nature of the study, the data collection process, security-sensitive research) and advise how the main issues will be addressed. If the project is funded, give details here, and whether there are any potential conflicts of interest involved in the study. NB: Section 5 below addresses: recruitment; voluntary participation; consent; and the right to withdraw. Those details need not also be entered here.</p>	
<p>The main ethical concerns identified in my research are the following.</p> <ol style="list-style-type: none"> 1. We will be gathering as part of our research, some sensitive and possibly confidential information in relation to turnover, marketing policies, data gathering and budgets. We will deal with this by ensuring that all data gathered via interviews, audio recordings and surveys will be anonymised, and process checked by my supervisors before the analysis process. 2. The project is not funded, and no participants will get any reimbursement for partaking in the study. 3. I have personal relationships with some of the key executives in the organisations that will hopefully participate in the project. The integrity of interviews conducted with these participants will be addressed through the structuring of the interview protocol and questions in conjunction with my supervisors. 4. Consumers will be selected from social contacts and the Regulators will be contacted formally as part of this study. 5. Measuring awareness or knowledge can create some challenges. It is important to measure what respondents know as well as what they do not know. There is a risk that people respond by guessing rather than admitting that they do not know Bishop (1980) and questions regarding awareness and knowledge will be structured so that respondents feel comfortable reporting a “don’t know”. 6. I also intend to interview our own marketing department as part of this process. In relation to interviewing our own marketing department cognizance will be given to a possible power imbalance and it will be explained in advance that participation is voluntary and can be terminated at any time. The interview will be structured in 	

consultation with my supervisors to address the proper protocol given the unique circumstances involved.

7. All research and data gathered will be done in compliance with the GDPR legislation.

4	Human Participants
----------	---------------------------

If the study includes Human Participants (or their data), please give a description of who will be included.

Please note this should include sample size/number of participants, whether the project will focus on any particular groups/individuals, if it will include any at risk or vulnerable participants, participants aged 16 years or under, etc. Please also specify the rationale for including / excluding groups of participants.

- If the research involves secondary data not in the public domain, give details in this section.

I intend to interview Management professionals from up to 10 cross national organisations between Retail, Media, sporting organisations and possibly some Governmental bodies.

In addition, I intend to interview representatives from the DPC who have overall responsibility for the implementation of this directive and possibly the European Commission as part of the regulatory framework.

Finally, I intend to survey up to twenty volunteers from selected groups all of whom are consumers of online content.

All participants will be voluntary, will be asked for consent prior to the commencement of research and all are over 18 years of age and in the case of consumers will be a mix of male and female and the respondents will be matched with the statistical data of the profile of users using online content.

5	Recruitment, Voluntary Participation, Consent and Right to Withdraw
----------	--

If the study includes Human Participants, please give a brief description of the recruitment process, how voluntary participation will be ensured, if (and how) informed consent will be obtained prior to participants taking part in the study, and the right of withdrawal from the research process.

Help:

- This should include clear information on how participants will be identified, approached and recruited; whether the study will include any covert research or

deliberate deception; whether help is required from a third party/ gatekeeper to access participants; what information will be given to participants, etc.

- If expenses or any incentives are to be offered to participants, give full details.
- If research involves students, colleagues and/or other employees then specify the rationale for this and how issues of coercion or feelings of obligation will be addressed.
- If data is held on participants, research using that data may require permission from the participant.
- Regarding withdrawal from the study, discuss the different stages/dates a participant could withdraw or withdraw their data, and how they could do this.

I have identified up to 20 cross national organisations that may give a good representative sample across different businesses.

In addition, I will interact with the Regulator and up to 20 consumers of online content.

In the case of the business suite intend to contact their Marketing Departments directly in some instances or indirectly via some key executives in the business that I would know in a professional capacity.

The research will be carried out by means of expert interviews and possibly focus groups. All participants will be required to sign a consent form prior to the commencement of the research.

Permission will be sought to use any of the information gathered for the purposes of a dissertation and possible presentation at Digital West Event and the individuals and organisations will be anonymised to protect their identities.

Confidentiality and anonymity will be warranted and there will be no reward for participation.

It will be explained to them from the outset that they can withdraw from the project at any time by contacting me prior to publication and they will be given details of the project timeline to enable them to do so if they wish.

As indicated above a pilot study will take place using social contacts as participants in the Consumer segment of our study as well as an interview with one industry representative and one expert in regulation in preparation of our questions with Industry groups and the Regulator.

This will enable us to prepare relevant questions, hone our interview technique and ensure that we are gathering relevant information in our limited timeframe. I will be guided in developing my questionnaires and interview technique with my primary

supervisor Dr. Janine McGinn who has considerable relevant experience in this area having recently completed her doctoral research thesis.

6

Risks and Benefits

Please give a brief description of how, when and where the research will take place and whether there are any risks and/or benefits involved.

Help:

- This should include information on what participants will be required to do, the rationale for this and the level of risk involved.
- When considering risks, please refer to risks to the participants (e.g., for research in sensitive areas, where there is a balance of power), the researcher, any other parties to the research; and also, any health and safety issues for anyone involved (e.g., for lone researchers carrying out fieldwork).

The research will be carried out by means of initial contact with a follow up interview and possibly a focus group with the Regulators and Industry representatives. The initial contact will be via e-mail firstly giving a detailed description of the nature of our study as detailed in our Participant Information Leaflet attached. Once we receive the signed consent form, we will begin our research.

Our consumer group will be contacted via text message or e-mail with a questionnaire to be filled in.

Given the current Public Health situation I do not envisage any face-to-face meetings and any interviews will be conducted via phone or other electronic means.

Participants will not be required to do anything that compromises their safety thereby minimizing any risks.

7	Personal Data, Anonymity and Confidentiality
<p>Please specify what type of information/data will be collected/analysed and the source(s). In addition, specify if and how the anonymity of participants will be ensured, and information be kept confidential.</p> <p><u>Help:</u> This should include information on whether new information/data are being collected or uses data that are already in the public domain; whether the data includes personal data; whether the data includes sensitive personal data e.g. health data, sexual orientation, race, religion; how the data will be processed and stored; who will have access to it; who it will be shared with; how long data will be retained; how it will be destroyed; the Data Protection requirements for any sensitive personal data, etc. In addition, include whether there may be any requirements for disclosure of information to other parties due to professional practice or legal reasons. If there are limits to confidentiality, explain clearly how the participants would be advised about these limits and possible outcomes.</p>	
<p>The information collected will solely relate to the awareness of the directive and data privacy policies of the organisations involved consumer behaviour and Regulatory guidelines and may involve evidence of turnover and marketing budgets to give some perspective to the study.</p> <p>All transcripts and audio recordings will be anonymised in order to protect the organization and individual and to encourage participation.</p> <p>Given that there are no vulnerable or at-risk persons participating in the research there should be no situation where we must break confidentiality.</p> <p>Signed consent forms will be kept until the conclusion of the research but will be stored separately to the interview transcripts or audio recordings which will be assigned pseudonyms to protect the identity of the interviewees.</p> <p>All the research information signed consent forms and original audio recordings will be securely stored on an encrypted laptop until after the Master’s degree has been conferred and the findings from this study have been presented at the Digital West Conference in 2022 after which the data will be deleted. The researcher will be the only person with access to this device.</p> <p>A transcript of interviews in which all identifying information has been removed will be retained in line with the timeframe as outlined above. Under freedom of information legalization participants will be entitled to access the information you have provided at any time.</p>	

8	Reporting and Dissemination
<p>Please give details of the planned dissemination and specify if the findings from the research will be published and whether any permission is required for this.</p> <p><u>Help:</u> This should include information on the methods of dissemination (e.g., dissertation/thesis) and/or what will be published and where (research papers, conference presentations). Specify if any permission is needed (e.g., from participants, clients, gatekeepers, etc.) prior to publication, and whether there are any potential issues relating to Intellectual Property Rights when creating or using materials.</p> <p>This research is solely for the purpose of a research Dissertation and possible presentation at the Digital West Conference 2022, an annual digital media conference in association with GMIT. Permission will be sought from all participants on that basis.</p> <p>I don't envisage any issues in relation to intellectual property rights unless some new constructs arise during the course of this research project.</p>	

9	Location of research
<p>Will the research take place outside of Ireland?</p> <p>YES <input type="checkbox"/> NO <input checked="" type="checkbox"/> If yes, give details below.</p> <p><u>Help:</u> If yes, please specify where the research will take place. Research must comply with the laws of the country where it is taking place and also comply with local Data Protection and Intellectual Property legislation: you must confirm that your research is compliant with local requirements and how you have ascertained this. Advise if the project requires ethical approval in-country and how this has been ascertained. If approval is required, a copy of this should be included in the application or details of the process of how it will be obtained. Please make reference to insurance and indemnity cover for the project where relevant.</p> <p><u>Note:</u> If data is to be processed or stored outside the EEA contact dpo@gmit.ie</p>	

10	Collaborative Projects
Is the research a collaborative project (i.e., it involves more than one institution)?	
YES <input type="checkbox"/> NO <input checked="" type="checkbox"/> If yes, give details below.	
<p><u>Help:</u> If yes, please specify the other institutions involved and if ethical approval needs to be / has been given by them. Please also specify what procedures have been put in place to ensure ethical compliance from all partners.</p> <p><u>Note: If personal data is being shared between institutions, then a data sharing agreement must be in place. Contact dpo@gmit.ie</u></p>	

11	Any other permission or external ethical approval required to undertake the project
Please specify if the project requires any other ethical approval or permissions not mentioned previously in this application and how and when these will be obtained.	
<p><u>Help:</u></p> <ul style="list-style-type: none"> • Other permissions: ethical approval does not give the right of access to the Institute’s students, staff or the use of Institute premises to carry out research, and you may need to contact an appropriate Institute gatekeeper for agreement to approach potential participants or for the use of premises, so please give details. • Gatekeepers: permission of a gatekeeper for initial access to participants may be required or to carry out data collection on their premises. • If the project requires approval from an external ethics committee, this should normally be obtained prior to submitting this application. • If a Disclosure and Barring Service check is required due to the specific participant group, give details. • Regarding insurance and indemnity cover, some projects will require individual confirmation of cover. See the Research Ethics Procedures document for more details. 	

None that I aware of at this time.

SUPPORTING DOCUMENTATION: what to submit with the application

For projects involving human participants, you must submit, where appropriate, the Participant Information Sheet/s and consent form/s. You must also submit every communication a participant will see or receive. Failure to do so will cause delays to the application.

Please find attached a participant information leaflet, a consent form, interview schedule/guide as well as a draft consumer questionnaire.

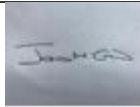
DECLARATIONS AND SIGNATURES**STUDENT**

I confirm that I will undertake this project as detailed in Part A and Part B of the application. I understand that I must abide by the terms of this approval and that I may not make any substantial amendments to the project without further approval. I understand that research with human participants or their data must not commence without ethical approval.

Signature	Patrick Rowland	Date	14/04/21
-----------	-----------------	------	----------

RESEARCH SUPERVISOR RECOMMENDATION FOR STUDENT PROJECT

I confirm that the committee has considered part A and part B of the application. The project is viable and the student has appropriate skills to undertake the project. Where applicable, the Participant Information Sheet and recruitment procedures for obtaining informed consent are appropriate and the ethical issues arising from the project have been addressed in the application. I understand that research with human participants must not commence without ethical approval. I recommend this project for approval.

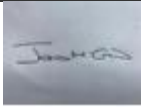
Name	Research Supervisor	Signed		Date	14/04/21
------	---------------------	--------	---	------	----------

Comment(s):

I am pleased to present this for ethical review. It might be helpful to the TPREC to know that this postgraduate researcher, has specialist knowledge and qualifications in engineering, and in the assessment of regulatory frameworks as he is qualified as a barrister (JMcG).

LECTURER ON BEHALF OF PROGRAMME BOARD

I confirm that the project will be undertaken as detailed in stage one and stage two of the application. I understand that I must abide by the terms of this approval and that I may not make any substantial amendments to the project without further approval. I understand that research with human participants or their data must not commence without ethical approval.

<i>Signed</i>		<i>Date</i>	14/04/21
---------------	---	-------------	----------

PROJECTS APPROVED BY THE RESEARCH ETHICS SUB-COMMITTEE					
<i>I confirm that this project was considered by the Taught Programme Research Ethics Committee and has received ethical approval.</i>					
<i>Chair</i>		<i>Signed</i>		<i>Date</i>	

This form will be retained for the purposes of quality assurance of compliance and audit for THREE years

PARTICIPANT INFORMATION LEAFLET FOR RESEARCH PROJECT 2021

- Interviews/Focus Groups

I would like to invite you to take part in a research study. Before you decide, you need to understand why the research is being done and what it would involve for you. Please take time to read the following information carefully. Ask questions if anything you read is not clear or if you would like more information. Take time to decide whether or not to take part.

PROPOSED RESEARCH TOPIC /TITLE

A study of the societal awareness and effectiveness of the EU Privacy and Electronic communication directive (EU Cookie law) in Ireland one year after implementation.

WHO I AM AND WHAT THIS STUDY IS ABOUT:

My name is Pat Rowland and I in the process of preparing a thesis as part of my requirement to submit a dissertation for a Master’s in Digital Media and Marketing.

The aim of this analysis is to measure the awareness and effectiveness on a regulatory, business and consumer level of the recent EU Privacy and Electronic Communication (e-privacy) directive (EU Cookie Law), (S.I. No. 336/211) and how this may affect future policy.

Although there is some European research in this field there is limited research in Ireland apart from helpful guidance notes from the Data Protection Commission and numerous Legal publications outlining the requirement to comply and penalties for noncompliance with the directive. The regulators moved to update its guidance in 2020 after identifying widespread failings of compliance during a sweep of websites in 2019. Given the widespread noncompliance we are attempting to gauge awareness of the directive by the various stakeholders.

WHAT WILL TAKING PART INVOLVE?

The main purpose of the research is to determine the societal awareness of the aforementioned E-privacy directive in Ireland and ultimately whether further policy changes are warranted to increase the level of awareness of this important directive.

To do this we intend to gauge the level of awareness and effectiveness of the Directive across three different sub-sets

- The Regulatory framework more specifically the Data Protection Commission
- The Business framework more specifically at an executive level.
- Consumers of Online Content

A comparative case study analysis of the awareness and effectiveness of the implementation of the E-privacy directive (2019) across the three different stakeholder groups will be carried out to gauge the level of awareness of these new regulations across different stakeholders and contexts.

This research will consist of a qualitative research approach with semi structured expert interviews, surveys and possibly a focus group study with some of the industry participants. We have set out below what the interaction with the three subsets will involve.

Business Framework: We hope to conduct interviews with individuals at management level with a minimum of 10 diverse organizations all of whom are active on social media and are involved in Digital marketing Campaigns. There will a broad range of organizations interviewed from retail to wholesale, Sporting Bodies and possibly even some state institutions. Interviews are scheduled to take 30 Minutes approximately, will be recorded if permission is given for same and will be conducted remotely via Microsoft Teams or similar medium.

Regulator: There will interviews with the Regulator's as to their perception of awareness and compliance of the directive. Interviews again are scheduled to take 30 Minutes approximately, will be recoded if permission is given for same and will be conducted remotely via Microsoft Teams or similar medium.

Consumer: We intend to survey up to 20 website users to gauge their awareness of the new legislation. We would hope that this sample group will be a mix of male and female and the respondents will be matched with the statistical data of the profile of users using online content. This consumer group will be contacted via text message or e-mail with a questionnaire with appropriate privacy riders to be filled in which will take around 15 minutes to complete.

Topics for Discussion: Awareness of the privacy Directive, Cookie and Privacy Policies, Effectiveness of legislation, % of consumers managing Cookies, Ways to improve awareness, Alternatives to Cookies, Industry and Consumer attitudes, Trust, Ethics, Ethical Design.

WHY HAVE YOU BEEN INVITED TO TAKE PART?

You have been invited to take part as you fall within one of the three Research Groupings as detailed above and have been selected on the basis that you or your organization has an interest in this study, is a user of online content and/or has given a preliminary indication that you are willing to participate.

DO YOU HAVE TO TAKE PART?

There is no Obligation to participate in this Research Study. Participation is entirely voluntary, and all participants will be asked for consent prior to the commencement of research interviews or surveys.

You can refuse to answer any question or withdraw from the process at any stage prior to publication except in the case of the Consumer survey whereby you will be unable to withdraw once the questionnaire is submitted as your responses will be unidentifiable.

Your response, and all data, will be treated with full confidentiality and transcripts of all interviews and recordings will be anonymised.

WHAT ARE THE POSSIBLE RISKS AND BENEFITS OF TAKING PART?

In any project where there is sensitive data being collected there is a risk that confidentiality and anonymity may be compromised, and we have detailed below how we intend to protect this data and eliminate/mitigate any breaches.

Awareness studies are essential tools in the understanding and evaluation of the success of any legislation and this legislation forms part of the suite of legislation emanating from the GDPR regulations with similar penalties for non-compliance. Both supervisory authorities and courts are now taking action for non-compliance, and it is essential that organizations comply with these regulations and look for alternatives to online behavioural advertising which require consumer consent under the e-privacy directive. This study may help in gauging the awareness of this

directive and give suggestions on how to improve awareness and compliance or develop alternatives to the use of cookies.

WILL TAKING PART BE CONFIDENTIAL?

The information collected will solely relate to the awareness of the directive and data privacy policies of the organizations involved consumer behaviour and Regulatory guidelines and may involve evidence of turnover and marketing budgets to give some perspective to the study.

All transcripts and audio recordings will be anonymised in order to protect the organization and individual and to encourage participation.

Given that there are no vulnerable or at-risk persons participating in the research there should be no situation where we must break confidentiality.

Signed consent forms will be kept until the conclusion of the research but will be stored separately to the interview transcripts or audio recordings which will be assigned pseudonyms to protect the identity of the interviewees.

HOW WILL INFORMATION YOU PROVIDE BE RECORDED, STORED AND PROTECTED?

All the research information signed consent forms and original audio recordings will be securely stored on an encrypted laptop until after the Master's degree has been conferred and the findings from this study have been presented at the Digital West Conference in 2022. The researcher will be the only person with access to this device.

A transcript of interviews in which all identifying information has been removed will be retained in line with the timeframe as outlined above. Under freedom of information legislation, you are entitled to access the information you have provided at any time.

WHAT WILL HAPPEN TO THE RESULTS OF THE STUDY?

This research is solely for the purpose of a research Dissertation and possible presentation at the Digital West Conference 2022, an annual digital media conference in association with GMIT and in academic journals if requested. Permission will be sought from all participants on that basis.

All the participants can request a copy of the completed study.

WHO SHOULD YOU CONTACT FOR FURTHER INFORMATION?

Researcher: Pat Rowland: Pat.Rowland@research.gmit.ie

Primary Supervisor: Dr Janine McGinn: Janine.Mcginn@gmit.ie

Secondary Supervisor: Dr Eoin Cullina: Eoin.Cullina@gmit.ie

PARTICIPANT CONSENT FORM

By signing and returning this consent form you are indicating your agreement with the following statements:

- I have read and understood the attached *Participant Information Leaflet* for this study.
- I have had the opportunity to ask questions and discuss the study.
- I have received satisfactory answers to all my questions, where I have had a query.
- I have received enough information about this study.
- I do/do not consent for the interview/focus group will be audio recorded.
- I understand I do not have to answer any of the questions and that I may exit the interview at any time.
- I do/do not wish to be sent a summary of the findings when the project is complete
- I agree to take part in the study.

Participant's Signature: _____

Date:

Participant's Name in Print: _____

Contact Email: _____

RETURNING THE CONSENT FORM: We would ask you to please return the attached consent form to Pat.Rowland@research.gmit.ie

INTERVIEW SCHEDULE/GUIDE

Interview Questions Document.

Researcher: Mr. Pat Rowland Master of Science Student in Digital Media and Marketing program 2021.

Research Context: A comparative case study analysis of the awareness and effectiveness of the implementation of the E-privacy directive (2019) across three different stakeholder groups. This research will be carried out to gauge the level of awareness of these new regulations across different stakeholders and contexts.

This research will consist of a qualitative research approach with semi structured expert interviews, surveys and possibly a focus group study with some of the industry participants, Regulators and Consumers.

Research Title: A study of the societal awareness and effectiveness of the EU Privacy and Electronic communication directive (EU Cookie law) in Ireland one year after implementation.

Prompts for Researcher

- a) Indicate that all responses and all data garnered from this research will be treated with full confidentiality and that all participants will be assured of their anonymity. In the case of recorded interviews, the name of the participant will be stated on the recording, but the recording will be erased once the transcript is written, and each participant will be assigned an encrypted pseudonym.
- b) Completion of consent forms.
- c) Permission to record the interview and required signature.
- d) Approximate duration of the interview (30 minutes)
- e) The aim of the interview is to measure the awareness and efficacy on a regulatory/ business/ consumer level of the recent EU Privacy and Electronic Communication (e-privacy) directive (EU Cookie Law), (S.I. No. 336/211) and how this may affect future policy.

In addition, we hope to explore whether any further policy changes are warranted to increase the level of awareness of this important directive and whether consumers are aware of and are taking cognizance of this legislation.

f) Participant information: Name / gender / age bracket / contact information/number of years employed within the organization /Job title; / areas you are responsible for/responsibility for data privacy/regulation.

Sample Questions:

Q1. How aware is your organization with the recent e-privacy directive?

- a. Are you familiar with this recent legislation?
- b. Who in your organization is responsible for its implementation/compliance?
- c. How advanced is your organization in their implementation plans?
- d. How confident are you that you are complying with this directive?
- e. What does successful compliance look like?
- f. How would you rate this legislation in terms of Data Privacy?
- g. Do you see this legislation and the whole privacy discussion as a mere compliance need or do you see any possibilities to use this as a business strategy for growth?

Q2 (a). Explain how committed your organization is to Data Privacy?

Q2 (b). Please give examples of other recent initiatives to improve your Data privacy policy.

Q3. How has the recent EU directive helped you improve your privacy policies?

Q4. How do you perceive this legislation from a consumer privacy standpoint?

Q5. How does this legislation help your customers increase their trust in your organization?

Q6. What % of respondents (consumers) actively manage cookies when visiting your website?

Q7. What impact have these regulations had on your business and privacy policies?

Q8. How has this legislation helped your customers increase their trust in your organization?

Q9. Has the rate of Cookie non acceptance decreased since you first implemented your CMP?

Q10. How aware are you of new browser tracking technologies being developed to replace cookies? Please give examples.

Q11. How can the Regulators keep up with the technological developments?

Q12. How can the awareness of the directive be improved?

Q13. How is your Marketing spending split between Traditional mediums and Digital?

DRAFT CONSUMER QUESTIONNAIRE

You are being asked to complete the following questionnaire as a consumer of Online content in Ireland in 2021. This questionnaire will take approximately 10-15 minutes of your time. The purpose of this study is to gauge the societal awareness of the recent EU Privacy and Electronic Communication directive in Ireland. The information gained from this study will be used as part of a postgraduate thesis and possible presentation at the Digital West Conference in 2022. Your

involvement in this study is completely voluntary. Your response, and all data, will be treated with full confidentiality and all information is completely anonymous. Information will be stored online in a secure password-protected space. You can withdraw from the study at any point before the final submission of this questionnaire and your response will be deleted. Once you submit the questionnaire you will no longer be able to withdraw as your responses will be unidentifiable.

By clicking the button below,

I confirm that I have received an explanation of the nature and purpose of the study and what my involvement will be.

I confirm I am at least 18 years of age.

I understand that my participation is voluntary and that I can decide to opt-out of the research at any time until I submit the final questionnaire and I can do so by exiting the webpage.

I understand that all information gathered about me during this study will be treated with full confidentiality.

- I consent, begin the study
- I do not consent, I do not wish to participate

DRAFT CONSUMER QUESTIONNAIRE

Q1. Do you identify as

- Male
- Female
- Other

Q2. What age are you at present?

- 18-25
- 26-35
- 36-55
- 55+

Q3. Are you a consumer of online content and digital media?

- Yes
- No

Q4. How often do you use the following online platforms?

Please only put one tick, but answer EVERY line

	Rarely or never	Less than 1 a Week	Once a Week	2-3 times a Week	4-6 times a Week	1-2 times a Day	3-4 times a Day	5+ a Day
Social Media (F/B, Twitter, Instagram, TikTok)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Websites	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Internet Ads	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please only put one tick, but answer EVERY line

	Rarely or never	Less than 1 Week	Once a Week	2-3 times a Week	4-6 times a Week	1-2 times a Day	3-4 times a Day	5+ times a Day
E-Mail Marketing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other (Please Specify)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q5. Are you aware of Cookies?

- Yes
- No

Q6. Are you aware of the recent EU Privacy and Electronic Communication (e-privacy) directive implemented in Ireland in 2020?

- Yes
- No

Q7. Have you recently noticed more Cookie banners in accessing your content?

- Yes
- No

Q8. Do you think the Cookie Acceptance tools improve your privacy?

- Yes
- No

Q9. Do you read Cookie policies before accepting them?

- Yes
- No

Q10. Do you find Cookie Policies annoying?

- Yes
- No

Q11. Are you aware of 3rd Party Cookies?

- Yes
- No

Q12. Do you know that personalized information is passed on to a third party if you accept the clause in the cookie policy of a site?

- Yes
- No

Q13. Are you aware of the fact that you can monitor and control the cookies through your privacy settings?

- Yes
- No

Q14. Are you concerned about Data privacy?

- Yes
- No

Q15. Do you feel that online providers know too much about you?

- Yes
- No

Appendix B: Consumer Questionnaire

Questions

Responses

144

EU Privacy Directive (Cookie Law) Awareness Questionnaire

Section 1

1. You are being asked to complete the following questionnaire as a consumer of Online content in Ireland in 2021. This questionnaire will take approximately 10-15 minutes of your time. The purpose of this study is to gauge the societal awareness of the recent EU Privacy and Electronic Communication directive in Ireland. The information gained from this study will be used as part of a postgraduate thesis and possible presentation at the Digital West Conference in 2022. Your involvement in this study is completely voluntary. Your response, and all data, will be treated with full confidentiality and all information is completely anonymous. Information will be stored online in a secure password-protected space. You can withdraw from the study at any point before the final submission of this questionnaire and your response will be deleted. Once you submit the questionnaire you will no longer be able to withdraw as your responses will be unidentifiable.

By clicking the button below,

I confirm that I have received an explanation of the nature and purpose of the study and what my involvement will be.

I confirm I am at least 18 years of age.

I understand that my participation is voluntary and that I can decide to opt-out of the research at any time until I submit the final questionnaire and I can do so by exiting the webpage.

I understand that all information gathered about me during this study will be treated with full confidentiality.

- I consent, begin the study.
- I do not consent; I do not wish to participate.

Section 2

Section

2. Do you identify as

Male

Female

3. What age are you at present

18-24

25-34

35-44

45-54

55-64

65+

4. Are you a consumer of online content and Digital media

Yes

No

5. How much time do you spend online per day

<30 Minutes

30-60 Minutes

1-2 Hours

2-3 Hours

3 Hours +

Time Per Day Online

6. How often do you access online content via the following platforms or marketing campaigns?

Please only put one tick, but answer **EVERY** line

Rarely or never One week 2-3 times a week 4-6 times a week 1-2 times a day 3-4 times a day 5+ times a day

Google or similar search engines	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social media (F/B, Insta, Tic/Tok)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Internet Ads	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email marketing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Discussion Forums	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Review Networks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7. Which is the single most important device you use to connect to the Internet at home or elsewhere?

- Smartphone
- Tablet
- Laptop
- Desktop Computer
- Smart TV

8. Which search engine do you use the most to get online?

- Google
- Safari

- Bing
- Baidu
- Yahoo
- Firefox
- Duck Duck Go
- Yandex
- Brave
- Gener8
-
-

9. Are you aware of cookies which can be defined as small pieces of code downloaded onto a device by a browser when someone visits a website?

- Very aware
- Somewhat aware
- Not aware

10. What do you think the main purpose of Cookies are?

- To track user behaviour in some manner or means
- To improve your website experience
- To help the websites to work better

11. Are you aware of the recent EU Privacy and Electronic Communication (e-privacy) directive otherwise known as the EU Cookie Law?

- Very aware

- Somewhat aware
- Not aware

12. Are you aware of the GDPR regulations implemented in 2018 in relation to your personal data and privacy

- Very aware
- Somewhat aware
- Not aware

13. Have you recently noticed an increase in cookie banners in accessing your content?

- Yes, Significant increase
- Yes, Moderate increase
- No very little change

14. Do you think the Cookie Acceptance tools improve your privacy?

- Greatly Improve my privacy
- Moderately Improve my privacy
- Minimally Improve my privacy

15. Do you find Cookie Policies annoying?

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Not at all annoying

Very annoying

16. Do you read Cookie Policies before accepting them?

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Always

Rarely

17. Did you know that personalised information may be passed on to a third party if you accept the clause in the cookie policy of a site?

- Yes
- No
- Maybe

18. Are you aware of the fact that you can monitor and control the cookies through your privacy settings?

- Very aware
- Somewhat aware
- Not aware

19. Are you concerned about your privacy when browsing and buying online?

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Not at all concerned

Very Concerned

20. Do you feel that you are able to effectively protect your data today?

- Yes
- No
- Not Sure

21. If you have answered **no** to the question above which of the following reasons are most relevant?

- If I want the service, I have to accept how my data is being used
- I don't understand my other choices
- I feel my personal data is already available
- I don't know what companies are doing with my data

I don't trust companies to follow their stated policies

22. Do you trust organisations to protect your online data?

Yes

No

Maybe

23. Would you be more likely to trust providers that are fully transparent about how they use your data?

More Likely

Somewhat more likely

Less Likely

24. Do you feel that online providers know too much about you?

Yes

No

25. If saying no to cookies means the website is not as easy to use, or parts of the site didn't work as normal, would you:

Decide to consent to Cookies

Use another website

Continue using the site despite the poorer experience

26. Do you pay more attention to cookie notices from organisations you are not familiar with or do not interact with frequently?

Yes

No

27. Would you consider changing your search engine to some of the providers that prioritize searchers privacy or place a premium on searchers profiles?

Yes

No

Maybe

28. Have you changed your browser preference in the last year due to privacy concerns?

Yes

No

29. If you considered changing your browser provider in light of privacy concerns what search engines would you consider? Please give details below

30. Would you be more likely to consent to being tracked if you were rewarded with discounts or special offers?

More Likely

Somewhat more Likely

Less Likely

31. In light of the Covid19 pandemic would you be more willing to share your data more than you normally would if this data helped in providing information to support public health and safety questions?

- Much more willing
- Somewhat more willing
- No more willing
- Much less willing

32. Given the ongoing pandemic which of the following options do you most support in relation to data privacy as a tool to help deal with the pandemic?

- No privacy laws should be suspended
- A few privacy laws should be suspended for specific exceptions
- Many privacy laws should be suspended but basic protections should be maintained
- All privacy laws should be suspended to protect public health
-

33. Do you feel that Organisations cookie policies are nudging you towards consent?

- Yes
- No
- Not sure

34. Do you feel that cookie policies are purposely made difficult to navigate so as to nudge the user towards accepting?

- Yes
- No
- Not sure

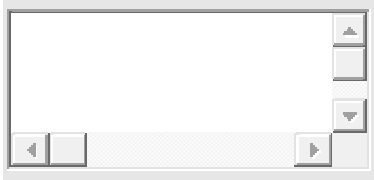
35. Do you feel that Cookie Policies are couched in legalistic language making it difficult to understand?

- Yes
- No
- Not sure

36. Who should have primary responsibility for protecting your data privacy?

- Government
- Internet service providers
- Social media providers
- Individuals
-

37. How can the authorities improve the awareness of laws and regulations governing Cookie use and Online privacy?



Add new

Appendix C: Questions to Business Cohort.

PARTICIPANT INFORMATION LEAFLET FOR RESEARCH PROJECT 2021

Interviews/Focus Groups

I would like to invite you to take part in a research study. Before you decide, you need to understand why the research is being done and what it would involve for you. Please take time to read the following information carefully. Ask questions if anything you read is not clear or if you would like more information. Take time to decide whether or not to take part.

PROPOSED RESEARCH TOPIC /TITLE

A study of the societal awareness and effectiveness of the EU Privacy and Electronic communication directive (EU Cookie law) in Ireland one year after implementation.

WHO I AM AND WHAT THIS STUDY IS ABOUT:

My name is Pat Rowland and I am in the process of preparing a thesis as part of my requirement to submit a dissertation for a Master's in Digital Media and Marketing.

The aim of this analysis is to measure the awareness and effectiveness on a regulatory, business and consumer level of the recent EU Privacy and Electronic Communication (e-privacy) directive (EU Cookie Law), (S.I. No. 336/211) and how this may affect future policy.

Although there is some European research in this field there is limited research in Ireland apart from helpful guidance notes from the Data Protection Commission and numerous Legal publications outlining the requirement to comply and penalties for noncompliance with the directive. The regulators moved to update its guidance in 2020 after identifying widespread failings of compliance during a sweep of websites in 2019. Given the widespread noncompliance we are attempting to gauge awareness of the directive by the various stakeholders.

WHAT WILL TAKING PART INVOLVE?

The main purpose of the research is to determine the societal awareness of the aforementioned E-privacy directive in Ireland and ultimately whether further policy changes are warranted to increase the level of awareness of this important directive.

To do this we intend to gauge the level of awareness and effectiveness of the Directive across three different sub-sets

- The Regulatory framework more specifically the Data Protection Commission

- The Business framework more specifically at an executive level.
- Consumers of Online Content

A comparative case study analysis of the awareness and effectiveness of the implementation of the E-privacy directive (2019) across the three different stakeholder groups will be carried out to gauge the level of awareness of these new regulations across different stakeholders and contexts.

This research will consist of a qualitative research approach with semi structured expert interviews, surveys and possibly a focus group study with some of the industry participants. We have set out below what the interaction with the three subsets will involve.

Business Framework: We hope to conduct interviews with individuals at management level with a minimum of 10 diverse organizations all of whom are active on social media and are involved in Digital marketing Campaigns. There will a broad range of organizations interviewed from retail to wholesale, Sporting Bodies and possibly even some state institutions. Interviews are scheduled to take 30 Minutes approximately, will be recorded if permission is given for same and will be conducted remotely via Microsoft Teams or similar medium.

Regulator: There will interviews with the Regulator's as to their perception of awareness and compliance of the directive. Interviews again are scheduled to take 30 Minutes approximately, will be recoded if permission is given for same and will be conducted remotely via Microsoft Teams or similar medium.

Consumer: We intend to survey up to 20 website users to gauge their awareness of the new legislation. We would hope that this sample group will be a mix of male and female and the respondents will be matched with the statistical data of the profile of users using online content. This consumer group will be contacted via text message or e-mail with a questionnaire with appropriate privacy riders to be filled in which will take around 15 minutes to complete.

Topics for Discussion: Awareness of the privacy Directive, Cookie and Privacy Policies, Effectiveness of legislation, % of consumers managing Cookies, Ways to improve awareness, Alternatives to Cookies, Industry and Consumer attitudes, Trust, Ethics, Ethical Design.

WHY HAVE YOU BEEN INVITED TO TAKE PART?

You have been invited to take part as you fall within one of the three Research Groupings as detailed above and have been selected on the basis that you or your organization has an interest in this study, is a user of online content and/or has given a preliminary indication that you are willing to participate.

DO YOU HAVE TO TAKE PART?

There is no Obligation to participate in this Research Study. Participation is entirely voluntary, and all participants will be asked for consent prior to the commencement of research interviews or surveys.

You can refuse to answer any question or withdraw from the process at any stage prior to publication except in the case of the Consumer survey whereby you will be unable to withdraw once the questionnaire is submitted as your responses will be unidentifiable.

Your response, and all data, will be treated with full confidentiality and transcripts of all interviews and recordings will be anonymised.

WHAT ARE THE POSSIBLE RISKS AND BENEFITS OF TAKING PART?

In any project where there is sensitive data being collected there is a risk that confidentiality and anonymity may be compromised, and we have detailed below how we intend to protect this data and eliminate/mitigate any breaches.

Awareness studies are essential tools in the understanding and evaluation of the success of any legislation and this legislation forms part of the suite of legislation emanating from the GDPR regulations with similar penalties for non-compliance. Both supervisory authorities and courts are now taking action for non-compliance, and it is essential that organizations comply with these regulations and look for alternatives to online behavioural advertising which require consumer consent under the e-privacy directive. This study may help in gauging the awareness of this directive and give suggestions on how to improve awareness and compliance or develop alternatives to the use of cookies.

WILL TAKING PART BE CONFIDENTIAL?

The information collected will solely relate to the awareness of the directive and data privacy policies of the organizations involved consumer behaviour and Regulatory guidelines and may involve evidence of turnover and marketing budgets to give some perspective to the study.

All transcripts and audio recordings will be anonymised in order to protect the organization and individual and to encourage participation.

Given that there are no vulnerable or at-risk persons participating in the research there should be no situation where we have to break confidentiality.

Signed consent forms will be kept until the conclusion of the research but will be stored separately to the interview transcripts or audio recordings which will be assigned pseudonyms to protect the identity of the interviewees.

HOW WILL INFORMATION YOU PROVIDE BE RECORDED, STORED AND PROTECTED?

All the research information signed consent forms and original audio recordings will be securely stored on an encrypted laptop until after the Master's degree has been conferred and the findings from this study have been presented at the Digital West Conference in 2022. The researcher will be the only person with access to this device.

A transcript of interviews in which all identifying information has been removed will be retained in line with the timeframe as outlined above. Under freedom of information legislation, you are entitled to access the information you have provided at any time.

WHAT WILL HAPPEN TO THE RESULTS OF THE STUDY?

This research is solely for the purpose of a research Dissertation and possible presentation at the Digital West Conference 2022, an annual digital media conference in association with GMIT and in academic journals if requested. Permission will be sought from all participants on that basis.

All of the participants can request a copy of the completed study.

WHO SHOULD YOU CONTACT FOR FURTHER INFORMATION? Researcher: Pat Rowland: Pat.Rowland@research.gmit.ie Primary Supervisor: Dr Janine McGinn: Janine.Mcginn@gmit.ie Secondary Supervisor: Dr Eoin Cullina: Eoin.Cullina@gmit.ie

PARTICIPANT CONSENT FORM

By signing and returning this consent form you are indicating your agreement with the following statements:

- I have read and understood the attached Participant Information Leaflet for this study.
- I have had the opportunity to ask questions and discuss the study.
- I have received satisfactory answers to all my questions, where I have had a query.
- I have received enough information about this study.
- I do/do not consent for the interview/focus group will be audio recorded.
- I understand I do not have to answer any of the questions and that I may exit the interview at any time.
- I do/do not wish to be sent a summary of the findings when the project is complete
- I agree to take part in the study.

Participant's Signature: _____

Date:

Participant's Name in Print: _____

Contact Email:

RETURNING THE CONSENT FORM: We would ask you to please return the attached consent form to Pat.Rowland@research.gmit.ie

INTERVIEW SCHEDULE/GUIDE

Interview Questions Document.

Researcher: Mr. Pat Rowland Master of Science Student in Digital Media and Marketing program 2021.

Research Context: A comparative case study analysis of the awareness and effectiveness of the implementation of the E-privacy directive (2019) across three different stakeholder groups. This research will be carried out to gauge the level of awareness of these new regulations across different stakeholders and contexts.

This research will consist of a qualitative research approach with semi structured expert interviews, surveys and possibly a focus group study with some of the industry participants, Regulators and Consumers.

Research Title: A study of the societal awareness and effectiveness of the EU Privacy and Electronic communication directive (EU Cookie law) in Ireland one year after implementation.

Prompts for Researcher

a) Indicate that all responses and all data garnered from this research will be treated with full confidentiality and that all participants will be assured of their anonymity. In the case of recorded interviews, the name of the participant will be stated on the recording, but the recording will be erased once the transcript is written, and each participant will be assigned an encrypted pseudonym.

b) Completion of consent forms.

c) Permission to record the interview and required signature.

d) Approximate duration of the interview (30 minutes)

e) The aim of the interview is to measure the awareness and efficacy on a regulatory/ business/ consumer level of the recent EU Privacy and Electronic Communication (e-privacy) directive (EU Cookie Law), (S.I. No. 336/211) and how this may affect future policy.

In addition, we hope to explore whether any further policy changes are warranted to increase the level of awareness of this important directive and whether consumers are aware of and are taking cognizance of this legislation.

f) Participant information: Name / gender / age bracket / contact information/number of years employed within the organization /Job title; / areas you are responsible for/responsibility for data privacy/regulation.

Sample Questions:

Q1. How aware is your organization with the recent e-privacy directive?

- a. Are you familiar with this recent legislation?
- b. Who in your organization is responsible for its implementation/compliance?
- c. How advanced is your organization in their implementation plans?
- d. How confident are you that you are complying with this directive?
- e. What does successful compliance look like?
- f. How would you rate this legislation in terms of Data Privacy?
- g. Do you see this legislation and the whole privacy discussion as a mere compliance need or do you see any possibilities to use this as a business strategy for growth?

Q2 (a). Explain how committed your organization is to Data Privacy?

Q2 (b). Please give examples of other recent initiatives to improve your Data privacy policy?

Q3. How has the recent EU directive helped you improve your privacy policies?

Q4. How do you perceive this legislation from a consumer privacy standpoint?

Q5. How does this legislation help your customers increase their trust in your organization?

Q6. What % of respondents (consumers) actively manage cookies when visiting your website?

Q7. What impact have these regulations had on your business and privacy policies?

Q8. How has this legislation helped your customers increase their trust in your organization?

Q9. Has the rate of Cookie non acceptance decreased since you first implemented your CMP?

Q10. How aware are you of new browser tracking technologies being developed to replace cookies? Please give examples.

Q11. How can the Regulators keep up with the technological developments?

Q12. How can the awareness of the directive be improved?

Q13. How is your Marketing spending split between Traditional mediums and Digital?

Appendix D: Questions for Regulator.

Question 1.

In 2020 the DPC moved to update its guidance after identifying widespread failings of compliance during a sweep of websites in 2019. Why do you think there was such a low rate of compliance in 2019?

Question 2.

Has the rate of compliance increased since they issued their guidance note in April 2020?

Question 3.

Did they limit their enforcement in light of the Covid Pandemic cognizant of the fact that many businesses were just trying to survive?

Question 4.

In their 2020 Annual report it was stated that during the period of the Cookie sweep Organizations were given a six-month deadline within which to bring their websites and other services using cookies into compliance. During that period the DPC conducted an extensive public awareness campaign in relation to the new, signaling its intention to begin follow-up enforcement action during Q4 of 2020.

4(A) Can you give me details of what was involved in that Public Awareness Campaign?

4(B) How did it compare to the awareness campaign around GDPR in 2018?

4(C) How did the budget for awareness compare to the awareness campaign around GDPR?

4(D) Was the Cookie Sweep the DPC's way of increasing awareness of the directive?

Question 5.

Do you think this awareness campaign was a success, has compliance improved a year on from the guidance?

Note to Question 5.

My research would indicate that awareness amongst consumers of the e-privacy directive is low with 51% of the respondents having no awareness compared to only 13% who have no awareness

of the GDPR regulations. Similarly, only 12% are very aware of the directive as compared to 45% who are very aware of the GDPR regulations.

Per my research interviews with the business cohort all claimed to be aware of the directive yet compliance was low. The results mirror the consumer survey with most companies having minimal awareness of the directive compared to GDPR. Of the 10 interviewees only two were in substantial compliance, the rest all had compliance issues ranging from minor to serious with two respondents having no cookie policy at all. One PLC interviewed as part of the study classified Google analytics as strictly necessary and referred consumers to a Google link showing how to opt out of being tracked by Google Analytics across all websites. Two of the websites had chatbot functions pop up after only strictly necessary functions were selected and in a lot of the interfaces it was unclear whether the consumer was turning on or off the cookies. Two of the websites listed the different type of cookies but gave the consumer no choice to opt out.

Additionally in an interview with a prominent digital marketing company they indicated that only 52% of their clients were in compliance with the directive despite their prompting and partnership with One Trust to provide a solution. Interestingly they cited Covid firstly and awareness secondly as to why these entities were not in compliance,

One leading lawyer in this area when interviewed felt there was such a low level of compliance because people were not aware of it.

The main reason for this she felt was that a lot of businesses outsource the hosting and development of their websites and she felt that a lot of the developers were not as aware as they should be of this directive.

She felt that this gap in the link meant the Business suite were reliant on their hosting providers to comply and she felt that the third-party providers were not as focused as they should be on this. With GDPR a lot of the work was done by HR professionals because it dealt with a lot of personal data, with the e-privacy directive because it dealt with cookies it was left to IT/Online professionals who would maybe not have the same experience in compliance.

She felt that enquires to her office regarding compliance with the directive increased after the Cookie sweep.

Question 6.

Was the awareness campaign directed more at Controllers of websites than the general public, my evidence as set out above is that the awareness of the directive is extremely low amongst consumers compared to GDPR.

Do you think this is a miss given that this is the cohort you are trying to protect?

Question 7.

Would you agree that awareness is an essential tool in the understanding and evaluation of the success of any legislation?

Question 8.

Do you accept, given the evidence above and from your cookie sweep that awareness of this directive is low?

Question 9.

How can awareness of this directive be improved?

Question 10.

Do you think that compliance with this directive is much lower than with the GDPR regulations of 2018?

Question 11.

Can the Regulator's keep up with technological advancements? (Google FLOC, Apple ios14.5 anti ad tracking update)

Question 12.

A lot of the respondents felt that the business cohort were suffering at the expense of the big tech companies who are already moving to block cookies under the pretence of privacy but maybe with a view to monopolizing the use of data themselves. What are your views on this?

Question 13.

Given the wide-ranging compliance issues as detailed above and huge disparity in the clarity of the CMP interfaces do you think it would be helpful to almost standardize the CMP so that compliance becomes easier and clearer.?

Question 14.

Given the widespread acceptance of Cookie policies as set out in the note below do you think this work is futile given that of the companies interviewed only between 5 to 10% of their customers actively managed cookies with an average of over 90% just accepting cookies?

14(A) Do online consumers really care about their privacy?

14(B) Is there an element of Cookie Fatigue which is really diminishing the effectiveness of this directive?

Note to Question 14

Only 43% of the consumers surveyed believed that cookie policies improved their privacy, 42% find cookie policies annoying with almost 70% admitting to not reading cookie policies before accepting them. Despite their stated concerns for privacy and the fact that 50% would consider changing their browser to a more privacy friendly platform; only 6% have actually changed their browser in the last year. Many consumers see Cookie policies as nothing more than an unwanted impediment to the sole purpose of getting online.

Although all our research identifies privacy as a major concern for consumers using these media platforms there is conflicting evidence of how much it actually affects their usage on the Internet. **The Privacy paradox** argues that there is effectively a gap between privacy attitudes and social behavior and that whilst individuals might be concerned about their privacy it does not prevent them sharing their information online without protecting their online behaviour possibly with the purpose of achieving greater benefits from the online transaction.

Question 15.

Have enforcement actions increased since December 2020?

15(A) Are they trying a more consensual approach to try and coax organizations to comply. In your email you indicated that your cookie work has now moved to enforcement, does this mean we will see increased enforcement over the next few months?

Question 16.

Given that the Data protection Commissioner has recently achieved a €4M budget increase for 2022 do you feel that the DPC currently has enough resources to successfully promote and enforce the directive?

16(A) Did lack of resources previously impact on promotion and enforcement?

