GRIFFITH COLLEGE DUBLIN

LLM Dissertation Submission Cover Sheet

Student name:	**Shindy Hor**
Student number:	**3092276**
Dissertation title:	**Protection of Personal Data in Digital Service: Analysing Coerced Consumers' Consent and the relevant Legal Frameworks in the EU**
Supervisor's name:	**Eoin Delap**
Supervisor's signature:	

Plagiarism disclaimer:

I understand that plagiarism is a serious offence and have read and understand the college's policy on plagiarism and that my dissertation will be checked for plagiarism through TURNITIN. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this dissertation, or if I have knowingly allowed others to plagiarise my work in this way.

I hereby certify that this dissertation is my own work, based on my personal study and/or research, and that I have acknowledged all material and sources used in its preparation. I also certify that the dissertation has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.

Signature of student: Shindy Hor **Date:** **14 August 2023**

Note to LLM students: You **MUST** submit TWO HARD-BOUND COPIES + A COPY ON MOODLE. You MUST retain the receipt issued to you as proof of submission.

FOR OFFICE USE ONLY:

No. of copies received (please tick):	2 x hard-bound	
Confirmation from student that soft copy submitted on Moodle:	Yes	
Date:		
Received by:	**Name:**	
	Signature:	

Protection of Personal Data in Digital Service: Analysing Coerced Consumers' Consent and the relevant Legal Frameworks in the EU

Research dissertation presented in partial fulfillment of the requirements for the degree of

LLM in International Commercial Law

(QQI)

Law School, Griffith College Dublin

[Shindy Hor]

[2023]

CANDIDATE DECLARATION

Candidate Name: Shindy Hor

I certify that the dissertation entitled: Protection of Personal Data in Digital Service: Analysing Coerced Consumers' Consent and the relevant Legal Frameworks in the EU

submitted for the degree of: LLM in International Commercial Law

is the result of my own work and that where reference is made to the work of others, due acknowledgment is given.

Candidate signature: *Shindy Hor*

Date: 14 August 2023

Supervisor Name: Eoin Delap

Supervisor signature: 

Date: 14 August 2023

ACKNOWLEDGEMENTS AND DEDICATION

I would like to seise this moment to convey my heartfelt appreciation to the individuals who have played a pivotal role in the successful culmination of this thesis

My deepest appreciation goes to my supervisor, Eoin Delap, whose guidance, insights and invaluable support were pivotal in shaping the trajectory of this study.

I want to give a special thanks to my colleagues and friends for their support, encouragement, and enriching discussions that made my research journey even more meaningful.

I extend deep gratitude to libraries and databases for providing essential resources that greatly contributed to this research. Your dedication to knowledge advancement has been invaluable.

I am profoundly grateful to my parents, Mr and Mrs Hor, for their unwavering love, care, and sacrifices. This journey would not have been possible without your continuous support, guidance, and dedication to educating and preparing me for the future. I also want to express my gratitude to my brother and sister, Sunny and Shirley, for standing by me with their unwavering support.

This research is dedicated to all those who are interested in understanding profound importance of consent, not merely as a legal construct, but as a fundamental pillar of human autonomy, choice, and ethical decision-making. May our collective efforts continue to illuminate the path towards an enlightened, equitable, and ethically conscientious digital future, where the sanctity of consent is honoured and safeguarded in all its dimensions.

TABLE OF CONTENTS

Title page……..……..... ii

Candidate Declaration……..…….…….. iii

Acknowledgements and Dedication…….……... iv

List of Figures……. viii

List of Abbreviations…… ix

Abstract…….. x

Chapter 1: Introduction…….…….... 1

(1.1) Background……. 1

(1.2) Aims of the Research……... 1

(1.3) Methodology……... 2

(1.4) Structural Framework…….. 2

(1.5) Expected Outcome…….. 4

Chapter 2: Concept and Implications of Coerced Consent in Digital Services…… 5

(2.1) Introduction to Consent and its Importance……...……. 5

(2.2) Understanding the concept of coerced consent in the context of digital services…...…… 7

(2.3) The scope of Moral and Legal Aspects of Digital Consent and its Challenges…...……... 9

Conclusion for Chapter 2……...……...… 14

Chapter 3: Legal Framework of Consent in European Union (EU)……...……..….. 15

(3.1) Privacy and Data Protection……...……..… 15

(3.1.1) Overview of General Data Protection Regulation (GDPR)……..…… 17

(3.2) Data subjects' rights in light of consent……...……...…..... 18

(3.3) The definition of Consent under the EU Legal Framework……..…….... 19

(3.3.1) Requirements for valid consent…….…….……. 21

(3.3.2) Informational Roles of Data Controllers in Obtaining Consent from Data Subjects for Various Personal Data Processing Purposes……. 24

(3.3.3) Examples of Data Protection Legislation across EU in regard to consent..... 25

(3.3.4) Understanding of GDPR's Valid Consent by some National Authorities……..... 27

(3.4) Legal Framework of Cookies……...…… 29

(3.4.1) The implementation of e-Privacy Directive……..…..……. 29
(3.4.2) What are Cookies?..... 32
(3.4.3) How consent can be demonstrated through cookies?..... 35
(3.4.4) The validity of Consent pertaining to Cookie Usage in different EU countries….. 39
Conclusion for Chapter 3……..……. 41

Chapter 4: Addressing Coerced Consent and Loopholes in EU Regulations……..…… 43
(4.1) Identifying and Analyzing Coerced Consent Practices in Digital Services……..……... 43
(4.1.1) The Impediments to Personal Autonomy in the Process of Information Collection……. 45
(4.1.2) Lack of Transparency…….……...……...…… 47
(4.1.3) Lack of Choices…….……... 50
(4.2) Assessing the Impact of Dark Patterns on Consent in Digital Services……...… 51
(4.2.1) Cookie banner or Consent Wall…….…….... 53
(4.3) Dark Patterns in Tricky Layouts: Deceptive Design and Privacy Implications……..…. 54
Conclusion for Chapter 4…….…….. 57

Chapter 5: Assessment…… 58
(5.1) Evaluating Consent in the Digital Era: Effectiveness of Regulatory Framework and Privacy Measures……..…….. 58
(5.2) Privacy by Default and Design……...…..…… 61
(5.3) Examining the Proposed e-Privacy Regulation in Addressing Coerced Consent and Identifying Loopholes…….…….…….. 63
(5.4) Is GDPR sufficient to Address Coerced Consent?..... 65
(5.5) Navigating New EU Legislation Addressing Dark Patterns: Challenges and Scope…..…. 67
(5.5.1) Digital Services Act (DSA)…….……. 67
(5.5.2) Digital Markets Act (DMA)……. 68
(5.5.3) Proposal of Data Act…….……...……. 68
(5.5.4) Proposal of AI Act…… 69
Conclusion for Chapter 5……... 70

Chapter 6: Conclusions…….…….. **72**
(6.1) Strengths and Contributions…… 72
(6.2) Limitations and Future Directions……... 73

LIST OF FIGURES

Figure 1: Example of the practice of Dark Pattern……..…….... 54

Figure 2: Example of a Cookie Banner from the official website of Bloomberg…….….. 55

Figure 3: Sneaky Reading Order Manipulation in Consent Banners…….…… 57

Figure 4: Example of a deceptive layout……...……. 58

LIST OF ABBREVIATIONS

AI	**Artificial Intelligence**
CFR	**Charter of the Fundamental Rights**
CJEU	**Court of Justice of the European Union**
CNIL	**Commission Nationale Informatique & Libertés (French DPA)**
DMA	**Data Market Act**
DPA	**Data Protection Authority**
DPC	**Data Protection Commission**
DSA	**Data Services Act**
ECHR	**European Convention on Human Rights**
EDPB	**European Data Protection Board**
EEC	**European Economic Community**
EU	**European Union**
GDPR	**General Data Protection Regulation**
HTTP	**Hypertext Transfer Protocol**
ISP	**Internet Service Providers**
LSO	**Local Shared Objects**
OECD	**Organisation for Economic Co-operation and Development**
WP	**Article 29 Working Party**

ABSTRACT

In the dynamic digital era, consent is a cornerstone of online interactions. This research delves into coerced consent within digital services, examining its ethical and legal dimensions and highlighting challenges. It underscores the importance of informed consent, which can be compromised by intricate technology and manipulative designs like dark patterns. The EU's regulatory framework, notably the GDPR and e-privacy laws, is central. The study assesses their role in privacy and data protection, but acknowledges their potential inadequacy in the ever-growing digital landscape. It also discusses the emerging regulations like the AI Act, Data Act, DSA, and DMA, which are proposed to complement the existing framework. However, due to their recent introduction and pending implementation, their immediate impact on coercion and dark patterns remains uncertain.

Addressing coerced consent, the research highlights issues curbing user autonomy, transparency, and choices within the EU's regulatory scope. The study underscores the importance of adaptable regulatory frameworks while noting that dark patterns raise legal concerns due to their potential violation of regulations. The research significantly contributes to data privacy and consent discussions by critically examining coerced consent's complexity. It blends legal analysis with socio-legal insights, offering a comprehensive perspective. While robust, the study acknowledges that the impact of new regulations depends on their eventual enactment. It identifies avenues for future exploration and the potential implications of coerced consent in specific digital contexts such as social media.

In essence, this research navigates the intricate terrain of coerced consent within digital services, highlighting ethical, legal, and practical dimensions. It underscores the need for transparent consent practices and adaptable regulatory frameworks to preserve users' rights amid the dynamic digital evolution.

Keywords: coerced consent, data privacy, digital services, EU regulatory framework, dark patterns.

INTRODUCTION

In today's digital age, our interactions with a plethora of online services and platforms are intricately intertwined with the concept of consent. Consent serves as the cornerstone of our legal system, embodying the principles of autonomy, choice, and ethical decision-making. As we navigate the dynamic landscape of digital services, the significance of obtaining valid and informed consent becomes paramount, yet the complexities surrounding this fundamental concept are often overlooked. This research endeavours to delve into the multifaceted dimensions of coerced consent within digital services, critically examining its ethical and legal implications, and shedding light on the challenges it poses.

Background

The exponential growth of digital technologies has revolutionised how we engage with various aspects of our lives, from e-commerce to social media, necessitating an in-depth exploration of the consent mechanisms that underpin these interactions. While consent is hailed as a protective shield for individual rights and data privacy, the digital realm presents unique challenges that demand thorough scrutiny. The intertwining of digital services with our daily lives has given rise to complex issues such as restricted choices, manipulation, and a lack of awareness – all of which can dilute the very essence of consent. Furthermore, the emergence of deceptive practices like dark patterns raises concerns about the validity of the consent obtained. Throughout this research, the terms "user," "data subject," and "consumer" will be used interchangeably.

Aims of the Research

This research comprises four primary objectives, each of which will be addressed in its dedicated chapter.

The first objective of this research is to thoroughly examine coerced consent within digital services, delving into its ethical and legal dimensions. This objective involves exploring various types of consent in the digital context, while also addressing the challenges associated with manipulation and the constraints of limited choices.

The second objective entails a comprehensive exploration of the European Union's legal structure for consent, with a particular emphasis on privacy and data protection. This objective entails analysing the General Data Protection Regulation (GDPR), defining criteria for valid consent, and examining the legal aspects of cookies, including the application of the e-Privacy Directive and the validity of consent across different nations.

The third objective is to assess the impact of coerced consent practices and dark patterns on data subjects' autonomy and privacy rights within the framework of EU data protection regulations. This objective involves examining challenges in obtaining authentic consent, with a focus on transparency and ethical considerations in data processing.

The last objective aims to assess the efficacy of regulatory frameworks, privacy measures, and pertinent legislations, such as the GDPR, proposed e-Privacy Regulation, DSA, DMA, Data Act, and AI Act, in tackling challenges related to coerced consent and dark patterns in the digital era. The research will provide a comprehensive analysis of the dynamic data privacy landscape and regulatory reactions, along with identifying potential gaps in these strategies.

Methodology

This research employs a blend of predominantly doctrinal analysis, involving an extensive review of legal literature, regulations, case law, and policy documents related to consent, data protection, and privacy. This analysis aims to establish a comprehensive grasp of the legal frameworks governing consent within the digital landscape. Additionally, a socio-legal approach will be integrated, intertwining the doctrinal analysis with an exploration of the societal, ethical, and practical consequences of consent. This entails examining real-world cases, user experiences, and the broader impact of consent-related practices on individuals and society.

Structural Framework

This research is organised into four comprehensive chapters, each addressing distinct facets of the intricate landscape surrounding coerced consent within digital services and the European Union's regulatory framework. The structural framework is designed to provide a systematic exploration

of consent's ethical, legal, and practical dimensions, as well as the efficacy of existing regulations in safeguarding data subjects' rights.

Chapter 2: Concept and Implications of Coerced Consent in Digital Services

This introductory chapter lays the foundation by elucidating the vital role of consent in our legal system and its extension to the digital realm. It delves into the nuances of coerced consent within the digital context, examining challenges posed by manipulation and limited choices. Additionally, it explores the moral and legal aspects of digital consent, paving the way for a comprehensive understanding of the complexities ahead.

Chapter 3: Legal Framework of Consent in European Union (EU)

The third chapter undertakes a deep dive into the EU's legal framework for consent, particularly focusing on privacy and data protection. It provides an overview of the GDPR, delves into data subjects' rights in relation to consent, and comprehensively defines the requirements for valid consent under the EU framework. The chapter also examines the legal framework governing cookies, offering insights into the implementation of the e-Privacy Directive and the validity of consent across different EU nations. Real-world case studies will be explored to illustrate the intricate challenges of securing informed consent in the digital landscape.

Chapter 4: Addressing Coerced Consent and Loopholes in EU Regulations

In this chapter, the focus shifts to addressing coerced consent practices and challenges arising within EU regulations. The examination encompasses identifying and analysing practices that impede personal autonomy during information collection, lack transparency, and limit choices for data subjects. Furthermore, the chapter assesses the impact of dark patterns on consent in digital services, highlighting deceptive designs and privacy implications.

Chapter 5: Assessment

The fifth chapter undertakes a comprehensive assessment of the regulatory measures and privacy frameworks in place to combat coerced consent and dark patterns. It evaluates the effectiveness of existing regulations, explores the implications of the proposed e-Privacy Regulation, and examines the relevance of GDPR in addressing these issues. Additionally, it navigates through new EU legislations – Digital Services Act (DSA), Digital Markets Act (DMA), Data Act, and Artificial

Intelligence (AI) Act – to identify their contributions and potential challenges in addressing coerced consent and deceptive practices.

Chapter 6: Conclusion

The research culminates with an overarching conclusion that synthesises the findings from the preceding chapters. It offers a comprehensive perspective on the effectiveness of regulatory measures, the significance of consent, and the challenges posed by coerced consent practices in the digital landscape. The conclusion also highlights potential areas for further research and underscores the importance of adapting regulatory frameworks to protect data subjects' rights and autonomy in the digital era.

Expected Outcome

By amalgamating rigorous legal analysis with socio-legal insights, this research endeavours to untangle the intricate web of coerced consent within digital services. Through the attainment of the stipulated objectives, this study seeks to make a valuable addition to the ongoing dialogue concerning data privacy, consent, and the efficacy of regulations. Importantly, considering the persistent existence of coerced consent practices, this research highlights the need for continued improvement in regulatory frameworks. Ultimately, the aim is to cultivate a deeper comprehension of how consent functions within the digital realm and to advocate for the evolution of regulatory mechanisms to ensure robust safeguarding of individual rights in the ever-evolving landscape of digital interactions.

CHAPTER 2: CONCEPT AND IMPLICATIONS OF COERCED CONSENT IN DIGITAL SERVICES

(2.1) Introduction to Consent and its Importance

A number of requirements must be satisfied for consent to be considered legitimate, which is a challenging matter that calls for cautious handling. Consent is the procedure by which A authorises B to conduct C.[1] Consent is granted when an individual who possesses the mental ability to make an ethical judgment and righteous choice regarding the matter at hand, voluntarily agrees to it. Consent becomes invalid and considered as an act of coercion if it is acquired from an individual who lacks the capability or accountability to make sound and accountable decision.[2]

Consent is a fundamental element of our legal system and holds significant importance. It is not surprising considering our society highly values a person's freedom of choice in various aspects of our lives, such as being consumers, employees or citizens. The core cultural ideas of choice and autonomy are strengthened through consent.[3] Consent is often applied as a legal notion in the realm of digital products and services. Our interactions with search engines, electronic commerce (e-commerce) and social media sites and numerous other digitally facilitated firms are established through the foundation of consent. Privacy policies, terms and conditions of service, the utilisation of tracking cookies, and a plethora of other commercial practices are usually subject to our approval.[4]

Richards and Hartzog as well as other privacy law academics have observed and recorded in other works the consent frameworks which are widely used in the digital service field. However, in reality, the practice of such frameworks falls well short of the ideal which is known as the "gold standard" of consent.[5] To put it simply, both parties have deliberately and freely chosen to fulfil the agreed legal duties under a contract. Consider the contracts you have in relation to e-commerce

---

[1] Stephen Breen, Karim Ouazzane and Preeti Patel, 'GDPR: Is your consent valid?' (2020) 37(1) Business Information Review < https://doi.org/10.1177/0266382120903254 > accessed 13 June 2023.
[2] Franklin Miller and Alan Wertheimer, *The Ethics of Consent: Theory and Practice* (Oxford University Press 2009) 12.
[3] Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (2019) 96 Washington University Law Review < https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview > accessed 13 June 2023.
[4] Neil Richards and Woodrow Hartzog, 'Privacy's Trust Gap' (2017) 126 The Yale Law Journal < https://ssrn.com/abstract=2899760 > accessed 8 August 2023.
[5] Ibid.

or any social media websites and the mobile apps downloaded in mobile devices. What about artificial intelligence virtual assistants such as Apple's Siri and Amazon's Alexa that could be monitoring and recording your private conversation. Do consumers or data subjects aware and fully understand the terms of their agreements?[6]

Although the concept of consent originated in centuries-old Roman contract law, it has subsequently spread to other branches of law.[7] Privacy and data protection are regarded as fundamental rights by the EU, valuing consent while being cautious about relying solely on it in their approach.[8] This perspective holds substantial influence on the existing EU privacy and data protection regulations. Even internationally, the importance of consent as a fundamental component of data protection is acknowledged.[9] The data protection framework in EU has traditionally viewed consent as a legitimate legal foundation that, when appropriately employed, can validate the processing of personal data.[10]

A consent is considered as an informed consent and commonly defined as informational self-determination which holds that every individual has the right to decide for themselves to what degree information about them is shared with other individuals. In the realm of a digital-based services, businesses often need the individuals to provide consent before sharing or releasing of

[6] Woodrow Hartzog, 'The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?' (2010) 15(4) Communication Law and Policy < https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4539&context=faculty_scholarship > accessed 8 August 2023.

[7] Riikka Koulu, *Dispute Resolution and Technology: Revisiting the Justification of Conflict Management* (COMI 2016) 257 and 259 in Alexandra From, 'Cookie Consents and Notices under the EU Data Protection Framework' (Master's Thesis, University of Helsinki 2020) < https://helda.helsinki.fi/bitstream/handle/10138/317229/From_Alexandra_Thesis_2020.pdf?sequence=3&isAllowed=y > accessed 21 June 2023.

[8] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28(1) Information & Communications Technology Law < https://ssrn.com/abstract=3254511 > accessed 8 August 2023.

[9] Frederik Zuiderveen Borgesius, 'Informed Consent: We Can Do Better to Defend Privacy' (2015) 13 IEEE Security Privacy 103 in Alexandra From, 'Cookie Consents and Notices under the EU Data Protection Framework' (Master's Thesis, University of Helsinki 2020) < https://helda.helsinki.fi/bitstream/handle/10138/317229/From_Alexandra_Thesis_2020.pdf?sequence=3&isAllowed=y > accessed 21 June 2023.

[10] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent', (adopted on 13 July 2011) 01197/11/EN WP 187 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf > accessed 8 August 2023.

their private information. Although all conditions for informed consent might be met, the consent may not necessarily hold validity due to ethical or legal concern.[11]

(2.2) Understanding the concept of coerced consent in the context of digital services

Richard Thaler, an American economist laid down three categories of consent such as coerced consent, unwitting consent and last but not least the incapacitated consent.[12]

A coerced consent is where you have no choice but to provide your consent under duress to assess certain services. Coercion could also happen where individuals are being manipulated. Richard and Hartzog states that consumers at times do not have genuine options for instance, when it comes to Internet Service Providers (ISPs), since these businesses frequently monopolised the supply of broadband services. Opting not to use it essentially means choosing not to have home Internet access.[13]

Data subjects have little options when it comes to particular platform-layer services. The fact that Facebook (now known as Meta) owns websites like Instagram further limits the options available to people who are concerned about data practices. Now, Facebook regularly dominates as the primary or sole option for social networking to communicate with friends and family. Therefore, the key drive of this research is to sheds light on the issue with such restricted choices for majority of customers to provide consent or not in the digital world.[14]

This is particularly applicable in cases involving the existence of monopoly control or a similar circumstance. The capacity of businesses to affect how consumers' make the decisions through interface design, is just as important as their market power in determining the degree of coercion that people encounter. As a consequence, there are "dark patterns," as user experience designer Harry Brignull described them. Brignull defines dark patterns as deceptive tactics employed in websites and apps to manipulate data subjects into making unintended purchases or sign-ups.[15] The concept of dark patterns will be examined in Chapter 4.

---

[11] Alan F Westin, 'Privacy and Freedom' (1968) 25(1) Washington and Lee Law Review 166.
[12] Richards and Hartzog (n 3).
[13] Ibid.
[14] Ibid.
[15] Dr Harry Brignull, Deceptive Patterns < https://www.deceptive.design/ > accessed 4 July 2023.

Unwitting or unintentional consent occurs when consumers are unaware of the data risks, procedures, and agreements involved in a transaction, often due to the complex digital landscape. This can lead to them providing consent without a clear understanding of data collection purposes, influenced by busy schedules or distractions. Additionally, clicking "I agree" to terms of service and privacy policies legally binds individuals to contracts.[16]

Incapacitated consent pertains to situations where legal consent is unattainable, as in cases of minors or those inherently unable to provide consent. Ignoring legally incapacitated children's consent can lead to severe financial or physical harm. Notably, companies like Apple and Facebook have faced criticism for allowing minors to use parent's credit cards for in-app purchases, while the United Kingdom (UK) government investigated dating apps like Tinder and Grindr due to reports of minors bypassing age restrictions, leading to cases of child rape.[17] Since this research is on the analysis of coerced consent, the remaining two aspects of consent will not be discussed in details.

In today's society, digital technologies mediate our lives through services exchanged for data. Data subjects provide consent by agreeing to privacy policies and terms of service, but this often falls short of meeting ethical standards for meaningful consent. Consent holds moral significance, transforming interactions by legitimising activities that may otherwise be illegal.[18]

Consent plays a crucial role in various aspects of our lives. It allows for consensual sexual intercourse, medical procedures, and exchange of personal data. These behaviours may escalate into major crimes including sexual assault, bodily harm and breach of privacy if they are done without consent. Data subjects are given notice of how their information is gathered and utilised, and they are given the option to proceed with sharing the information or decline. This system provides the basis for consent for data transfer. In the digital realm, what constitutes valid consent and its appropriate boundaries? When data subjects grant permission for the handling and

[16] Woodrow Hartzog, 'Website Design as Contract'(2011) 60(6) American University Law Review < https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1617&context=aulr&httpsredir=1&referer= > accessed 4 July 2023.
[17] Ibid.
[18] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Bloomsbury Publishing 2007) in Elizabeth Edenberg and Meg Leta Jones, 'Analyzing the legal roots and moral core of digital consent' (2019) 21(8) New Media and Society < https://journals.sagepub.com/doi/pdf/10.1177/1461444819831321 > accessed 27 June 2023.

processing of our personal data, what exactly are they authorising? How can we guarantee that consent in digital transactions has ethically evolving effects?[19]

The term digital consent is used as the concept of consent in the context of computing encompassing the obtaining, analysing, utilisation and exchange of confidential data. Consent has evolved as a crucial component in international privacy issues and cross-border technological advancement, despite the fact that data protection regulations have differed in their approaches to it.[20] Consent is frequently regarded as the principal means of safeguarding data subjects' authority over their personal information. Data subjects' authority in managing their personal information is usually considered as being best protected through consent. However, the effectiveness of consent in preserving individual privacy has faced significant scrutiny.[21] Many studies and analyses on consent question the feasibility of consent as a viable solution or aim to enhance current procedures.[22]

(2.3) The scope of Moral and Legal Aspects of Digital Consent and its Challenges

There are two distinctive interpretations of consent, according to writers Faden and Beauchamp, that need highlighting. First of all, consent is a moral idea that includes the intended exchange of rights and responsibilities through effective inter-party communication. Therefore, consent reshapes the moral ground between individuals, legitimising activities that would have been considered unlawful. Secondly, consent has been codified into legal frameworks. The extent of consent may have legal validity and binding effect if certain legal conditions or organisational guidelines controlling it are satisfied. The moral concept of consent serves as the foundation for

[19] Ibid.
[20] Elizabeth Edenberg and Meg Leta Jones, 'Analyzing the legal roots and moral core of digital consent' (2019) 21(8) New Media and Society < https://journals.sagepub.com/doi/pdf/10.1177/1461444819831321 > accessed 27 June 2023.
[21] Solon Barocas and Helen Nissenbaum, 'Big Data's End Run Around Procedural Privacy Protections' (2014) 57(11) Communications of the ACM 31 – 33 in Edenberg and Jones (n 20).
[22] Lorrie Faith Cranor, 'Necessary but not sufficient: Standardized mechanisms for privacy notice and choice' (2012) 10(2) Journal on Telecommunications and High Technology Law < http://www.jthtl.org/content/articles/V10I2/JTHTLv10i2_Cranor.PDF > accessed 27 June 2023.

the legal concept. Nonetheless, issues occur when legally binding consent misses the opportunity to reflect the morally valid exchange of rights and responsibilities.[23]

The legal framework surrounding consent has evolved differently across countries and regions. Examining the emergence, growth, and conflicts around digital consent in international law is vital to figuring out if these distinctions can be ethically justified. This can be done by exploring a few European countries and their legal frameworks to examine how consent is used to authorise processing of personal data,[24] which will be discussed further in Chapter 3.

Contrary to the legal theory, consent in the moral term serves to alter the relationship between both individuals. The remarkable aspect of consent is its capacity to make actions that would typically be considered unethical or unlawful acceptable and legitimate.[25] Consent from an individual, in a widest definition entails a clear and deliberate exchange of rights and responsibilities communicated effectively between the persons involved.[26] When a consenter provides legitimate consent to the recipient, a consentee regarding a specific activity, their unique relationship changes. Although there is a connection between the moral and legal notions of consent, issues might occur once the legally enforceable consent misses the opportunity to reflect the appropriate morally acceptable transfer of rights and duties.[27]

At the heart of digital consent lies its moral essence. In this context, five essential elements that define consent as a moral notion will be laid out. Firstly, establishing specific conditions regarding acceptable and unacceptable data utilisation. Secondly, providing pertinent details necessary for the consentee. Thirdly, ensuring freedom to select from a range of feasible choices. Next, a clear specification of the range of actions involved. Lastly, ensuring fair treatment of the consenter without compromising other fundamental rights.[28] To provide a comprehensive understanding of when consent is necessary or not, the underlying conditions have to be delineated to establish the

[23] Ruth R Faden and Tom L Beauchamp, *A History and Theory of Informed Consent* (Oxford University Press 1986) 274 – 297.
[24] Alan Reed and Michael Bohlander (eds), *Consent: Domestic and Comparative Perspectives* (Routledge 2017) in Edenberg and Jones (n 20).
[25] Heidi M Hurd, 'The moral magic of consent' (1996) 2(2) Legal Theory 121 - 146 in Edenberg and Jones (n 20).
[26] Miller and Wertheimer (n 2) 79 – 105.
[27] Edenberg and Jones (n 20).
[28] Ibid.

bigger picture. The subsequent four aspects outline the parameters and specifications of the consent transaction, however, they all depend on a thorough comprehension of the larger context.

In the realm of digital consent, it is essential to establish a distinct demarcation of the conditions under which the gathering, storage, utilising and dissemination of personal data may be permitted or not. This is the first aspect which is the "importance of clear background conditions". Regrettably, the state of affairs right now does not fully satisfy this need. Despite our society's careful consideration of the appropriate terms for disclosing personal information in exchange for digital services, the principles and assumptions ingrained in the technology itself frequently become the default norm as a result of the rapid integration of technology into our daily lives.[29]

People constantly believe they have little control over the terms of service provided by the digital services we use every day. A significant number of individuals were not mindful of the degree to which digital enterprises that offered consumers free of charge services where their personal data were obtained, processed and shared.[30] It is therefore, essential to elucidates the meaning of consent as a moral concept to understand the expectations of the society pertaining to the gathering, processing and disclosure of personal data.[31]

There are debates among theorists as to what exactly qualifies as purposeful and effective communication of the passing on of rights when it comes to consent. Tom Beauchamp contends that ethically transformative consent requires total autonomy. According to him, consent is only morally transformative when a person consciously gives permission to another person to carry out a specific action while having a good grasp of the situation and being free from considerable outside influence.[32] On the other hand, Miller and Wertheimer contend that requesting autonomous permission is overly burdensome and overly dependent on the person giving consent. They propose for a consideration of the circumstances whereby a consent transaction takes place. They contend that if the person seeking permission has treated the consenter fairly and the consenter expresses their symbol of consent, then the act of consent is morally transforming.[33]

---

[29] PEW Research Center, 'The State of Privacy in Post-Snowden America', (2016) < https://www.pewresearch.org/short-reads/2016/09/21/the-state-of-privacy-in-america/ > accessed 29 June 2023.
[30] Ibid.
[31] Edenberg and Jones (n 20).
[32] Tom Beauchamp, *Autonomy and consent* (2009) in Franklin Miller and Alan Wertheimer, *The Ethics of Consent: Theory and Practice* (Oxford University Press 2009) 55 – 78.
[33] Miller and Wertheimer (n 2) 94.

In spite of the major instances where theorists disagree over what makes consent ethically transformative, philosophers do agree on a number of important points. Ethical philosophy may provide direction to the convoluted international legal system of consent in this overlap. These fundamental moral principles may have their roots in various moral systems, all of which offer a different explanation as to why consent is morally necessary as per theorist, John Rawls. While it is crucial to establish the moral essence of consent, it is advisable to embrace diverse theoretical perspectives that elucidate the essence of consent and offer practical insights on its optimal implementation.[34]

The other aspects of consent shall be discussed. The second aspect which can also be known as the "voluntariness" aspect where individuals should have the freedom to select from a range of feasible choices. Coercion, deception or a lack to comprehend what the transaction entails weaken the moral power of consent, according to practically all theories of consent. It must be offered without expectation for consent to exert its moral power which means the consent given must be free from coercion, deception or manipulation.[35]

The third aspect of consent is "knowledge". For consent to be valid, individuals must be in possession of the essential knowledge and have a thorough grasp of that knowledge in for them to be able to agree in an informed manner. Each party must be aware of the pertinent facts in order to comprehend what the person has agreed to disclose and how that information will be used. Only then will the parties be able to agree on the parameters of the permission provided by consent.[36]

By eroding the fundamental understanding of the circumstance needed for morally legitimate exchange of rights, deception and various types of manipulation may weaken the moral significance of consent. In light of this awareness requirement, the consent provided by a minor could not be regarded as a valid consent ethically, morally or legally unless they have shown a certain level of knowledge and understanding relevant to the specific context and consent transaction. The proposed consent transaction must be understood enough by both parties for the

[34] John Rawls, *Political Liberalism* (Columbia University Press 2005) in Edenberg and Jones (n 20).
[35] Larry Alexander, 'The ontology of consent. Analytic Philosophy' (2014) Legal Studies Research Paper 14/137 1-12.
[36] Keith Hyams, 'When Consent Doesn't Work: A Rights-Based Case for Limits to Consent's Capacity to Legitimise' (2011) 8(1) Journals of Moral Philosophy 110-138.

agreement to be enforceable, and both parties must exhibit epistemic competence in connection to it. Accurate information about the proposed consent transaction must also be provided.[37]

The fourth aspect of consent is the "scope". Individuals ought to possess a clear grasp of the rights they have transferred to a different entity and a shared understanding of the parameters of the authorisation they have been provided before making any valid transfer of rights.[38] These calls into question the notion that individuals may provide their permission to the gathering and use of their personal data for any purpose. This notion is often included in existing conditions of service.[39]

The last aspect is "fairness" where a fair environment is necessary for the consent transaction so that individuals may decide how and under what conditions they are ready to trade private data. In order to protect an effective system of democracy, it is vital for individuals to have critical conversations as a society about the legal uses of personal information that serve significant societal benefits. A fair system where people have the option to decide whether to participate in additional data sharing must also be ensured and individuals need to determine the necessary measures to do that.[40]

The moral framework presented here offers a common foundation for determining whether various nations' legal systems adhere to high moral norms. Defining the moral essence of digital consent establishes a shared normative benchmark and allows for acceptable variations within its boundaries. By referring to a universal moral core of digital consent, we can assess the normative effectiveness of different legal reasoning and standards. A philosophical strategy rooted in fundamental human rights and privacy interests leads us to establish an international structure for digital consent.[41]

[37] Beauchamp in Miller and Wertheimer (n 2).
[38] Tom Dougherty, 'Yes Means Yes: Consent as Communication' (2011) 43(3) Philosophy and Public Affairs < https://philpapers.org/archive/DOUYMY.pdf > accessed 8 August 2023.
[39] Neil C Manson, 'Permissive consent: a robust reason-changing account' (2016) Philosophical Studies: An International Journal for Philosophy in the Analytic Tradition 1-18.
[40] Miller and Wertheimer (n 2) 79 - 105.
[41] Rawls (n 34).

CONCLUSION FOR CHAPTER 2

In conclusion, the concept of consent in digital services is complex and has significant implications for ethical and legal boundaries in handling personal data. Current practices often fall short of ideal meaningful and informed consent, with issues of coerced consent arising due to monopoly power and manipulative tactics. Understanding consent's moral and legal aspects is crucial for evaluating its validity, emphasising freedom, knowledge, and fairness. Establishing a common understanding of consent's moral essence can guide ethical exchange between individuals and inform international digital consent frameworks that respect human rights. Addressing coerced consent highlights the need for improved practices and regulations to ensure genuine, informed, and voluntary consent, promoting an ethical digital landscape.

As we transition to the next chapter, we will delve into the legal intricacies surrounding the concept of consent. This exploration will provide a comprehensive understanding of the legal foundations that underpin consent within the digital realm, further enriching our perspective on this crucial topic.

CHAPTER 3: LEGAL FRAMEWORK OF CONSENT IN EUROPEAN UNION (EU)

(3.1) Privacy and Data Protection

The notion of having control over one's information, also known as informational self-determination, is widely used to illustrate the concept of informed consent in relation to privacy and personal data. A brief explanation of privacy and personal data protection concepts would be helpful in discussing the boundaries of consent concerning the privacy and protection of personal information.[42] It is acknowledged in several international and regional treaties that privacy is a basic human right with global relevance.[43] The capacity of a person or group of people to safeguard their private affairs, including their personal information, is known as privacy. The inputs to this discussion examine the fundamental rights that are profoundly affected by digitisation. Particularly crucial in this context are the rights to privacy and data protection as per Articles 7 and 8 of the Charter of the Fundamental Rights (CFR)[44] and right to a private life under Article 8 of European Convention on Human Rights (ECHR).[45] [46]

Maja Brkan shows in her piece for this special edition how the collecting of enormous quantities of personal data for the sake of targeted advertising and profiling puts fundamental rights in jeopardy. Brkan contends that although data protection tools are essential, they are insufficient to stop unethical behaviour in online political advertising. Since it provides efficient enforcement tools, data protection often takes centre stage in the EU when it comes to reducing risks associated with the digital transition. As it offers strong enforcement tools, data protection plays a significant role in reducing risks related to the digital revolution at the EU level. Merely relying on data protection laws may not suffice if other fundamental rights are also compromised in the process.[47]

---

[42] Bart Custers (eds) 'Consent and Privacy' (2019) < https://ssrn.com/abstract=3383465 > accessed 7 July 2023.
[43] Edward J Bloustein and Nathaniel J Pallone, *Individual and Group Privacy* (Routledge 2017) 194.
[44] Charter of Fundamental Rights of the European Union, [2000] OJ C364/1.
[45] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).
[46] Orla Lynskey, 'Deconstructing data protection: The ''added-value'' of a right to data protection in the EU legal order', (2014) 63(3) International and Comparative Law Quarterly, < http://eprints.lse.ac.uk/57713/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Lynskey%2C%20O_Lynskey_Deconstructing_data_protection_2014_Lynskey_Deconstructing_data_protection_2014.pdf > accessed 7 July 2023.
[47] Maja Brkan, Monica Claes and Clara Rauchegger, 'European fundamental rights and digitalization' (2020) 27(6) Maastricht Journal of European and Comparative Law < https://doi.org/10.1177/1023263X20983778 > accessed 7 July 2023.

The tension between privacy and national security often arises in situations of combating terrorism, where regulations like anti-terrorism laws can prioritise security over explicit consent for accessing and using personal data, primarily in the public sector. However, private entities rely on consent as the legal basis for processing personal information.[48] It is worth noting that this research will not be focusing on the specific issue of cybercrime or terrorism but rather on the broader implications of consent within digital services.

The first legally binding agreement that recognises the protection of people with regard to the automated storage and use of their personal data is Convention 108 by Council of Europe.[49] The ECHR includes the processing of personal data under Article 8. The right of people to have their personal information respected, including their home address and communications, is guaranteed under this article. There are, however, limitations to this right that are permitted by law and supported by factors such as for the purpose of defending the security of nation, combating crime, protecting individuals' liberties and rights as well as preserving morality.[50]

Privacy and personal information are clearly defined legal concepts. As a fundamental right acknowledged by the EU, the right to of personal data protection is widely acknowledged. The 1995 Directive includes provisions safeguarding this right. It has now been replaced by the General Data Protection Regulation (GDPR)[51] and it demonstrates a more explicit and cautious approach towards addressing the need for individual control over personal data as compared to its predecessor. Indeed, the EU legislator aimed to enhance individual control over personal data, as clearly stated in the paper's policy recommendations leading up to the GDPR proposal and reflected within the text of the GDPR.[52]

---

[48] Ibid.
[49] Council of Europe Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108.
[50] Dolores-Fuensanta Martínez-Martínez, 'Unification of Personal Data Protection in the European Union: Challenges and Implications' (2018) 27(1) El profesional de la información < http://www.elprofesionaldelainformacion.com/contenidos/2018/ene/17_esp.pdf > accessed 8 July 2023.
[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119/1.
[52] Viviane Reding, Vice President of the European Commission and EU Justice Commissioner, 'Your data, your rights: Safeguarding your privacy in a connected world' (Speech at the World Privacy Platform "The review of the EU data protection framework", Brussels, 16 March 2011) < https://europa.eu/rapid/press-release_SPEECH-11-183_en.pdf > accessed 8 July 2023.

In line with globalisation, technical improvements, and the Union's stage of growth of the digital economy, the GDPR provides a comprehensive framework. Additionally, it ensures the legal protection that individuals seek when their personal data is processed. The Regulation marks a key legal turning point in the area of privacy and personal data protection, denoting a considerable change in emphasis towards the development of a true culture of privacy and personal data protection.[53]

(3.1.1) Overview of GDPR

The European Commission continuously refused to implement data protection provisions into Community law throughout the seventies and eighties, despite numerous requests from the European Parliament. Subsequently, it said that Convention 108[54] was the suitable piece of legislation and urged Member States to sign and enforce it, arguing that this was a basic rights matter that was beyond of its purview.[55]

In 1995, the European Economic Community (EEC) succumbed under the strain of national data protection bodies operating as trans-governmental enterprises and implemented a Data Protection Directive.[56] This directive was formulated under Article 100A of the Treaty establishing the European Community to harmonise national provisions that impact the internal market. As a result, data protection legislation has been incorporated into Community Law and EU has emerged as one of the most prominent promoters for the establishment of regulations pertaining to data protection.[57]

In 2009, the European Commission began publicising its plans to revise the data protection legislation then in place and proposed for a Regulation 2016/679/UE or widely known as the GDPR, in 2012. It became effective in the EU six years later. The GDPR continues the legacy of the 1995 Directive, with many definitions and principles remaining the same[58] and it strengthens

[53] Martínez (n 50).
[54] Council of Europe Convention 108 (n 49).
[55] Burkard Eberlein and Abraham Newman, 'Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union' (2008) 21(1) < https://doi.org/10.1111/j.1468-0491.2007.00384.x > accessed 8 August 2023.
[56] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L281/31.
[57] Julien Rossi, 'Data Protection and Right to Privacy. Investigating the Contested Notion of "Personal Data"' (PhD thesis, Université de Technologie de Compiègne 2020) < http://julienrossi.com/these/Julien%20Rossi%20-%20PhD%20Summary%20FINAL.pdf > accessed 26 June 2023.
[58] Ibid.

the legal certainty by modernising and improving the Directive. It establishes strong enforcement as a community rule and legitimate European legislation.[59]

(3.2) Data subjects' rights in light of consent

As mentioned above, the processing of personal data is permitted under Article 8(2) of the CFR provided certain conditions are met. According to this, the processing of personal data must be fair and for specific objectives, either with the data subject's consent or another legitimate legal basis.[60]

Data protection as a fundamental right involves individual control over personal data, but relying solely on control has limitations, especially when considering consent's role.[61] Despite critiques, the notion of data protection through control persists, as noted by Woodrow Hartzog. Consent aims to enable self-determined data handling, yet overestimating individual capacity can harm data practices and regulatory effectiveness.[62]

According to Article 6 of the GDPR, enterprises in the digital economy rely on the consent of data subjects for data processing. However, Article 8 of the CFR protects decision-making autonomy and aims for true consensus. Consent may not be sufficient for self-determination due to unbalanced power relations. The GDPR's consent requirements, in line with Article 8 of the CFR, are strengthened by the possibility that dominant social networks may erode contractual autonomy.[63]

Legislative primacy ends with open norms, leading courts to assume responsibility. The Court of Justice of the European Union (CJEU)'s active role is evident in the Google Spain ruling,[64] deriving criteria from Articles 7 and 8 CFR to shape the legal system. The court's establishment of the "right to be forgotten" intervenes in ongoing legislation. While akin to a high court in

[59] Martinez (n 50).
[60] Charter of Fundamental Rights of the European Union, [2000] OJ C364/1.
[61] Jorn Reinhardt, 'Realizing the Fundamental Right to Data Protection in a Digitized Society' in Marion Albers and Ingo Wolfgang Sarlet (eds), *Personality and Data Protection Rights on the Internet* (Springer 2022) 63.
[62] Woodrow Hartzog, 'The Case Against Idealising Control' (2018) 4 European Data Protection Law Review 425 < https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4050&context=faculty_scholarship > accessed 8 August 2023.
[63] Jorn Reinhardt, 'Realizing the Fundamental Right to Data Protection in a Digitized Society' in Marion Albers and Ingo Wolfgang Sarlet (eds), *Personality and Data Protection Rights on the Internet* (Springer 2022) 64.
[64] Case C-131/12 *Google Spain v Agencia Española de Protección de Datos and Mario Costeja González* [2014] ECR I-317.

addressing systemic concerns, it must meet fundamental requirements, accounting for the complexity of fundamental rights.

(3.3) The definition of Consent under the EU Legal Framework

Consent is often seen as only being legitimate when it is informed consent in regard to the principles of privacy and data protection. Giving people thorough information about the particulars of their permission and making sure they are aware of the possible repercussions of doing so are essential components of informed consent.[65] When it comes to protection of the rights and liberties of the data subject, is crucial to ensure the lawfulness of your processing activities as a primary requirement. Gaining consent is a fundamental aspect of adhering to GDPR regulations. Although consent is the simplest legal basis for processing personal data, it is also prone to withdrawal by data subjects and poses a higher risk of legal repercussions for data controllers.[66] In the English case of ***Gillick***,[67] the court established that having the capacity to consent means having enough understanding and intelligence to make an independent decision regarding a matter, along with the ability to comprehend the proposed information and communicate one's own desires effectively.[68]

Since Article 8(2) of the CFR specifically mentions consent as a legal basis for processing personal data, it is considered to be crucial under EU data protection legislation. Consent should accurately represent a person's real intentions, taking into consideration their capacity for decision-making, hence autonomy is essential to getting consent. Whether a person is able to make a wise decision must be taken into account. Consent has been a complex notion in legal contexts for many years, encompassing more than a mere "yes." Despite variations in the concept across different legal systems and areas of law, there has been a consistent recognition that consent should be both voluntary and informed, whether in the domains of consumer contract law or medical law.[69]

---

[65] Bart Custers (eds) 'Consent and Privacy' (2019) < https://ssrn.com/abstract=3383465 > accessed 7 July 2023.
[66] IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide* (4th edn, ITGP 2020) 121.
[67] *Gillick v West Norfolk and Wisbech Area Health Authority* [1986] AC 112 (HL) (UK).
[68] Simone Van der Hof, 'I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2017) 34(2) Winsconsin International Law Journal < https://wilj.law.wisc.edu/wp-content/uploads/sites/1270/2017/12/van-der-Hof_Final.pdf > accessed 14 July 2023.
[69] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Bloomsbury Publishing 2007) 7 -9.

The GDPR enforces stricter consent requirements from data subjects than the Data Protection Directive, offers stronger protection for children, and imposes more stringent rules for processing special categories of personal data, necessitating entities to review their consent practices for GDPR compliance. Consent as per Article 4(11) of the GDPR, refers to the voluntarily expressed or freely given preferences of an individual that are specific or explicit, informed, and unambiguous. It must be granted by a statement or affirmative action indicating acceptance to the use of their personal data.[70]

According to Article 7(1) of the GDPR, the data controller is obliged to provide evidence demonstrating that the data subject has given consent for their personal data to be processed. The responsibility lies with the data controller to bear the burden of proof and they have to determine an appropriate method to prove that consent does not require additional data collection. Once the process of the activity of processing is over, the data controller is obligated to prove consent for the duration of that processing and it is not legally required to comply with legal responsibilities.[71]

It is the data controller's responsibility to establish whether it is a genuine and legitimate consent. Article 7(2) states that consent should be requested explicitly and independently when a data subject consents as part of a written statement that includes many topics. It needs to be simple to comprehend, accessible, and written in straightforward terms. The declaration will not be enforceable if any element of it is in violation of the GDPR.[72]

As per Article 7(3), data subject is able to change their minds at any time about the processing of personal data or known as the right to withdrawal and must be made aware of their right to withdraw permission before providing it, and the procedure for doing so should be as simple as giving it in the first place. If the supply of a service or the performance of a contract depends on obtaining agreement for the processing of personal data that is not necessary for upholding the contract's terms, extra attention should be paid to this while assessing the freedom of consent as stated under Article 7(4).[73]

---

[70] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (Springer 2017) 93.
[71] European Data Protection Board (EDPB), 'Guidelines 05/2020 on consent under Regulation 2016/679' (Adopted on 4 May 2020) < https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf > accessed 10 July 2023.
[72] Ibid.
[73] Ibid.

(3.3.1) Requirements for valid consent

i) *Freely Given Consent*

In order to guarantee that the data subject's choice to provide consent was made of their own free will, freely given consent is a sort of consent that is gained without coercion. It highlights the value of having the power to exercise one's rights and liberties. This idea acknowledges that an individual's consent should not be swayed by outside forces that compromise their autonomy. Therefore, the data controller must ensure that the data subject genuinely has the choice to refuse and that there will be no consequences for doing so when consent is requested.[74]

ii) *Specific consent*

Additionally, consent has to be explicit, indicating that the precise objectives of the processing must be outlined. A personal data request from an insurance firm to assess risk can be an example of explicit consent. The data subject must be informed of the purposes for processing, the methods used to accomplish those purposes, and whether or not a third party will be handling their data.[75] In certain situations, specific consent is not always needed. For instance, when an online retailer collects a customer's personal information to process a purchase, it falls under data processing for contractual fulfilment. Consent is only required for creating the customer's account, while informing them about other lawful data processing activities necessary for order fulfilment is still important.[76]

In the case of ***Deutsche Telekom AG***,[77] the CJEU observed that where a data subject has been promptly notified on the processing of their personal data for a particular data processing operation, it is not necessary to get a new consent, even in the event of a change in the data controller. Nevertheless, the latest instance of ***Planet49***,[78] the CJEU reinforced the need for consent to be

[74] Article 29 Data Protection Working Party (n 10).
[75] Breen, Ouazzane and Patel (n 1).
[76] EDPB (n 71).
[77] Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland* [2011] ECR I-3441.
[78] Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019] ECR I-801.

explicit and emphasised that it must pertain directly to the processing of the relevant data, without any room for inference or assumption about other objectives.[79]

iii) *Informed consent*

Ensuring that consent is both informed and specific are closely interconnected. It is essential to provide sufficient information to data subjects so that they can make an informed decision and give their consent. As the data controller, it is their responsibility to ensure that the information is transparent and easily understandable, particularly when utilising personal data for commercial purposes.[80]

iv) *Unambiguous consent*

Consent in data processing should be unambiguous where it indicates a clear and explicit approval from the data subject. Typically, written consent forms are provided and the data subject simply needs to confirm their understanding and approval. It is crucial that the written consent is not misleading and clearly states that the data subject is granting consent for the specific processing activities. As true consent requires a clear and affirmative act, pre-selected options or opt-ins cannot be regarded as valid consent.[81] A privacy policy or terms and conditions form that only has a checkbox for acceptance is problematic because it does not guarantee that the data subject has read or understood the policy and unaware of its consequences.[82]

A plain affirming statement must be used to communicate consent. Data subject has to be affirmative as opposed to anything that is accomplished by means of inactivity or silence. It emphasises the need for an active and deliberate act of consent from the data subject. The active selection of a check box in a pop-up window that asks the data subject to confirm their consent is an illustration of affirmative action for obtaining consent. The data subject must actively take the required action to give consent to this action. Additionally, the use of ambiguous language, where

[79] Sara Rasilainen, 'Valid Consent and Purpose Limitation Principle under the Eu General Data Protection Regulation' (Bachelor's Thesis, Tallinn University of Technology 2020) < https://digikogu.taltech.ee/en/Download/2c0349ba-4011-4b52-9ff0-3ab92736474d > accessed 10 July 2023.
[80] Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' 17/EN WP260 < https://ec.europa.eu/newsroom/article29/items/622227/en > accessed 8 August 2023.
[81] EDPB (n 71).
[82] IT Governance Privacy Team (n 66) 124-125.

data subjects are asked to uncheck a box in order for their personal data not to be processed would likely be against the Regulation due to its failure to adhere to the necessary standards.[83]

v) *Withdrawal of consent*

If data subjects opt to withdraw their consent, the entity responsible for data control must either halt the processing of their personal information or identify alternative legal grounds for the processing. The ability for data subjects to revoke their consent is essential for their consent to be considered genuinely voluntary, as stated in Article 7(3) and Recital 42. If individuals are unable to freely and knowingly choose to withdraw their consent, it cannot be seen as willingly given. Additionally, throughout the entirety of the processing procedure, the data controller must be capable of demonstrating both the presence of consent and the option for individuals to freely withdraw that consent.[84]

If the data subject lacks the ability to revoke consent, the data controller is logically unable to fulfill their obligation of demonstrating consent for any subsequent processing, rendering future processing no longer discretionary. The criteria for the usability of withdrawing consent also exists, which specifies that withdrawing consent should be as simple as granting it. As a result, when consent is given electronically, such as by clicking a mouse on a computer, the data subject must be able to withdraw it with the same simplicity.[85]

Moreover, as emphasised in Recital 42 of the GDPR, the individual whose data is being processed should not experience detriment when revoking consent. In ***Meta Platforms Inc. v. Bundeskartellamt***,[86] the latest legal development pertaining to consent validity in GDPR. Initially centered on Facebook's dominant market position in a competition law context, the German competition authority placed limitations on Facebook's data processing without consent under the GDPR. Facebook appealed, but the CJEU had recently delivered the judgment which sided with the authority, stating that data subjects' consent must be obtained for lawful data processing. The

[83] EDPB (n 71).
[84] IT Governance Privacy Team (n 66) 125.
[85] Gabbi Meskenaite, 'An examination of the criteria for valid consent under the GDPR in the light of the rationale and technological neutrality' (Master's Thesis, Lund University 2022) < https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9096679&fileOId=9099573 > accessed 10 July 2023.
[86] Case C-252/2 Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 22 April 2021 - *Meta Platforms Inc.and Others v Bundeskartellamt* [2021] OJ C320/16 < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CN0252 > accessed 8 August 2023.

authority also highlighted an imbalance of power in data subjects' consent due to Facebook's dominance, implying that consent might result from coercion. The CJEU clarified that a dominant social network position should not invalidate data subjects' consent. Data subjects should retain the freedom to refuse non-essential data processing without losing service access, aligning with the Recital 42.[87]

(3.3.2) Informational Roles of Data Controllers in Obtaining Consent from Data Subjects for Various Personal Data Processing Purposes

To establish the consumer's understanding of multiple purposes of personal data processing, the data controller must demonstrate that the data subject actively gave consent, received clear and easily accessible information in plain language about the processing which allows them to comprehend the consequences fully.[88]

This follows the CJEU's decision in the ***Orange Romania*** case.[89] To prevent any ambiguity in defining the goals of data being kept and processed, it is the data controller's duty to seek clear and unambiguous permission from the data subjects. Particularly when data is processed based on consent, the data controller is responsible for demonstrating genuine consent.[90] In a case involving Orange Romania, sales representatives failed to inform clients about data collection goals prior to gaining consent, resulting in creditor rights enforcement.[91]

The Bucharest Court sought CJEU clarification on valid consumer consent conditions. CJEU confirmed that lawful data processing requires freely given, informed, and unambiguous consent under Article 4 of the GDPR.[92] While some personal information verification for contract formation is acceptable, obtaining consent for copying and storing identification documents is

[87] Case C-252/21 *Meta Platforms and Others v Bundeskartellamt* [2023] ECR I-537.
[88] Juanita Goicovici, 'Granularity and Specificity of Consent and Implications Thereof for the Data Controller in the Light of the Principle of 'Purpose Limitation'' (2022) 9(2) InterEULawEast < https://hrcak.srce.hr/file/424613 > accessed 22 July 2023.
[89] Case C-61/19 *Orange Romania SA v Autoritatea Naţionala de Supraveghere a Prelucrarii Datelor cu Caracter Personal* [2020] ECR I-901.
[90] Goicovici (n 88).
[91] Elena Kaiser, 'The Concept of 'Freely Given, Specific and Informed' Consent under the Scrutiny of the European Court of Justice' (2020) 6(4) European Data Protection Law Review 607.
[92] Court of Justice of the European Union, 'Press Release No 137/20 Judgment in Case C-61/19 *Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării* Datelor cu Caracter Personal (ANSPDCP)' (11 November 2020) < https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-11/cp200137en.pdf > accessed 22 July 2023.

unwarranted.[93] Orange Romania's pre-selected checkbox did not imply active consent, thus, the process for obtaining consent was coercive and its explanations about data processing were insufficient. Despite client refusals, Orange Romania proceeded with contracts, failing to demonstrate valid consent under Article 7(1) of the GDPR.[94]

(3.3.3) Examples of Data Protection Legislation across EU in regard to consent

In 1978, France enacted its initial data protection legislation, which can be seen as a law governing algorithms due to its content and scope. According to the first guiding principle, information technology ought not to undermine an individual's freedom or integrity. The second principle asserts that any decision with significant legal or consequential implications cannot be made solely through automated information processing, without involvement or oversight by a judicial body. The third principle affirms individuals' entitlement to be informed about and contest automated decision that affect them. An explicit "agreement" is required under Section 31(1) of the 1978 Act[95] in order to retain in computer memory any personal information pertaining to sensitive data such as philosophical, ethnic backgrounds, political views or religious associations.[96]

The UK was relatively slow in enacting privacy legislation, passing its Data Protection Act in 1984.[97] However, early investigations and legislative discussions, which mostly addressed privacy in the private sector, had a crucial influence in creating the worldwide privacy discourse.[98] The legislation incorporated consent in a fragmented manner, specifying specific disclosure protocols for household and payroll processing, among other settings. Consent was mandated for obtaining additional disclosures, the same as in the other specified nations.[99]

The first nation to incorporate consent as a core component of its data protection legislation concerning computing was Germany. In order to specify the responsibilities and authority of different governmental levels and departments with regard to certain data banks and equipment,

---

[93] Tom de Cordier and Thomas Dubuisson, 'EU Court of Justice clarifies concept of "informed consent" for collection of personal data' (*Lexology*, 17 November 2020) < https://www.lexology.com/library/detail.aspx?g=6cf3217e-e687-4b5d-97f0-d2107e6ff7e7 > accessed 23 July 2023.
[94] Kaiser (n 91) 608-609.
[95] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. (France).
[96] Edenberg and Jones (n 20).
[97] Data Protection Act 1984 (UK).
[98] Mark Littman and Peter Carter-Ruck, *Privacy and the Law* (Stevens and Sons Limited 1970).
[99] Edenberg and Jones (n 20).

the first data protection law was passed in 1970. The Federal Data Protection Act of 1977[100] established consent as the primary and consistent means of legalising data processing, applicable to both public and commercial sectors. Processing personal information is legitimately permitted only if it complies with a specific legislation or obtained consent.[101]

Apart from Germany, early data protection regulations tended to place more emphasis on consistency, transparency and limits on automated processing in Europe than they did on consent or human control. In most cases, consent was only brought up when it involved a party other than the one in charge of data gathering, storing or processing. The relevance of consent in technology regulations from the seventies to the late eighties was mostly unimportant outside of Germany. Consent is not given top priority in international data privacy recommendations by Council of Europe's Convention 108 and the Organisation for Economic Co-operation and Development (OECD). Concerned about a possible economic collapse caused by data protection legislation of different countries across the European Community, the European Parliament encouraged the European Commission to address the problem of data subjects' protection in 1990.[102]

As mentioned above, the Directive was implemented five years later with the aim of protecting data subjects' rights to data protection. Despite efforts to comply with the Directive, there were notable variations in the national laws enacted. The Directive defines consent as the voluntary, precise, and informed indication of a person's preferences for the use of their personal data. While the majority of nations adopted the Directive's language on consent without modification, there were variations in some countries, Germany required "clearly distinguishable" approval for different purposes and Italy mandated written consent. Explicit and unambiguous consent in Luxembourg and only unambiguous consent was needed in Spain and Sweden. Both the UK and France omitted an explicit definition of consent, with the France including it into general standards for legitimate processing and UK relying on implied consent.[103]

[100] Federal Data Protection Act 1977 (Bundesdatenschutzgesetz, BDSG) (Germany).
[101] Edenberg and Jones (n 20).
[102] Ibid.
[103] Ibid.

(3.3.4) Understanding of GDPR's Valid Consent by some National Authorities

i) *Guerin Media Prosecuted by Irish Data Protection Commission (DPC) for Unsolicited Marketing Emails without Consent*

The DPC received complaints regarding Guerin Media Limited sending unsolicited commercial emails to people's work email accounts without their consent. There was no way to opt out of the emails. Guerin Media Limited was punished for 42 violations of the e-Privacy Regulations 2011 (S.I. 336/2011),[104] despite past warnings and comparable complaints. The firm was fined €4,000 after entering a guilty plea to four sample offences. As the material was unrelated to the recipients' responsibilities, the misunderstanding that consent is not required for business-to-business communications was disproved. To prevent violations, organisations should evaluate the exceptions to the regulations governing consent for electronic marketing and implement opt-out options.[105]

ii) *Spanish Data Protection Authority (DPA)'s Ruling on Invalid Consent Due to Double Denial*

A patient complained to the Spanish DPA about a hospital, claiming that an unfilled tick on a form and a statement concerning data sharing resulted in invalid consent in 2019. The DPA decided against the hospital in February 2020, stating that the form's double denial approach resulted in passive consent, violating GDPR's requirement for clear affirmative action. This case contrasts with a Danish decision discussed below, emphasising the necessity of affirmative and unambiguous action for valid consent.[106]

iii) *Investigation by Danish DPA: Cookie Consent Challenges and GDPR Compliance*

An investigation about the Danish Meteorological Institute (DMI)'s website's integration of third-party plugins from Google's ad network that stored cookies without proper authorisation was received by the Danish DPA in August 2018. Before user involvement, the first cookie banner

[104] European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, S.I. No. 336/2011.
[105] 'Data Protection Commission welcomes latest successful prosecution of Marketing Offences' (Data Protection Commission, 5 December 2022) < https://www.dataprotection.ie/en/news-media/data-protection-commission-welcomes-latest-successful-prosecution-of-marketing-offences#:~:text=Guerin%20Media%20Limited%20pleaded%20guilty,Statutory%20Instrument%20336%20of%202011 > accessed 7 August 2023.
[106] *Agencia Española de Protección de Datos, Procedimiento* PS/00187/2019, 25 February 2020 in Meskenaite (n 84).

merely included a 'OK' button, storing cookies.[107] The website's cookie consent setup, where personal information of data subjects was collected by cookies and shared with Google Ad Services for targeted advertising, was said to have broken GDPR transparency and lawfulness by the complainant, an expert in ad-tech concerns. Since its founding as a publisher in 2004, DMI has made money off of its website while promising to fix any unethical behaviour discovered.[108]

The banner featured "OK" and "Show details" choices after changes, however choosing not to accept required selecting pre-ticked checkboxes after clicking for more information. The DPA rejected the Institute's appeal in February 2020, noting the lack of detail and precision in the consent procedure and the failure to address "specific" or "unambiguous" criteria. Notably, pre-ticked boxes were not taken into account, which illustrates the difficulty in interpreting consent laws.[109] The authority emphasised the need for "informed consent," stating that individuals should be clearly informed about the data controller's identity and processing objectives. In critiquing a specific consent solution, the authority pointed out a deficiency in disclosing joint data controllers, such as Google. The Danish regulator's approach seems stricter than the CJEU's, focusing on transparency and perhaps fair design elements in consent notices.[110]

Understanding the realm of cookies within digital services and their regulatory framework is crucial to gaining insight into how consent is practiced and its potential implications, including the risk of coercion. Cookies play a fundamental role in data collection and processing, often influencing user experiences and targeted advertising. By comprehending the legal requirements surrounding cookie usage and consent, stakeholders can evaluate whether consent is obtained genuinely or if there is a possibility of coercion or undue influence. This understanding helps safeguard data subjects' privacy rights and ensures that consent practices align with ethical and legal standards in the digital landscape.

[107] Datatilsynet, 2018-32-0357, *DMI's behandling af personoplysninger om hjemmesidebesøgende*, 11 February 2020 in Meskenaite (n 85).
[108] Natalija Bitiukova, 'Danish DPA zooms in on the cookie consent banner design and peeks into the ePrivacy and GDPR relationship' (*LinkedIn*, 18 February 2020) < https://www.linkedin.com/pulse/danish-dpa-zooms-cookie-consent-banner-design-peeks-bitiukova > accessed 7 August 2023.
[109] Datatilsynet (n 107).
[110] Bitiukova (n 108).

(3.4) Legal Framework of Cookies

(3.4.1) The implementation of e-Privacy Directive[111]

The 1995 Directive was complemented by the e-Privacy Directive, which was enacted in 2002. It also known as the cookie law. It protects the privacy of digital communications made over public networks, including those made through more conventional means of communication like telephones. Cookies are within the scope of the e-Privacy Directive, whether or not the information they contain is deemed personal data. The idea that gadgets used by data subjects and the data they store are seen to be a part of their private sphere and should be protected is reaffirmed in Recital 24. The e-Privacy Directive and the GDPR must both be adhered to by a corporation if it processes personal data by means of cookies.[112]

In accordance with the 2002 e-Privacy Directive, member states were required to limit the use of electronic networks for archiving, surveillance, tapping and access to communication and web browsing. The data controller has to provide data subjects the option to object to such processing while also providing them with transparent and detailed explanation.[113]

The collection, storage and use of personal data and the protection of privacy in the electronic communications industry were controlled by Article 5(3) of the e-Privacy Directive, which applied to the handling of cookies. The e-Privacy Directive required no consent for the use of cookies to handle data prior to its 2009 revision. Article 5(3), on the other hand, permits the use of cookies as long as data subjects are notified of the procedure and have the option to decline cookie insertion and storage.[114] Under the previous regime, storing cookies was permitted only if data subjects were given clear and comprehensive information about the processing purposes and provided the right to refuse. The clause was changed to expressly state that after being notified of the processing

[111] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L201/37.
[112] Jos Dumortier, 'Evaluation and Review of the ePrivacy Directive (2016) 2(2) European Data Protection Law Review 247.
[113] Ibid 249.
[114] Christina Markou, 'Behavioural Advertising and the New "EU Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination' in Serge Gutwirth, Ronald Leenes and Paul De Hert, *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016) 214.

purposes, data subjects must grant their consent prior to the using and storing of cookies on their gadgets.[115]

This approach followed an informed opt-out model for cookies. By changing the notice and consent requirements from an informed opt-out strategy to an informed opt-in strategy, the 2009 Directive revised Article 5(3) of the e-Privacy Directive.[116] As a result of the substantial modification made to this clause, lawmakers enhanced user protection significantly. The usage of cookies is permitted only when data subjects have explicitly granted consent after receiving concise and thorough reasoning and details about the purpose of data monitoring. The exception to this rule is limited to essential cookies. The granting of consent to cookies by data subjects may be indicated by using the proper browser or other programme settings, in accordance with Recital 66 of the 2009 Directive.[117]

The 2009 e-Privacy Directive[118] mandates that member states make sure that information is only stored or accessed on a data subject's device with their explicit agreement upon receipt of full disclosure of the grounds for processing as specified in the 1995 Directive. Technical storage or access is allowed notwithstanding the need for consent for the user-requested information society benefit or for the sole purpose of message delivery.[119] The Commission affirmed that the e-Privacy laws will be reviewed after the implementation of the GDPR and the adoption of the Digital Single Market strategy, both of which have been implemented and adopted to date.[120]

In accordance with Article 3 of the ePrivacy Directive, the processing of personal data associated with the provision of electronic communications services on publicly accessible networks inside the European Community is covered by the Directive. The scope of the Directive encompasses services that primarily involve the transmission of signals rather than content

[115] Alexandra From, 'Cookie Consents and Notices under the EU Data Protection Framework' (Master's Thesis, University of Helsinki 2020) < https://helda.helsinki.fi/bitstream/handle/10138/317229/From_Alexandra_Thesis_2020.pdf?sequence=3&isAllowed=y > accessed 16 July 2023.
[116] Edenberg and Jones (n 20).
[117] Markou (n 114) 216.
[118] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11.
[119] Edenberg and Jones (n 20).
[120] Dumortier (n 112).

provision. Depending on whether they are categorised as digital interaction services, information society services, the advancement of technology might result in the emergence of functionally comparable services that fall under several legal regimes such as webmail and Internet protocol-enabled services.[121]

Exceptions under e-Privacy Directive

Exemptions from the cookie consent requirement are outlined in Article 5(3) of the ePrivacy Directive. These exceptions include cookies used solely for delivering an expressly requested internet-based service by the subscriber or user as well as cookies absolutely essential for the technical function of communication transmission. The amended e-Privacy Directive 2009, also known as the 'Citizens' Rights Directive', emphasises that cookie consent and notice are not required when the technical storage or access of cookies is strictly necessary for enabling the use of a specific service explicitly requested by the subscriber or user, as stated in Recital 66.[122]

Websites are only needed to request consent for cookies that are unimportant and not required for the delivery of online services, according to the ePrivacy Directive. The website may still operate and deliver its services without these cookies, even if accepting them could have extra advantages for the website operator.[123] The Working Party (WP) identified certain cookies, such as authentication session cookies, user interface customisation cookies and first-party user-input session cookies, as exempt from consent requirements. The WP emphasised the need for data subjects' consent for third party cookies, targeted advertisement and tracking cookies, while also acknowledging that first-party cookies for anonymised statistical purposes may be excluded from cookie consent requirements.[124]

[121] Dumortier (n 112) 248.
[122] Article 29 Data Protection Working Party, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (Adopted on 2 October 2013) 1676/13/EN WP 208 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf > accessed 8 August 2023.
[123] From (n 115).
[124] Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption' (Adopted on 7 June 2012)00879/12/EN WP 194 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf > accessed 24 July 2023.

(3.4.2) What are Cookies?

There is not much research devoted to the study of web cookies despite the significant influence they have on our web browsing experience. Cookies are often described as straightforward text files that websites send and keep on users' computers in the majority of extant research and papers, which are mostly written by computer technicians and engineers.[125] A cookie may be viewed as a tiny file that a web server keeps in a local browser directory from a larger viewpoint. They refer to cookies as a kind of memory or refers to as a "state".[126]

According to technical definitions, a cookie is a mechanism that allows a server to provide data and related information to a data subject and the same server will preserve those data. Cookies transformed the web by providing it with memory, recording past activities and granting them a historical context that often goes unnoticed by data subjects. Viewing cookies as purely technical has obscured their broader significance, prompting a need to re-evaluate our understanding.[127]

Cookies have the capacity to acquire a variety kind of data about the data subjects, such as the advertising they have clicked, the sites they have seen and any other characteristics that the website thinks pertinent to learn about the data subjects. Additionally, cookies are used to keep track of things like language choices, goods in the shopping cart, and other actions or choices that users or visitors do while on a web page. Therefore, cookies may be used to create e-commerce consumer profiles with the goal of displaying personalised advertisements online.[128] As mentioned by Clifford, tracking has become a crucial part of the business models for numerous Web 2.0 services, leading to the development of user profiles as a result. Website service providers depend on targeted advertising as a source of income, enabling them to provide consumers online services in return for their personal information rather than cash payments.[129]

---

[125] Elinor Carmi, 'Review: Cookies – More than Meets the Eye' (2017) 34(7-8) Theory, Culture and Society < https://doi.org/10.1177/0263276417736367 > accessed 16 July 2023.
[126] Riccardo Andrea Junior Varisco, 'Cookies in the European Data Protection Framework' (Master's Thesis, University of Oslo 2018) < https://www.duo.uio.no/bitstream/handle/10852/67266/Thesis-Completed.pdf?sequence=1&isAllowed=y > accessed 16 July 2023.
[127] Ibid.
[128] Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (adopted on 21 November 2000) 5063/00/EN/FINAL WP 37 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf > accessed 16 July 2023.
[129] Damian Clifford, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster -

Types of cookies

There are many different kinds of cookies, some of which are defined by their shelf life. "Session cookies" are transient files that disappear when a person closes their browser. In comparison to permanent cookies, they are less obtrusive.[130] Persistent cookies, tracking cookies and session cookies are the three main categories under which cookies may be divided. However, owing to its unique qualities in comparison to the others, a new category of local storage cookies will be mentioned for this research.[131]

Anonymous tracking cookies, distinct from regular Hypertext Transfer Protocol (HTTP) cookies, are persistent cookies employed for analytics, retaining data about website visits, user behaviour, and settings even after the browser is closed. They serve various purposes such as login functionality and online chat support, containing session and authentication information for the website's server.[132]

Local Shared Objects (LSO) often known as Flash Cookies are data pieces stored by websites using Adobe Flash software, functioning like persistent cookies to store preferences and track users even after a session has ended. In contrast to web browser cookies, local storage cookies are produced and set by the browser for particular purposes, enabling websites to store data independently. Other function-specific cookies are also included in browsers, however unlike browser cookies, Flash cookies are proprietary and not saved in the browser.[133]

Flash cookies encompass Zombie cookies (or ever cookies) and Super Cookies. Zombie cookies persistently track users across various storage locations. Super cookies are sizable, long-lasting, and challenging to remove, stored in hidden directories, making them undetectable by browsers, and remaining effective across different browsers.[134]

Tracking the Crumbs of Online User Behaviour' (2014) 5 JIPITEC < https://www.jipitec.eu/issues/jipitec-5-3-2014/4095 > accessed 16 July 2023.

[130] From (n 115).

[131] Chinmay Khandekar, 'Cookie Security and its Implementation in the Light of GD-PR and E-Privacy Regulation' (Master's Thesis Tallinn University of Technology 2019) < https://digikogu.taltech.ee/en/Download/aaccb661-fa99-4c2b-9ecd-04f9df4c4a18 > accessed 17 July 2023.

[132] Ibid.

[133] 'What is a Flash Cookies?' (*CookiePro*, 2 June 2020) < https://www.cookiepro.com/knowledge/what-is-a-flash-cookie/ > accessed 8 August 2023.

[134] Khandekar (n 131).

In contrast, persistent cookies remain stored on the user's device until their predetermined expiration date, which can range from minutes to several years. However, retaining cookies for an extended duration, particularly multiple years, may be seen as excessively lengthy. Persistent cookies retain the actions and preferences of data subjects within a site or across multiple websites, making them more invasive. The WP's Cookie Sweep Combined Analysis report in 2015 revealed that the surveyed websites predominantly employed persistent cookies over session cookies, with approximately 86% being persistent cookies and 14% session cookies.[135]

First-party and third-party cookies may be distinguished depending on their domain. The website itself stores and accesses first-party cookies, which are often used for functional reasons including recording user preferences like login information or language settings.[136] As opposed to first-party cookies, third-party cookies are set by a third party, which has contracts with several websites to advertise. The third party is generally an advertising network firm.[137] According to the findings of the Cookie Sweep Combined Analysis report, approximately 70% of the cookies utilised by the 478 surveyed websites were classified as third-party cookies. The poll finds that website owners often use privacy-invasive cookies, suggesting possible weaknesses in cookie-related data protection legislation.[138]

The WP acknowledges that rejecting all cookies would not be helpful for data subjects, acknowledges that although cookies might be obtrusive, they also have important value.[139] The internet sites that install the cookie for data subjects when they browse those web pages are the only one with access to it and can read its contents, despite the fact that cookies may store a lot of user-related information as a result of their distinctive identifiers.[140] The GDPR and e-Privacy Directive did not explicitly outline formal consent requirements but view written form as convenient for the controller's burden of proof. While most member states follow a generic opt-

[135] Article 29 Data Protection Working Party, 'Cookie Sweep Combined Analysis - Report' (Adopted on 3 February 2015) 14/EN WP 229 < https://ec.europa.eu/newsroom/article29/items/640605 > accessed 16 July 2023.
[136] Damian Clifford, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the Crumbs of Online User Behaviour' (2014) 5 JIPITEC < https://www.jipitec.eu/issues/jipitec-5-3-2014/4095 > accessed 16 July 2023.
[137] Markou (n 114).
[138] Ibid.
[139] Article 29 Data Protection Working Party (n 128).
[140] Article 29 Data Protection Working Party, 'Cookie Sweep Combined Analysis - Report' (Adopted on 3 February 2015) 14/EN WP 229 < https://ec.europa.eu/newsroom/article29/items/640605 > accessed 17 July 2023.

out approach, a few, such as Netherlands, Italy, Croatia and Germany, follow an opt-in consent method.[141]

Under GDPR and the e-Privacy Directive, consent requires data subjects to make unambiguous affirmative decisions, including checking or unchecking boxes or modifying technical cookie settings. Consent is not implied by inaction, pre-ticked boxes or silence. Unless it is in the context of cookies that are exempt from consent, the opt-out approach is typically not permitted. According to the WP, consent must include specific information about the cookie's purpose, third-party access, retention period, and technical details. The website can use a "layered approach" to display this information. Data subjects should be informed about how to accept or reject cookies and how to change their preferences later. Consent for cookies should be obtained before any processing begins, meaning websites must ensure no cookies are set until the user has given their consent or signalled their preferences for non-exempt cookies.[142]

Consent must be unambiguous, clearly indicating the data subject's intentions through an active and understandable choice. It should also be freely given, without any deception, coercion, or negative consequences. While access to specific website content may be conditional on accepting cookies for legitimate purposes, general access should not be restricted as per recital 25 of e-Privacy Directive. Data protection rules apply when information is stored or accessed, involving personal data processing.[143]

(3.4.3) How consent can be demonstrated through cookies?

The e-Privacy Directive's Recital 17 permits a variety of consent-getting techniques as long as they provide a freely given, precise, and informed statement of the data subjects' desires.[144] The use of browser settings is one of these techniques but it was criticised by the WP for being too permissive and vulnerable to Flash cookies.[145]

The WP recommended rejecting third-party cookies by default, which should be explicitly accepted by data subjects.[146] Additionally, browser settings alone do not suffice; providing clear

[141] Varisco (n 126).
[142] Ibid.
[143] Ibid.
[144] Article 29 Data Protection Working Party (n 122).
[145] Article 29 Data Protection Working Party (n 124).
[146] Ibid.

information about cookie purposes is crucial. Although the "privacy wizard" proposal for guiding data subjects through privacy configuration aligns with privacy by design, it has not been fully implemented in major browsers like Firefox, Chrome, or Internet Explorer.[147] The WP explored alternative consent methods, such as pop-up windows providing relevant information to data subjects and "splash screens" that compel data subjects to read important details upon entering the website. However, the effectiveness of the splash screen approach in practice is questionable, as data subjects might either leave the site or accept without fully understanding the information presented.[148]

Numerous privacy-focused tools like ad-blockers and anti-trackers have been developed and their compatibility with the e-Privacy Directive is yet to be clarified by the European Data Protection Board (EDPB). Currently, these browser add-ons seem to align with Recital 17 and offers a more refined way for data subjects to express their preferences. However, their use may conflict with the business policies of some websites until further clarification is given. AdNauseam, an innovative ad-blocker that not only prevents third-party cookies but also randomly "clicks" on advertisements to obstruct statistical and behavioural research, is prohibited by Google from being used with Chrome.[149]

While guidelines and requirements have been created to address issue of cookies and obtain consent, cookies themselves pose inherent challenges. For instance, Google's "CONSENT" cookie, which retains the data subject's consent to their policy after selecting general terms and conditions, comprising rules concerning cookies, is regarded as absolutely important for utilising their services. An excessive reliance on consent should be better understood, as some technical processes may continue without the data subjects' awareness, making it debatable whether the deletion of a cookie truly reflects the user's preferences.[150]

The idea of a contract of adhesion, where the weaker party accepts pre-written and non-negotiable stipulations by the other stronger party, is analogous in classical civil law. Policymakers came up with the concept of consumer status to address this and accept that consent may not always

[147] Eleni Kosta, 'Peeking into the cookie jar: the European approach towards the regulation of cookies' (2013) 21(4) International Journal of Law and Information Technology < https://ssrn.com/abstract=2675810 > accessed 8 August 2023.
[148] Article 29 Data Protection Working Party (n 124).
[149] Kosta (n 147).
[150] Ibid.

be freely supplied as intended. Policymakers are uncertain in the data economy and fail to consider the possibility of taking consumer protection measures. The GDPR and e-Privacy rules aimed to introduce effective sanctions, inspired by consumer protection, but they lack the authority to address monopolies.[151]

Informing data subjects about data processing has limitations, as methods like banners and cookie buttons lack effectiveness in conveying actual knowledge. The complexity of data processing and legal jargon often makes it difficult for the average user to understand or be interested in reading such information.[152] Currently, the data subject's awareness of the cookie issue is limited, often due to insufficient information about the data controller, particularly in the case of third-party cookies. In the recent ECJ case known as the "Facebook fan page" case,[153] it was ruled that Facebook and Page Administrators are joint controllers for analytics cookies, highlighting the ongoing challenges of consent and cookies, which need a drastic change in approach to avoid further issues.[154]

The key idea of "controller" is crucial in EU data protection laws, as it determines the parties responsible for data protection duties. However, identifying controllers, especially in cases involving cookies on websites and targeted advertising, can be challenging. The CJEU adopted a broad interpretation of the notion of "controller", which will continue to apply pursuant to the GDPR and could significantly impact the lawful use of cookies and online analytical services.[155]

The case involves a German corporation that created a Facebook fan page using the "Facebook Insights" tool to receive anonymous viewing statistics about visitors. Facebook uses cookies to gather personal information, although no personal information is actually obtained by the firm. Instead, it utilises targeted advertisements depending on the interests and conduct of visitors. The Schleswig-Holstein DPA issued an order to remove the fan page because the German corporation neglected to tell site users about Facebook's usage of cookies on its page. The corporation contended that any enforcement action should be addressed at Facebook explicitly, Facebook

[151] Varisco (n 126).
[152] Ibid.
[153] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] ECR I-388.
[154] Varisco (n 126).
[155] Charlotte Ducuing, Jessica Schroers and Els Kindt, 'The Wirtschaftsakademie Fan Page Decision: A Landmark on Joint Controllership - A Challenge for Supervisory Authorities Competences' (2018) 4(4) European Data Protection Law Review 548.

Ireland and they are under no responsibility of the personal data processed by Facebook's cookies as the corporation is not the controller. The German courts determined that Facebook Ireland, and not the business that owns the fan page, was the controller, and they questioned the CJEU over whether a DPA may execute a summon against a non-controller.[156]

Advocate General Bot (AG Bot) analysed the use of cookies in data processing, particularly in online tracking where consumer's behavior is observed for marketing purposes. AG Bot emphasised that online tracking, which involves monitoring and analysing data subject's habits to identify areas of interest, requires the data subject's consent under the Directive and new Regulation.[157] AG Bot identified a complex scenario with multiple data controllers, including Facebook Ireland, fan page holders, and Facebook Inc. The CJEU's 2018 judgment upheld this approach and clarified that accessing Facebook does not make users shared liability for data processing.[158] The focus was on whether Facebook Inc. qualified as a controller, with the CJEU ruling that starting a fan page grants Facebook permission to place cookies on visitors' devices, irrespective of whether they have Facebook accounts.[159]

The CJEU ruled that creating a fan page on Facebook involves setting parameters that impact personal data processing, making the page administrator a data controller. Enabling cookies on the page associates the holder with data processing through cookies, aligning with data protection laws' definition of a controller.[160] The data's privacy impact is notable, primarily for targeted advertising, including sensitive demographic details. The CJEU noted that controllers' responsibilities can vary based on involvement in processing stages.[161] Despite lacking access to gathered data, the fan page owner remains a controller. Cookies, common tools for online data collection, extend Facebook's data reach, involving various parties. The judgment highlights

[156] Robin Hopkins, 'The CJEU's Facebook Fan Page Judgment: Joint Data Controllers, Cookies and Targeted Advertising' (2018) 2(5) International Journal for the Data Protection Officer, Privacy Officer & Privacy Counsel 13.
[157] Rene Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, Effective and Complete Protection and Its Application to Data Access Rights in Europe' (2019) 10(1) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 92.
[158] Susanna Lindroos-Hovinheimo, "Who controls our data? The legal reasoning of the European Court of Justice in Wirtschaftsakademie Schleswig-Holstein and Tietosuojavaltuutettu v Jehovan todistajat" (2019) 28 (2) Information and Communications Technology Law < https://doi.org/10.1080/13600834.2019.1623447 > accessed 22 July 2023.
[159] Ducuing, Jessica and Kindt (n 155) 550.
[160] Hopkins (n 156) 13-15.
[161] Ducuing, Jessica and Kindt (n 155) 549.

evolving GDPR jurisprudence, underlining 'controller' scope and addressing cookie-related data protection concerns, especially in targeted advertising scenarios.[162]

(3.4.4) The validity of Consent pertaining to Cookie Usage in different EU countries

i) France Finds Big Data's Cookie Usage Results in Invalid Consent

The French DPA (CNIL) imposed a punishment on Google for its first infringement of the GDPR in January 2019. Individuals who purchased Android smartphones were required to agree to Google's terms and conditions for the establishment of their accounts, which featured a privacy provision. The consent procedure, which included the use of pre-selected checkboxes, failed to adhere to the principles of affirmative consent. The lack of distinct alternatives for bundling purposes under the 'Accept' category was insufficiently precise. The CNIL determined that Google's request for consent was deficient in terms of clarity and information, so falling short of the criteria set out by the GDPR.[163]

Amazon was penalised by CNIL in December 2020 for utilising cookies without getting legal authorisation. Their ad offered no options or information, merely an 'OK' button while automatically processing data. Upon viewing Amazon's French website, CNIL determined that this breached the GDPR since there were inadequate consent information. Amazon disputed the CNIL's authority and the difficulty of the EU's cookie consent guidelines.[164]

CNIL fined Google again for breaching GDPR consent rules in December 2020. Google placed cookies without consent, with unclear pop-ups and insufficient opt-out. CNIL found Google's updated 'I Accept' and 'More information' banners still lacking, not informing data subjects of the option to refuse easily. Multiple advertising cookies remained even after opting out, undermining free consent.[165] A year later, CNIL ruled Google violated data protection with complex consent options on 'google.fr' and 'youtube.com', stressing consent should be simple to give and refuse.

[162] Hopkins (n 156) 13-15.
[163] Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC in Meskenaite (n 85).
[164] Deliberation of the Restricted Committee SAN-2020-013 of 07 December 2020 concerning AMAZON EUROPE CORE in Meskenaite (n 85).
[165] Deliberation of the Restricted Committee SAN-2020-012 of 07 December 2020 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED in Meskenaite (n 85).

Google's claim of prior proceedings being different was rejected. Google asked CNIL to refer a question to the CJEU about lacking 'refuse all' option, but CNIL lacked the capacity.[166]

The French DPA issued a 60 million Euro punishment for improper management of personal data on the same day as Google was subject to CNIL sanctions. Data subjects have to choose between "Accept all" and "Manage data settings" on a cookie banner in order to access the social networking site. Before clicking "Accept cookies," choosing the latter option needed active consent for certain functions. In spite of this, CNIL discovered that clicking "Accept all" was simpler, which is against GDPR consent guidelines. The DPA has coined the phrase "Dark patterns," citing research on trickery in pop-up designs that coerce data subjects into providing their consent.[167]

ii) *German Court Rules Against Deceptive Cookie Banners*

The Federation of German Consumer Organisations (VZBV) sued Advocado, a German online legal services platform, in the Rostock Regional Court, alleging that the company's cookie banners violated GDPR rules. VZBV had initially informed Advocado of data collection issues and subsequent changes to the cookie banner, but deemed the new version non-compliant. The original banner had 'OK' and 'Show details' options, each with pre-selected checkboxes for various purposes. The updated banner replaced these options with 'Allow cookies' and 'Only use necessary cookies,' with the latter designed ambiguously.[168]

The court ruled that brief explanations and technical naming of cookies did not meet consent requirements, and the use of pre-selected checkboxes was unlawful. The misleading design of the 'reject cookies' option undermined unambiguous consent. This verdict followed the Planet49 case, reinforcing the need for clear and specific consent mechanisms.[169]

[166] Ibid.
[167] Deliberation of the Restricted Committee SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED in Meskenaite (n 85).
[168] Landgericht Rostock, 3 O 762/19, 15 September 2020 in Meskenaite (n 85).
[169] Ibid.

iii) *Danish DPA Rejects Misleading Cookie Banner Designs*

In October 2021, the Danish DPA found Danish retailer Ahlstrom had gathered personal data through improper cookie banners that did not meet GDPR consent rules. Ahlstrøm had used two ineffective banners prior to the investigation. The first banner lacked a reject option and specific consent. The second banner had misleading design, making refusal harder than consent, violating free and clear consent standards.[170]

Understanding how cookie framework functions is crucial for data subjects, especially in light of cases like the Danish DPA's findings on Ahlstrom. These instances highlight the significance of clear and compliant cookie banners that align with GDPR consent regulations. Transparent explanations about data collection, along with easily accessible options for rejecting or accepting cookies, ensure that individuals can make informed choices about their personal data. By comprehending the intricacies of cookie consent mechanisms, individuals can protect their privacy and exercise their rights effectively in the digital landscape.[171]

CONCLUSION FOR CHAPTER 3

In summary, the European Union's legal evolution concerning consent, especially in the context of data processing and cookies, demonstrates a steadfast commitment to protecting individual privacy rights. From the inception of data protection legislation to the modern GDPR, the focus has shifted towards ensuring well-informed, transparent, and unambiguous consent. This emphasis is evident in various cases across EU countries, where deceptive practices are being challenged to uphold the essence of meaningful consent.

As technology continues to advance, the significance of consent becomes more pronounced. It signifies a proactive step towards giving individuals control over their data in a digital world. The evolving legal landscape surrounding cookies and data protection underscores the EU's dedication to maintaining a balance between innovation and privacy rights. In essence, the EU's evolving

[170] Datatilsynet, Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS' behandling af personoplysninger om hjemmesidebesøgende, 2021-431-0125, 20 October 2021 in Meskenaite (n 85).
[171] Ibid.

approach to consent serves as a beacon for responsible data practices, safeguarding individual privacy while navigating the complexities of the digital age.

CHAPTER 4: ADDRESSING COERCED CONSENT AND LOOPHOLES IN EU REGULATIONS

In this chapter, we undertake a comprehensive critical analysis of coerced consent challenges and transparency gaps within the framework of EU data protection regulations. Despite the GDPR's focus on empowering data subjects, its effectiveness in mitigating associated risks is questioned. Often, individuals consent to data processing without fully grasping the consequences,[172] exacerbated by the prevalence of digital technology and algorithmic decision-making.[173] We delve into these complexities, alongside the intricate integration of AI and big data, while also examining consent manipulation through dark patterns and deceptive designs. This analysis uncovers persistent nuances within the regulatory landscape.[174]

(4.1) Identifying and Analysing Coerced Consent Practices in Digital Services

The WP asserted that the use of algorithmic data processing poses challenges for obtaining valid consent due to technological complexities and the inability to foresee the precise outcomes of the data, making it difficult to ensure informed consent from data subjects. The contradictory issue at hand has not been adequately resolved by the reform of consent methods.[175]

The introduction of AI and machine learning algorithms presents a novel problem in terms of ensuring informed consent and the consent is continuously valid, since data controllers and data subjects sometimes fail to forethought the processing techniques and results involved.[176] Obtaining valid consent that is both specific and informed becomes challenging in the context of AI and big data because it requires the data subject to understand all aspects and consequences of the processing, which can be difficult, especially when dealing with big data analysis.[177]

---

[172] Bart Custers (eds), 'Informed Consent in Social Media Use - The Gap between User Expectations and EU Personal Data Protection Law' (2013) 10(4) Scripted < https://ssrn.com/abstract=3047134 > accessed 8 July 2023.
[173] Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20(1) Theoretical Inquiries in Law < https://www7.tau.ac.il/ojs/index.php/til/article/view/1607/1709 > accessed 8 July 2023.
[174] Lilian Edwards and Michael Veale 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (2018), 16(3) IEEE Security and Privacy < https://doi.org/10.1109/MSP.2018.2701152 > accessed 26 July 2023.
[175] Article 29 Data Protection Working Party (n 10).
[176] Edwards and Veale (n 174).
[177] Maria Adeleide Adrienne Oostveen, 'Protecting Individuals Against the Negative Impact of Big Data: The Potential and Limitations of the Privacy and Data Protection Law Approach' (PHD Thesis, University of Amsterdam 2018). < https://pure.uva.nl/ws/files/21397315/Thesis_complete_.pdf > accessed 26 July 2023.

Big data is something that most individuals will come into contact with at least once in their lives, but the personalised internet experience which is the example of big data has a significant impact on many Europeans. Big data has a significant impact on personalisation, particularly through behavioural advertising, where online experiences and advertisements are tailored to individuals based on their location, browsing history, interests, and device characteristics.[178] Third-party businesses such as advertising networks gather comprehensive data on people, including their online surfing patterns social activities, demographic information and geographical locations. Utilising the provided data, the entities involved generate distinct profiles for each user and thereafter disseminate tailored advertisements to consumers who have been recognised using cookies.[179]

As this research focuses on the analysis of coerced consent, the concept of Big Data will only be mentioned briefly and not discussed in details to give some insights on how it can affect the coercion of consent. Prominent instances in recent times have given rise to ethical and legal apprehensions pertaining to the utilisation of datasets by corporations. Notably, the revelation in 2018 that Cambridge Analytica acquired personal information from more than 80 million Facebook's data subjects without consent and employed it to specifically target American voters during the 2016 United States (US) presidential election has contributed to these concerns.[180] Despite the fact that the emergence of Cambridge Analytica prompted the initiation of public discourse on the subject of data monitoring, these underlying conflicts have been there for a considerable period of time. In summary, the primary focus of this controversy is around issues of privacy and consent.[181]

When registering for internet-based platforms such as Facebook (now known as Meta), it is common for data subjects to consent to extensive Terms of Service agreements without properly reviewing its contents. This situation prompts inquiries on the legitimacy of consent and the obligation of data subjects to possess enough knowledge. The significance of concerns pertaining

[178] Frederik Zuiderveen Borgesius, *Behavioural Targeting', Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International 2015) 15–16.
[179] Eric Siegel, *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die* (Wiley 2013) 37.
[180] Adam J Andreotta, Nin Kirkham and Marco Rizzi, 'AI, big data, and the future of consent' (2022) 37 AI and Society < https://doi.org/10.1007/s00146-021-01262-5 > accessed 27 July 2023.
[181] Justin Sherman, 'Privacy and Consent: The Heart of the Cambridge Analytica Scandal' (*Venafi*, 2 April 2018) < https://venafi.com/blog/privacy-and-consent-heart-cambridge-analytica-scandal/ > accessed 27 July 2023.

to consent will grow in tandem with the growing integration of technology into our daily lives. In light of the Facebook-Cambridge Analytica incident, would individuals still possess the prerogative to voice their grievances if the sharing of data had been conducted in accordance with the requirements outlined in the Terms of Service? Should Facebook adhere to ethical standards by respecting our choices after we have consented by clicking "Agree"?[182]

Facebook's Data Policy reveals extensive data collection practices, including information from devices, device locations, connection details, and data shared with third-party apps and services. This raises concerns about data control, privacy rights, and data ownership, as Facebook's practices have been ongoing for years, yet they may be unfamiliar to many data subjects. Beyond the Cambridge Analytica scandal, we must acknowledge that Facebook is not the sole tech giant profiting from our personal information based on our often unread "Agree" clicks. This is a broader problem concerning digital consent, privacy, data-tracking, ownership and trust, extending far beyond Facebook and Cambridge Analytica. It is time to recognise this reality.[183]

The compromised nature of freely provided consent arises when a consumer is compelled to accept various reasons for data collection and processing, as determined by the data controller. This compulsion undermines the principle of consent. In order to maintain the legitimacy of consent, it is essential to uphold a level of precision by distinguishing between specific purposes chosen by the data operator and those that are not selected, and acquiring individual permission for each distinct processing purpose.[184]

(4.1.1) The Impediments to Personal Autonomy in the Process of Information Collection

For data subjects to maintain control over their data, they need knowledge about its processing, enabling them to make informed choices aligning with their preferences. Data collectors can provide this information through data usage policies, but relying solely on them for control is impractical.[185] Data subjects are granted with the right to access the information, as outlined in

[182] Ibid.
[183] Ibid.
[184] Goicovici (n 88).
[185] Tanya L Chartrand, 'The role of conscious awareness in consumer behavior. Journal of Consumer Psychology' (2005) 15(3) Journal of Consumer Psychology 203–210 < https://people.duke.edu/~tlc10/bio/TLC_articles/2005/Chartrand_2005.pdf > accessed 27 July 2023.

Article 15 and Article 13(2)(b) of the GDPR[186] but the proliferation of information within the current digital landscape presents a significant challenge to data subjects' capacities to maintain control over their personal data. This challenge arises from the sheer volume of information available, which may overwhelm individuals' cognitive capacities and hinder their ability to make well-informed choices on privacy, irrespective of their cognitive talents or access to information.[187]

Privacy and data protection systems, together with their associated statements and regulations, operate under the assumption that consumers possess the cognitive capacity to thoroughly analyse information. However, the rapid advancement of technology has resulted in the proliferation of lengthier and intricate information, therefore imposing a burden on data subjects' cognitive abilities.[188]

To ensure well-informed decision-making, data subjects should assess the anticipated advantages and drawbacks linked to the disclosure of data, aligning them with their preferences.[189] This process involves extensive cognitive processing, as demonstrated through a study conducted by Norwegian campaign-group. The study revealed that it took approximately 32 hours to read and understand the terms of 33 selected smartphone applications. It is important to acknowledge that the aforementioned duration merely pertains to the act of reading the materials, without considering the subsequent contemplation of the implications associated with agreeing to those policies.[190]

In addition to basic cognitive ability, different degrees of knowledge or "literacy" may also have an impact on how effectively people grasp information relating to privacy.[191] For instance, fewer than two out of seven questions pertaining to informational privacy were properly answered by

---

[186] Jan Hendrik Betzing (eds), 'The impact of transparency on mobile privacy decision making' (2019) 30(6) Electronic Markets < https://www.researchgate.net/publication/330936528_The_impact_of_transparency_on_mobile_privacy_decision_making > accessed 27 July 2023.
[187] I van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 Journal of Consumer Policy < https://link.springer.com/article/10.1007/s10603-018-9399-7 > accessed 27 July 2023.
[188] Jennifer Shore and Jill Steinman, 'Did You Really Agree to That? The Evolution of Facebook's Privacy Policy' (*Technology Science*, 10 August 2015) < https://techscience.org/a/2015081102/ > accessed 27 July 2023.
[189] Ooijen and Vrabec (n 187).
[190] Chiara Palazzo, 'Consumer campaigners read terms and conditions of their mobile phone apps... all 250,000 words' *The Telegraph* (Sydney, 26 May 2016) < https://www.telegraph.co.uk/technology/2016/05/26/consumer-campaigners-read-terms-and-conditions-of-their-mobile-p/ > accessed 27 July 2023.
[191] Ooijen and Vrabec (n 187).

consumers in a survey by Park, indicating a poor level of consumer literacy on data policy awareness.[192]

In their study, Jensen and Potts (2004) conducted an analysis of privacy rules from a sample of 64 US corporations, including prominent entities such as Google, Weather Channel, and eBay. The findings of their research, as determined by the Flesch Reading Ease Score, indicated that a mere 6% of these policies were deemed comprehensible for high school graduates or less. 54% were tough for those with more than 14 years of study, and 13% for postgraduates. The results of this study indicate that a considerable segment of the public, even individuals with advanced levels of education, may have difficulties in comprehending several privacy regulations.[193]

In today's digital world, powerful, unexplained algorithms, like black boxes with unknown consequences, put great strain on our limited information processing capacities. This abstract presentation causes an imbalance of information between data controllers and data subjects, ultimately resulting in a disruption of control over information.[194]

(4.1.2) Lack of Transparency

Multinational tech companies have privacy policies, developer agreements, and license agreements, but there is a lack of transparency regarding the processing of personal data, including location data, by smartphones and mobile apps. For instance, iPhone users must agree to Apple's terms without knowing the extent of their personal data processing during app installation and usage.[195]

GDPR compels service providers to enhance transparency when notifying data subjects about the processing of personal data, empowering individuals to make informed choices regarding their privacy. The primary objective of this initiative is to mitigate the presence of unequal access to information and enhance the safeguarding of data for individuals residing in the EU. It imposes a

[192] Yong Jin Park, 'Digital Literacy and Privacy Behavior Online' (2011) 40(2) Communication Research < https://doi.org/10.1177/0093650211418338 > accessed 27 July 2023.
[193] Carlos Jenson and Colin Potts, 'Privacy policies as decision-making tools: An evaluation of online privacy notices' (Proceedings of the 2004 Conference on Human Factors in Computing Systems Vienna, April 2004) < https://www.researchgate.net/publication/221515790 > accessed 27 July 2023.
[194] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) in Ooijen and Vrabec (n 187).
[195] Shakila Bu-Pasha (eds), 'EU Law Perspectives on Location Data Privacy in Smartphones' (2016) 2(3) European Data Protection Law Review 318.

requirement under Article 5(1)(a) that the handling of personal data must conform to the principles of lawfulness, fairness, and transparency.[196]

According to Article 6 of the GDPR, lawfulness requires obtaining active consent from data subjects. As stated in Chapter 3, consent as defined under Article 4(11) must meet certain criteria, including being freely given, specific and explicit, informed, and unambiguous. In accordance with Article 7(1) and (2), this consent necessitates that data subjects possess the ability to exercise their choice, actively opt in, get comprehensive information on data processing, and clearly differentiate the consent form from other contractual terms. Additionally, Article 12(1) of the GDPR required that all information be presented in a manner that is concise, transparent, comprehensible and readily accessible.[197]

To ensure data subjects are well-informed, it is imperative that the data controller takes measures to mitigate information asymmetry before proceeding with the collection of personal data from the data subjects, as outlined in Article 13. It is of utmost importance that data subjects be adequately informed about the "identity and contact details of the service provider" in accordance with Article 13(1)(a). Additionally, data subjects should be made aware of the purpose of the processing as outlined in Article 13(1)(c) and provided with information regarding the recipients of their personal data as specified in Article 13(1)(e). In order to ensure fairness and transparency in data processing, it is imperative that data subjects are provided with information of the data storage duration, in accordance with Article 13(2)(a). Furthermore, Articles 13(2)(b), 16 and 17 granted data subjects the rights to rectify and erase their data. Lastly, data subjects should be able to withdraw their consent at any given time, in accordance with Article 13(2)(c).[198]

Data subjects have the ability to provide consent in an active manner by either accepting or denying requests for permission. However, in order for this consent to be considered informed, it is essential that they have been provided with all the necessary information as outlined before. The GDPR does not include specific instructions on how to ensure transparency.[199] However, developers have the option to provide the necessary information inside the consent request, as suggested by Joshua Tan and others, in order to offer data subjects both context and choice.

[196] Betzing (n 186).
[197] Ibid.
[198] Ibid.
[199] Ibid.

Furthermore, it is essential that data subjects be provided with unrestricted access to a comprehensive privacy policy document at all times.[200]

While it is true that data subjects have the ability to access and read privacy policies, it is important to note that a significant portion of data subjects may not fully grasp the personal data processing practices used by service providers. Extensive research has consistently shown that service users have difficulties comprehending the intricate legal terminology used in privacy rules,[201][202] resulting in a significant proportion of individuals opting not to engage with them.[203] This results in a dearth of transparency, which is evident in the presence of information asymmetry between the understanding possessed by data subjects and the data controller about processing practices.[204]

As remarked by the WP, data subjects have the capability to exclusively enable or disable location services within the iOS operating system. When the device is in the OFF state, it does not collect or exchange any location data with applications. When activated, Apple collects anonymous location and Wi-Fi data, using a chosen method for detecting the data subject's location. In the context of Android devices, the accessibility of location information is governed by several modes, such as High Accuracy and Power Saving. The acquisition of this data necessitates the data subject's consent for location service under Google. Additionally, there exists a concealed

[200] Joshua Tan (eds), 'The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior' (Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, April 2014) < https://www.researchgate.net/publication/266655816 > accessed 28 July 2023.
[201] Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) Journal of Law and Policy for the Information Society < https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1&isAllowed=y > accessed 28 July 2023.
[202] Florian Schaub (eds), 'A Design Space for Effective Privacy Notices' (Symposium on Usable Privacy and Security, Ottawa, July 2015) < https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf > accessed 28 July 2023.
[203] Janice Y Tsai (eds), 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study' (2011) 22 Information Systems Research < https://www.researchgate.net/publication/220079706 > accessed 28 July 2023.
[204] Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and human behavior in the age of information' (2015) 347(6221) Science < https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.pdf > accessed 28 July 2023.

configuration that permits the scanning of Wi-Fi networks even when the Wi-Fi functionality is off, a feature that is likely unfamiliar to most data subjects.[205]

Global tech giants like Apple and Google have unbalanced app approval processes, neglecting international and regional data protection standards. This raises concerns about the gathering of data subjects' personal data and the necessity for legal accountability under European data protection laws, necessitating international cooperation for a transparent and secure electronic communication system using GPS or Wi-Fi for location services.[206]

(4.1.3) Lack of Choices

Privacy notices often lack meaningful choices, and using websites, apps, or devices is considered consent even if data subjects have not read them. The notices may describe data practices without clear opt-out options, leaving data subjects with limited choices and compromising their privacy. Data subjects usually consent to access desired services, making privacy notices ineffective in empowering informed decisions. Privacy controls are necessary to implement awareness of data practices.[207]

As mentioned above, the lengthy and complex information and limited options presented in privacy notifications render them mostly unimportant to data subjects.[208] According to a report issued by the White House, it has been observed that data subjects often exhibit a lack of engagement with terms and conditions, and often fail to comprehend the repercussions associated with providing consent.[209] Business enterprises possess the ability to modify their data practices and notifications at any given moment, rendering attempts to comprehend them ultimately

[205] Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices' (adopted on 16 May 2011) 881/11/EN WP185 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf > accessed 29 July 2023.
[206] Pasha (n 195) 319.
[207] Schaub (n 202).
[208] Fred H Cate, 'The Limits of Notice and Choice' (2010) 8(2) IEEE Security and Privacy 59-62.
[209] The President's Council of Advisors on Science and Technology (PCAST), 'Report to the President Big Data and Privacy: A Technological Perspective' (May 2014) < https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf > accessed 29 July 2023.

fruitless.[210] Privacy notifications and cautions are often presented at unfavourable circumstances, resulting in their disregard without careful examination.[211]

(4.2) Assessing the Impact of Dark Patterns on Consent in Digital Services

The implementation of the GDPR and other international privacy legislations has presented a challenging predicament for website operators. They find themselves grappling with the intricate legal obligations pertaining to the gathering and processing of data, necessitating a comprehensive comprehension and adherence to these regulations. In order to handle the situation, some operators use externalised cookie banners and consent-management systems, which often prove inadequate in guaranteeing adherence to regulations owing to configuration challenges or technological constraints in implementing user privacy preferences.[212]

The substantial discrepancy between the perceived level of privacy compliance of an organisation and its actual level of compliance is known as the compliance gap. Numerous organisations have included consent mechanisms on their online platforms; yet, they often fall short of satisfying the stipulations set out by prominent privacy legislations. Consequently, this situation engenders a deceptive perception of privacy for data subjects and a misguided perception of adherence to regulations for businesses, eventually exposing both parties to potential risks.[213]

In accordance with the aforementioned GDPR's requirements, the collection or processing of data subjects necessitate a legitimate legal foundation, whereby obtaining consent has considerable significance. Nevertheless, a considerable number of enterprises and vendors offering cookie consent technologies have shown a lack of comprehension and misinterpretation about the consent obligations outlined in the GDPR. In order to ensure compliance with ethical and legal standards,

---

[210] Paul M Schwartz and Daniel Solove, 'Notice and Choice: Implications for Digital Marketing to Youth' (The Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children, Berkeley, June 2009) < https://www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf > accessed 29 July 2023.
[211] Philip Inglesant and M Angela Sasse, 'The True Cost of Unusable Password Policies: Password Use in the Wild' (Proceedings of the 28th International Conference on Human Factors in Computing Systems, Atlanta, April 2010) < https://www.researchgate.net/publication/221517955_The_true_cost_of_unusable_password_policies > accessed 29 July 2023.
[212] Guy Tytunovich, 'The Privacy Compliance Gap: How Lack Of Consent Enforcement Is Exposing Brands To Millions In Fines And Penalties' (*Forbes*, 19 December 2022) < https://www.forbes.com/sites/forbestechcouncil/2022/12/19/the-privacy-compliance-gap-how-lack-of-consent-enforcement-is-exposing-brands-to-millions-in-fines-and-penalties/ > accessed 29 July 2023.
[213] Ibid.

consent should be obtained through an "opt-in" mechanism that requires data subjects to actively indicate their consent. It is crucial that individuals be adequately educated about the implications of their consent, and that the process is clear and unambiguous. Furthermore, consent should be freely given, without any kind of coercion, and data subjects should be provided with transparent options to either opt in or opt out of monitoring and data processing activities.[214]

Consent banners often fail to meet GDPR requirements by using prechecked boxes or making opting out more challenging than opting in. Some banners rely on implied consent when data subjects close or ignore them, which violates GDPR guidelines.[215] Manipulative practices, such as the deliberate exclusion of opt-out buttons and the disrespect for opt-out choices, are sometimes referred to as dark patterns which can leads to coercion of consent as shown in Figure 1 below. Subtle dark patterns include the use of intricate wording or the enhancement of visual prominence of the opt-in button. These strategies compromise the data subjects' autonomy and have the potential to violate data protection legislation, resulting in penalties imposed by regulatory authorities. The French DPA imposed significant fines on Google for $170 million and Facebook for $8 million in relation to their non-compliance with consent dialogues.[216]

[214] Ibid.
[215] Ibid.
[216] Daniel Kirkman, Kami Vaniea and Daniel W Woods, 'Dark Dialogs: Automated detection of 10 dark patterns on cookie dialogs' (2023 IEEE 8th European Symposium on Security and Privacy, Delft, July 2023) < https://www.danielwoods.info/assets/pdf/KVW_DarkDialogs_EuroSnP.pdf > accessed 30 July 2023.

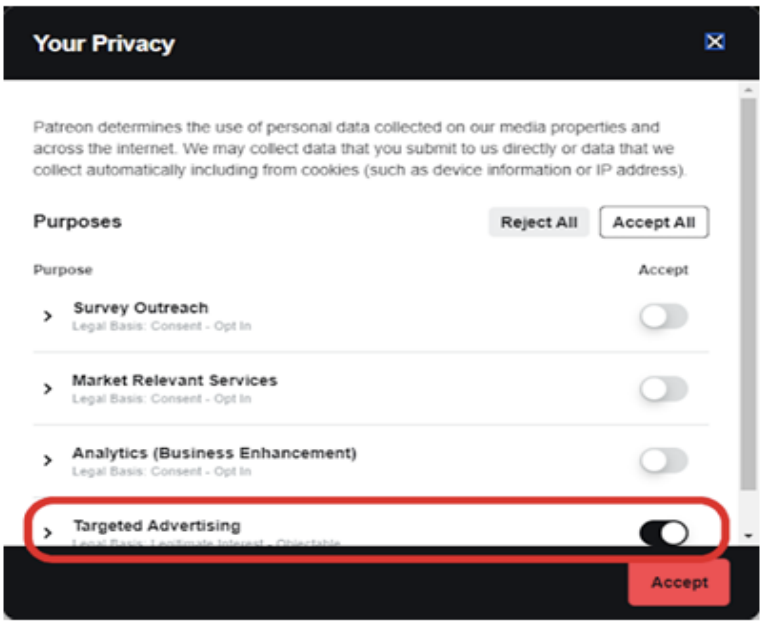

Figure 1: Example of the practice of Dark Pattern[217]

(4.2.1) Cookie banner or Consent Wall

The use of a consent wall or widely known as cookie banner on websites presents challenges as it forces data subjects to make a choice before accessing the site, potentially violating the "freely given consent" requirement of GDPR as illustrated in Figure 2 below. While it may be seen as manipulative and coercive, from a legal standpoint, its function is to provide clear and verifiable evidence of consent. However, in cases where the choices made by data subjects do not coincide with the intended purpose of the website, it is important to provide alternative access alternatives. This is necessary in order to respect the preferences of the data subjects and prevent any negative consequences.[218]

[217] Example of the practice of Dark Pattern from the official website of Patreon in Kirkman, Vaniea and Woods (n 216).
[218] Colin M Gray (eds), 'Dark Paterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective' (Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, May 2021) < https://dl.acm.org/doi/pdf/10.1145/3411764.3445779 > accessed 30 July 2023.

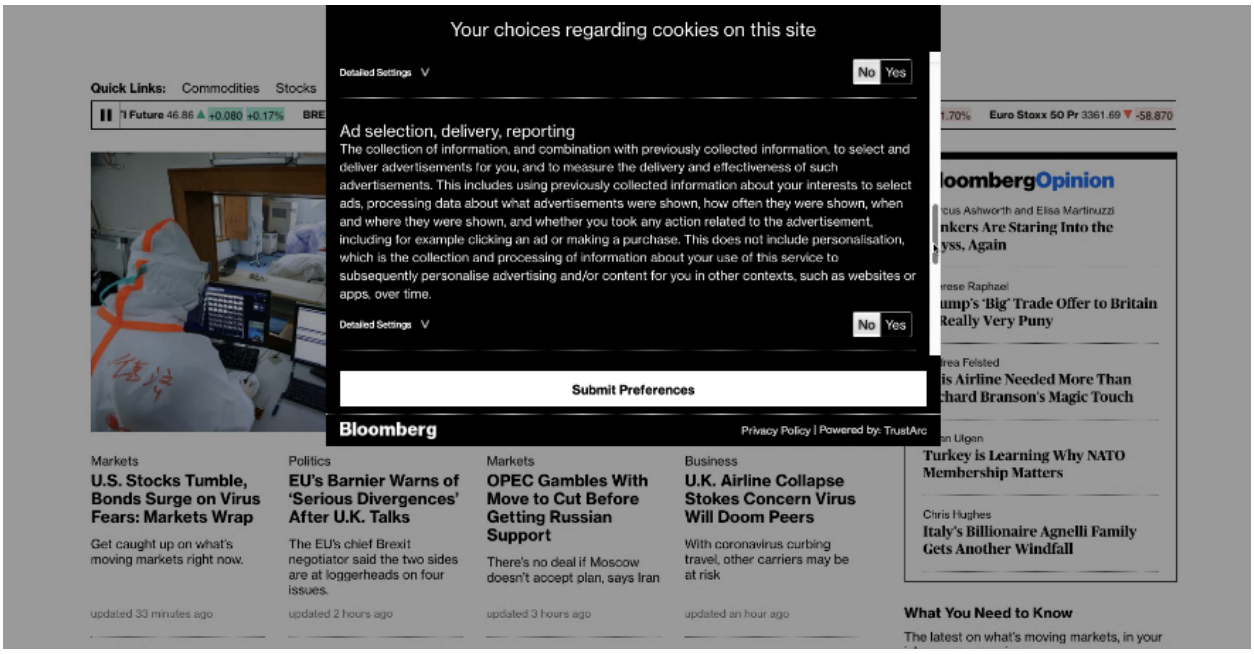

Figure 2: Example of a Cookie Banner from the official website of Bloomberg[219]

(4.3) Dark Patterns in Tricky Layouts: Deceptive Design and Privacy Implications

A limited-service option is provided, which presents a modified version of the website with restricted functionality and it can impact content availability. This enables data subjects to choose from a range of access choices that align with their privacy preferences. According to the WP, the permissibility of this alternative is contingent upon guaranteeing that the data subjects' withdrawal of consent does not lead to a diminished level of service or disadvantage, but precise delineations in the context of digital environments remain ambiguous.[220]

The design of the limited service may potentially contravene the legal obligation of obtaining informed consent, since it is necessary for data subjects to possess knowledge about the ramifications of withdrawing consent, which encompasses the potential limitations on service accessibility. The necessity for freely supplied consent may be violated when individuals are

[219] Example of a Cookie Banner from the official website of Bloomberg (recorded on 5 March 2020) in Gray (n 218).
[220] EDPB (n 71).

obligated to provide consent for full website access without being offered other choices.[221] Making certain configurations more difficult or costly to choose may act as a "punishment," deterring inexperienced data subjects from selecting risky settings.[222]

The implementation of a tracking wall by a designer compels visitors to accept monitoring technology in order to get access to content or services, hence eliminating the ability to withdraw consent. This situation gives rise to apprehensions over the freely given or voluntary nature of consent. The technique of reading order manipulation is used to surreptitiously provide information to the user. This may be achieved by strategically highlighting a "I consent" checkbox inside a concealed area and positioning the "More Options" hyperlink outside the customary reading order within the banner as demonstrated in Figure 3 below.[223]

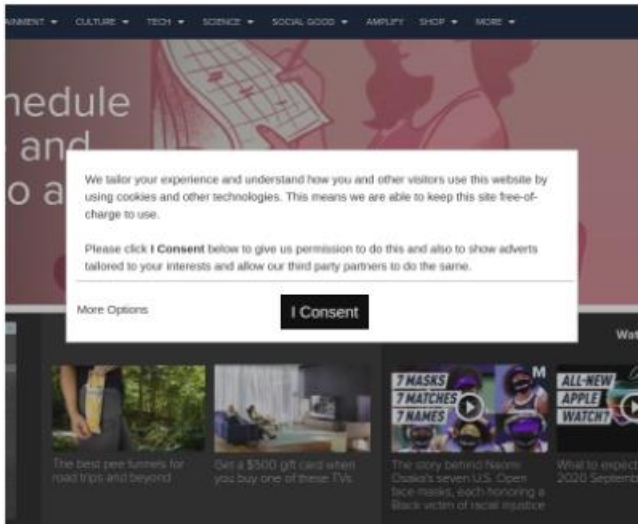

Figure 3: Sneaky Reading Order Manipulation in Consent Banners[224]

[221] Case C-61/19 *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* [2020] ECR I-158, Opinion of Advocate General Szpunar < https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62019CC0061 > accessed 31 July 2023.
[222] Alessandro Acquisti (eds), 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 50(3) ACM Computer Survey < https://dl.acm.org/doi/pdf/10.1145/3054926 > accessed 31 July 2023.
[223] Gray (n 218).
[224] Example of Sneaky Reading Order Manipulation in Consent Banners from the official website of Mashable in Gray (n 218).

As shown in Figure 4 below of an example of a Facebook's cookie banner with particular layout that tricks data subjects into choosing the essential and optional cookies. It is difficult for data subjects to grasp how "essential cookies" affect their privacy since the explanation provided to them on the site is ambiguous. In particular, the stark colour contrast favours a choice that consumers may not be aware has a higher influence on their privacy, giving the cookie banner's selection buttons a "dark pattern" appearance.[225] In addition, the lack of default toggling for optional cookies and the necessity for data subjects to navigate through to a different panel in order to reject them might be seen as violations of privacy rules like the GDPR.[226]

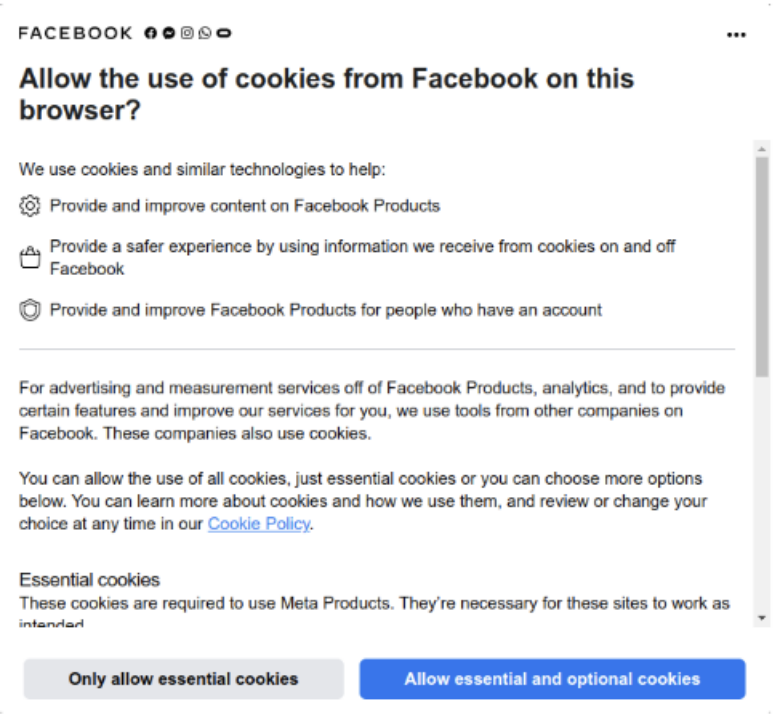

Figure 4: Example of a deceptive layout[227]

[225] European Data Protection Board, 'Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them' (Adopted on 14 March 2022) < https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf > accessed 1 August 2023.
[226] Cristiana Santos, Nataliia Bielova, and Célestin Matte, 'Are cookie banners Indeed Compliant with the Law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners' (2020) Technology and Regulation 72-73 < https://doi.org/10.26116/techreg.2020.009 > accessed 1 August 2023.
[227] Example of a deceptive layout from the official website of Facebook in Yana Dimova (eds), 'Tracking the Evolution of Cookie-based Tracking on Facebook' (Proceedings of the 21st Workshop on Privacy in the Electronic Society, Los Angeles, November 2022) < https://lepoch.at/files/facebook-cookie-tracking-wpes22.pdf > accessed 1 August 2023.

The analysis in this chapter sheds light on the persisting issue of coerced consent through dark patterns and deceptive designs within the EU data protection regulations. Despite the GDPR's intentions to empower data subjects, the complexities of digital technology, algorithmic decision-making and the lack of transparency create challenges. The prevalence of manipulative tactics, as evidenced by recent fines imposed on major companies, emphasises the need for stronger regulations to combat these practices. The analysis reveals that current mechanisms, like cookie banners, can fall short of ensuring informed and voluntary consent, leading to coerced agreements.

CONCLUSION FOR CHAPTER 4

In conclusion, the coercive nature of consent in digital services remains a critical concern within the EU regulatory landscape. The utilisation of dark patterns and deceptive designs undermines user autonomy and challenges the effectiveness of current data protection regulations. As the digital realm continues to evolve, the need for more robust legal frameworks becomes apparent. The subsequent chapter's exploration of new proposed regulations offers hope for addressing these issues and fostering a more transparent and ethically responsible digital environment. The ongoing collaboration between legal measures and technological advancements is crucial to ensure privacy, informed consent, and data protection in an increasingly interconnected world.

CHAPTER 5: ASSESSMENT

(5.1) Evaluating Consent in the Digital Era: Effectiveness of Regulatory Framework and Privacy Measures

Consent plays a crucial role in economic and social transactions, reflecting moral autonomy[228] and safeguarding individuals from unfair dealings.[229] Under the premise of educated customers and market competition, consent-based policies may promote market satisfaction.[230] The practicality of inferring consent from clicks is hindered by the susceptibility of users' behaviours to manipulation through the use of dark patterns. Dark patterns, particularly those involving the gathering and processing of cookies, are nevertheless often seen when using the internet in Europe despite the GDPR's introduction. Cookies allow targeted advertising and the transfer or sale of important personal data to third parties based on the browsing habits of visitors to a website, in addition to serving important services for websites.[231]

According to Article 5(3) of the 2002 e-Privacy Directive, as revised by 2009 Directive, consent is needed to store or access cookies and surveillance or tracking systems on data subjects' devices. Giving people control over their data and requiring website producers to get consent are the main objectives.[232] Website owners are free to create their own consent processes as long as they abide by EU law since there is no set structure required for consent requests. Cookie banners or consent walls which are widely displayed on websites are a frequent way to get consent.[233]

As discussed in Chapter 4, cookie banners come in a variety of designs and functions, from simple ones that just state that cookies are used without any other alternatives to intricate ones that let data subjects decline specific third-party services. Data subjects may, however, find it difficult

---

[228] Alan Schwartz and Robert E Scott, 'Contract Theory and the Limits of Contract Law' (2003) 113 Yale Law Journal < https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1467&context=faculty_scholarship > accessed 2 August 2023.
[229] Robert Cooter and Thomas Ulen, *Law and Economics* (6th edn, Pearson 2012) 342.
[230] Hugh Collins, *The Law of Contract* (Cambridge University Press 2003) 95.
[231] Omar Vasquez Duque, 'Cookies and The Illusion of Informed Consent: The Framing of The Decision Environment as Digital Manipulation' (2021) < https://ssrn.com/abstract=3957528 > accessed 2 August 2023.
[232] Jannick Sorenson and Sokol Kosta, 'Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites' (Proceedings of the World Wide Web Conference, San Francisco, May 2019) < https://www.researchgate.net/publication/330997511_Before_and_After_GDPR_The_Changes_in_Third_Party_Presence_at_Public_and_Private_European_Websites > accessed 2 August 2023.
[233] Santos, Bielova and Matte (n 226).

to comprehend the results and utilisation of their data due to information overload and deceptive dark patterns.

The instructions from the WP and DPA provide a framework for legally acceptable cookie consent under the GDPR, but they are devoid of specific advice on how to determine compliance with the law. There are still issues, such as the lack of established processes and automated technologies for audits, even though Recital 66 of the e-Privacy Directive advises strengthening enforcement by the National Authorities.[234]

The GDPR has a set of provisions that pertain to the dissemination of information in order to enhance the autonomy of data subjects. One such provision is the "right to explanation." According to Articles 13 and 14, it is essential to provide data subjects with comprehensive information on the objectives of data processing, the name of the data controller, who the data may be provided to and how long it will be kept by the individuals or entities. The notion of the "right to explanation" refers specifically to the context of automated decision-making, whereby individuals are entitled to receive relevant information on the reasoning for and effects of such choices.[235]

Nevertheless, the GDPR does not provide clear guidance for the specific degree of detail that should be included in explanations, which has resulted in continuing scholarly debates. In the era of big data, elucidating intricate algorithmic judgements is a significant challenge despite the enhanced level of control that comes with comprehending the underlying facts. The GDPR just provides a pre-emptive clarification of system operation, which is insufficient in effectively correcting disparities in information. However, the inclusion of the right to explanation is a significant advancement in tackling covert data processing and reducing risks to personal autonomy within the era of extensive data analysis.[236]

The GDPR leaves it up to data controllers to decide how to guarantee the right to information. As pointed out in Chapter 4, long and comprehensive privacy rules make it difficult for data subjects to comprehend and keep up with regular changes, particularly on mobile sites. As

[234] Ibid.
[235] Bryce Goodman and Seth Flaxman, 'European Union regulations on algorithmic decision-making and a ''Right to Explanation''' (2017) 38(3) AI Magazine < https://doi.org/10.1609/aimag.v38i3.2741 > accessed 3 August 2023.
[236] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For' (2017) 16(1) Duke Law and Technology Review < https://scholarship.law.duke.edu/dltr/vol16/iss1/2 > accessed 3 August 2023.

indicated in Article 12(7) and Recital 58 of GDPR, one potential remedy for this is the use of standardised icons to communicate important information regarding data processing, offering a streamlined and time-saving method. Once the GDPR is in effect, the European Commission is anticipated to develop comprehensive recommendations for the usage of privacy symbols.[237]

Icons have the potential to alleviate information overload and complexity, enhancing individual control and comprehension of data usage.[238] However, their standardised nature may lead to partial information, increasing the problem of data invisibility and necessitating careful consideration of design and implementation to effectively benefit data subjects.[239]

As indicated in Chapter 3, valid consent must be freely given, specific, informed, and unambiguous, signifying agreement through a clear affirmative action under Article 4 of the GDPR. Recital 32 emphasises that consent cannot be inferred from silence, inactivity, or pre-ticked boxes, granting data subjects more control over their data and ensuring voluntary decision-making. Consent may be expressed in plain words or deeds, for as by responding with an email address to a prominent disclaimer. "Unambiguous consent" differs from "explicit consent," which is used for sensitive data, under the GDPR. The regulation's final form makes a distinction between the two types of consent and having explicit consent, as opposed to unambiguous agreement, would have greatly expanded user control over personal data.[240]

As per Recital 32 of the GDPR, a straightforward action or remark, such as offering an email address in response to an obvious disclaimer, might be taken to indicate consent. Unambiguous consent is distinct from explicit consent, which only applies to sensitive data, under Article 9. In contrast to unambiguous agreement, which is differentiated between in the final version of the rule, explicit consent would have greatly expanded user control over personal data.[241]

Article 25 of the GDPR mandates the implementation of the "privacy by default" concept, which necessitates that controllers restrict the processing of personal data to what is strictly required for

[237] Lilian Edwards and Wiebke Abel, 'The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services' (2014) CREATe Working Paper 2014/15 < https://doi.org/10.5281/zenodo.12506 > accessed 3 August 2023.
[238] Chris Jay Hoofnagle and Jennifer M Urban, 'Alan Westin's Privacy Homo Economicus' (2014) 49 Wake Forest Law Review < https://ssrn.com/abstract=2434800 > accessed 3 August 2023.
[239] Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140(4) Daedalus < http://ssrn.com/abstract=2567042 > accessed 3 August 2023.
[240] Ooijen and Vrabec (n 187).
[241] Ibid.

defined purposes. This approach further ensures that data accessibility is inherently restricted, without the need for human participation. In the context of a social network, it is important to note that user profiles are not inherently public. By default, these profiles are set to a private mode, requiring users to actively modify their privacy settings in order to make their profiles publicly accessible.[242]

(5.2) Privacy by Default and Design

The privacy by design ideas put out by Ann Cavoukian propose the preservation of privacy in a manner that does not need human intervention. The incorporation of privacy as a default feature inside systems is crucial, since it guarantees the safeguarding of privacy by means of the implementation of non-identifiable interactions.[243] Article 25 of the GDPR's "data protection by default" encompasses a similar concept, although with a distinct emphasis on privacy and safeguarding personal data.[244]

Article 25 states that in order to comply with the Regulation's requirements and respect the rights of data subjects, data controllers have a limited duty to implement technological and organisational safeguards that effectively secure personal data. Beyond the need to ensure processing security under Article 32, this responsibility also includes default adoption of data protection standards and restrictions on data accessibility.[245] The concept of data protection by default comprises a range of concepts, including data reduction, purpose limitation, and minimum processing. Its objective is to gather and preserve just the essential data without necessitating the interaction of data subjects.[246] Given word limitations, this research will specifically concentrate on the concept of "privacy by default".

---

[242] Ibid.
[243] Jef Ausloos (eds), 'Guidelines for Privacy-Friendly Default Settings' ICRI Working Paper 12/2013 < https://dx.doi.org/10.2139/ssrn.2220454 > accessed 3 August 2023.
[244] Lina Jasmontaite (eds), 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4(2) European Data Protection Law Review < https://par.nsf.gov/servlets/purl/10081980 > accessed 4 August 2023.
[245] Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) Oslo Law Review < https://ssrn.com/abstract=3035164 > accessed 4 August 2023.
[246] Spanish Data Protection Authority (AEPD), 'Guidelines for Data Protection by Default' (2020) < https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto-en.pdf > accessed 4 August 2023.

Transparency, pseudonymisation, and restricting data processing to what is absolutely required for legal reasons are all requirements of the GDPR's Recital 78 which is the principle of "data protection by default," as stated in the EDPB rules. Consideration must be given to the privacy principles, especially data subjects' autonomy and consent. As well as avoiding dark patterns, the emphasis is on prioritising user requirements, fulfilling expectations, and fostering trust. In addition to meeting GDPR requirements, data protection by default promotes user trust by giving users' interests first priority.[247]

It is emphasised in Recital 5 of the proposed e-Privacy Regulation that it enhances, not diminishes, the degree of protection offered by the GDPR. In accordance with GDPR Article 25's "data protection by design and default," Recital 23 proposes that browsers should provide data subjects with a variety of cookie options. It should be made clear that the GDPR's data protection by default provisions also applicable to the processing of personal data using cookies, in particular tracking cookies used for behavioural advertising.[248]

As stated in Recital 5 of the proposed e-Privacy Regulation, which supplements the GDPR and upholds its provisions, data protection by default should be the rule. Additionally, studies reveal that it is preferable for cookies to have default settings that safeguard privacy, indicating that cookies must be covered by data protection by default.[249] The concept suggests that browsers may implement data protection by default. It mainly targets data controllers, including websites, but it is also important for creators of the goods, services, and applications as mentioned in Recital 78 of the GDPR.[250]

To prevent the usage of cookies for unnecessary purposes, data protection by default should be implemented. This would shield all data subjects from monitoring, behavioural advertising and profiling unless they voluntarily provide their consent in accordance with the GDPR. The best

[247] European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (Adopted on 20 October 2020) < https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf > accessed 4 August 2022.
[248] Max von Grafenstein (eds), 'Effective Regulation through Design - Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking Technologies in Personalised Internet Content and the Data Protection by Design Approach' (2021) < https://ssrn.com/abstract=3945471 > accessed 4 August 2023.
[249] Ausloos (n 243).
[250] Paarth Naithani, 'Curtailing the Cookie Monster through Data Protection by Default' (2022) 27(1) Tilburg Law Review < https://doi.org/10.5334/tilr.311 > accessed 4 August 2023.

course of action is to accept that the e-Privacy Regulation should implement data protection by default, forcing software developers and services to by default deny third parties' access to or storage of personal data. This comprehension holds vital importance within the framework of the e-Privacy Regulation, as it ensures the automatic safeguarding of all data subjects, irrespective of their engagement with consent banners or browser settings, and significantly lowers the tracking of data subjects online. It applies to both cookies and other tracking methods, such as fingerprinting.[251]

It is commendable that the Council's mandate does not include a clause that would have allowed browser settings to be interpreted as consent to cookies, but it should be made clear that, unless users opt-in on websites, rejecting non-essential cookies by means of browser settings is a legitimate rejection. Immediately putting a stop to the "cookie monster" with the aid of data protection by default will readily minimise data subjects' monitoring, bridging the gap while data subjects failed to interact actively with consent banners and settings.[252]

(5.3) Examining the Proposed e-Privacy Regulation in Addressing Coerced Consent and Identifying Loopholes

Given the brief mention of the e-Privacy Regulation[253] in the previous subsection, it is crucial to examine its efficacy in addressing coerced consent and whether any loopholes still exist. In accordance with Article 8 of the proposed e-Privacy Regulation, information may be collected and stored on devices for a variety of purposes, including user permission, transmission requirements, delivering a requested information society service, and service provider online audience measurement.[254]

[251] Ibid.
[252] Ibid.
[253] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 010 final < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 > accessed 5 August 2023.
[254] Article 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)' (Adopted on 4 April 2017) 17/EN WP247 < https://ec.europa.eu/newsroom/article29/items/610140/en > accessed 5 August 2023.

Concerns have been raised since the drafted e-Privacy Regulation omits the terms "strictly" and "explicitly" from Article 5(3) of the e-Privacy regulation, which might enable third-party cookies on data subjects' devices in the name of services that data subjects have requested. In light of the Council's stance on the e-Privacy Regulation, which indicates that data subjects' consent should be requested for third-party cookies and analytics, the terms "strictly necessary" and "specifically" were adopted which is essential to deliver a service.[255]

The use of browser settings for obtaining permission, as envisaged in Article 9 of the e-Privacy Regulation, is deemed inadequate under the GDPR owing to its insufficiency in terms of precision and provision of informative content. The inclusion of this provision has been omitted as demanded by the Council. The proposed e-Privacy Regulation's Article 10 mandates that browsers have the option to refuse third-party cookies, although the word "third party" raises issues since it might refer to first-party websites like social networking platforms. Use of the phrases "site-wide" and "internet-wide" is a substitute. Data subjects must agree to cookie settings when installing browsers as part of the requirement. Browsers may offer data subjects the choice to accept just first-party cookies, reject third-party cookies, or accept or reject all cookies. Similarly, the Council demanded to remove Article 10 from e-Privacy Regulation.[256]

The e-Privacy legislation and its associated rulings suggest that the storage of non-essential cookies should not occur without obtaining consent from data subjects. However, it is important to note that the criteria for obtaining consent differ between the e-Privacy Directive and the proposed e-Privacy Regulation. Although data protection by default is not specifically mentioned in both laws, it could bring data subjects further robust protection in conjunction with the consent requirement outlined in the e-Privacy legislation.[257]

The CJEU concluded that in the case of ***Planet49***,[258] in 2019, merely deselecting a pre-checked tracking cookie notification is insufficient to establish consent under EU law, and that active consent is required for a user to agree to a service provider's usage of cookies. A German company named Planet49 ran an online lottery in 2013 that required participants to share their contact details

[255] Ibid.
[256] Daniela Jezova, 'Principle of Privacy by Design and Privacy by Default' (2020) Regional Law Review < https://ssrn.com/abstract=3755514 > accessed 5 August 2023.
[257] Naithani (n 250).
[258] Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019] ECR I-801.

and consent to data sharing with advertising partners by ticking a checkbox. Another pre-ticked checkbox allowed Planet49 to set tracking cookies on data subjects' online activity which could be unticked without affecting lottery participation, but denying consent to cookies required manual action.[259]

The Court's ruling, in line with Advocate General Szpunar's stance, states that preselected checkboxes cannot constitute valid consent under Articles 2(f) and 5(3) of e-Privacy Directive. They stress the importance of freely given, specific, informed, and unambiguous consent as required by the E-Privacy Directive and data protection regulations. The Court takes a comprehensive approach to the information required to be presented to data subjects before obtaining consent, as stated in Articles 5(3) of the e-Privacy Directive and Article 13 of the GDPR, which necessitates clear and comprehensive details on cookie duration and third-party access.[260]

The decision in this case increases privacy protection in the digital age by extending protections beyond conventional boundaries and reiterating the significance of active consent as per the e-Privacy Directive. Controversial concerns, such the prerequisites for a valid consent and access to websites based on cookie consent, are brought up by the current legislative discussion on the proposed e-Privacy Regulation. Even after the e-Privacy framework revision, the Court's view of active consent would probably be applicable, although further clarity is still required in certain areas, particularly with respect to the disclosure obligations for online identifiers and other tracking methods.[261]

(5.4) Is GDPR sufficient to Address Coerced Consent?

Beyond focusing solely on fines, the true measure of the GDPR's success lies in how it shapes the future of data privacy. While some countries like Germany and France have actively imposed fines and enforced regulations, others, such as Ireland, have been less assertive due to economic

[259] Natascha Gerlach and Elisabeth Macher, 'The Way the Cookie Crumbles: CJEU Clarifies European Data Protection Rules for the Use of Cookies' (*Clearly Gottlieb*, 10 December 2019) < https://www.clearycyberwatch.com/2019/12/the-way-the-cookie-crumbles-cjeu-clarifies-european-data-protection-rules-for-the-use-of-cookies/ > accessed 5 August 2023.
[260] Agnieszka Jabtonowska and Adrianna Michatowicz, 'Planet49: Pre-Ticked Checkboxes Are Not Sufficient to Convey User's Consent to the Storage of Cookies' (2020) 6(1) European Data Protection Law Review 138-139.
[261] Ibid 142.

considerations and the presence of tech giants. This divergence in enforcement approaches could lead to economic disparities among EU member states and impact the overall harmonisation of the GDPR's implementation.[262]

Small businesses may be burdened by the shift from innovation-driven advancement to a future of strict restrictions for each digital product or service, especially with GDPR compliance. Emerging technologies like face detection, machine learning and AI pose challenges to consent-based privacy frameworks like the GDPR and may stifle innovation and development in the IT industry. The GDPR's continued efficacy will be a key determinant of how the field of data privacy develops in the future.[263]

Within an intricate regulatory landscape, there's a clear trend towards imposing more rules on companies, particularly in the digital sector. The Digital Services Act,[264] proposed e-Privacy Regulation,[265] and proposed AI Act[266] are among several GDPR-related legislations that aim to curtail the operational freedom of technology companies. The GDPR's emphasis on transparency of the usage of data subjects' personal information has influenced these regulations, which has revealed problematic practices and driving the push for more rules on companies.[267]

[262] Erin Hilliard, 'The GDPR: A Retrospective and Prospective Look at the First Two Years' (2022) 35 Berkeley Technology Law Journal 1288-1289 < https://btlj.org/wp-content/uploads/2022/01/0012-35-4-Hilliard.pdf > accessed 7 August 2023.
[263] Ibid.
[264] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L277/1.
[265] European Commission (n 253).
[266] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM (2021) 206 final < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 > accessed 6 August 2023.
[267] Hilliard (n 262).

(5.5) Navigating New EU Legislation Addressing Dark Patterns: Challenges and Scope

(5.5.1) *Digital Services Act (DSA)*[268]

The recently passed DSA by the EU targets major internet platforms like Facebook, YouTube, TikTok, and Twitter to combat illicit content and social hazards.[269] Alongside the DMA, these laws establish uniform guidelines for online platforms, fostering accountability and legal harmony across EU Member States.[270] The DSA focuses on creating a transparent online environment and safeguarding data subjects. It targets actions such as protecting minors, countering disinformation, and prohibiting profiling based on sensitive attributes. The DSA empowers users by enabling them to contest platform content through notice-and-choice mechanisms while banning deceptive consent tactics and dark patterns.[271] The legislation covers major platforms with over 45 million European users, bridging gaps in national laws. Additionally, non-legislative measures like the Code of Conduct have been implemented by IT companies to combat unlawful content.[272]

Article 25 of the DSA forbids the utilisation of deceptive design techniques in online interfaces by "online platforms," but it does not extend to other entities within the DSA's scope, leaving some ambiguity in the classification of on-platform games like Candy Crush. Recital 67 and Article 25(2) of the DSA aim to protect users' autonomous decisions and choices by prohibiting practices that manipulate, deceive, distort, impair, nudge, or exploit user decision-making and autonomy. Article 25(2) of the DSA exempts practices covered by the Unfair Commercial Practices Directive (UCPD) or GDPR, raising concerns about its effectiveness in combating dark patterns as many identified dark patterns fall under these existing legislations. UCPD is a consumer law which specifically forbids certain professional practices that might potentially induce consumers to make decisions they might not have made otherwise. Recital 67's ambiguity about the definition of a "neutral

---

[268] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L277/1.
[269] Paivi Korpisaari, 'From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act' (2022) 14(2) Journal of Media Law < https://doi.org/10.1080/17577632.2022.2148335 > accessed 25 July 2023.
[270] Auf Deutsch Lesen, 'A guide to the Digital Services Act, the EU's new law to rein in Big Tech' (*Algorithm Watch*, 21 September 2022) < https://algorithmwatch.org/en/dsa-explained/ > accessed 6 August 2023.
[271] Petteri Kalaoja, 'A Consent and Privacy Management Framework' (Master's Thesis, University of Applied Sciences 2022) < https://www.theseus.fi/bitstream/handle/10024/785039/Kalaoja_Petteri.pdf?sequence=2&isAllowed=y > accessed 25 July 2023.
[272] Korpisaari (n 269).

manner" might result in various ways that dark patterns are interpreted, which would make it difficult to enforce the DSA rules.[273]

(5.5.2) *Digital Markets Act (DMA)*

In order to prevent online platforms or known as 'gatekeepers' from undermining the efficacy of the rule, the DMA adds restrictions that prohibit non-neutral design, presentation, or subversion in their user interfaces. According to the description of dark patterns as deceptive design strategies that harm data subjects, Article 13(6) forbids gatekeepers from reducing the quality of essential platform services based on end-user preferences, guaranteeing fair competition in the online market.[274]

(5.5.3) *Proposal of Data Act*

The Data Act serves as a valuable addition to the GDPR since it offers explicit instructions and recommendations regarding the sharing and portability of data. The primary objective of this initiative is to promote innovation, competitiveness, and public welfare by facilitating increased accessibility and utilisation of data among different parties, while simultaneously safeguarding the privacy and autonomy of individuals.[275]

The Data Act aligns with the GDPR's definition of dark patterns and considers practices that interfere with data subjects' consent in data sharing or portability choices as potential dark patterns, even if they have other legal bases for data processing under Article 6(2)(a) of the proposed Data Act. These may involve complex interfaces, emotional language, or social pressure to hinder data-related choices. For example, offering incentives for unnecessary data sharing could be considered a dark pattern.[276] Third parties receiving data must refrain from using dark patterns or deceptive practices that undermine the data subjects' autonomy or ability to choose through a digital interface,

[273] M R Leiser and Cristiana Santos, 'Dark Patterns, Enforcement, and the emerging Digital Design Acquis - Manipulation beneath the Interface' (2023) < https://ssrn.com/abstract=4431048 > accessed 6 August 2023.
[274] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L265/1.
[275] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM (2022) 68 final < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN > accessed 6 August 2023.
[276] Ibid.

as outlined in Recital 34. This includes avoiding practices that coerce data subjects into disclosing excessive data and ensuring compliance with the GDPR's data minimisation principle.[277]

(5.5.4) *Proposal of AI Act*

The AI Act proposal aims to regulate AI systems' development, marketing, and use in the EU, and it includes provisions that prohibit manufacturers from incorporating dark patterns, such as subliminal techniques or exploiting vulnerabilities of specific groups, into their AI systems.[278]

The proposed AI Act prohibits the use of dark patterns in AI systems under Article 5(1)(a) and (b), which prevent manipulation techniques causing harm and exploitation of vulnerable groups.[279] Subliminal methods are covered under Article 5(1)(a) of the AI Act, however there is disagreement over their effectiveness among researchers such as Franklin[280] and Uuk.[281] The suggestion addresses the negative effects that manipulative AI systems may have physically or psychologically, but it should also take into account other negative effects on society, autonomy, addiction and time[282] as well as broader scope of manipulation methods should be used in lieu of subliminal approaches.[283]

Article 5(1)(b) of the AI Act forbids AI practices that prey on the flaws of certain groups, however it is critical to understand that when people are targeted for vulnerability, everyone is susceptible.[284] Although there is presently no convincing evidence to suggest that personalised dark patterns are used widely, this may change when machine learning, AI, and data collecting all come together.[285] The European Commission recognises the lack of study on personalised dark

[277] Leiser and Santos (n 273).
[278] European Commission (266).
[279] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22(4) Computer Law Review International < https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf > accessed 6 August 2023.
[280] Matija Franklin (eds), 'Missing Mechanisms of Manipulation in the EU AI Act' (2022) 35 The International FLAIRS Conference Proceedings < https://journals.flvc.org/FLAIRS/article/view/130723 > accessed 6 August 2023.
[281] Risto Uuk, 'Manipulation and the AI Act' (*The Future of Life Institute*, 18 January 2022) < https://futureoflife.org/wp-content/uploads/2022/08/FLI-Manipulation_AI_Act.pdf > accessed 6 August 2022.
[282] Franklin (n 280).
[283] Uuk (n 281).
[284] Franklin (n 280).
[285] Organisation for Economic Co-operation and Development (OECD) Committee on Consumer Policy, 'Dark Commercial Patterns' (2022) 336 OECD Digital Economy Papers < https://www.oecd-ilibrary.org/deliver/44f5e846-en.pdf?itemId=/content/paper/44f5e846-en&mimeType=pdf > accessed 6 August 2023.

patterns and advises looking into other customisation strategies without intrusive collecting of data or vulnerability exploitation.[286]

The recent introduction of the EU's legislative measures such as the DSA, DMA, proposal of e-Privacy Regulation, Data Act and AI Act, reflects a proactive approach to addressing the pervasive challenge of dark patterns. However, these regulations are still relatively new and the limited existing case law raises uncertainties about their ability to effectively complement the established GDPR and e-Privacy Directive in addressing coerced consent and deceptive design. Despite these efforts, the persistence of coerced consent, exemplified by recent fines imposed on major companies for employing deceptive tactics, underscores the ongoing nature of the issue.

These fines demonstrate that existing laws are indeed having an impact in holding companies accountable for their actions. As such, the effectiveness of the new proposed regulations lies in their potential to further strengthen these legal frameworks and enhance their ability to combat dark patterns. The path ahead requires careful observation and assessment to ascertain whether these new regulations will effectively contribute to reducing such practices. Patience is essential as we await the maturation of these regulations and their impact on the landscape of deceptive design, ensuring that the legal measures in place truly address and mitigate these concerns.

CONCLUSION FOR CHAPTER 5

In the realm of digital interactions, the challenge is to secure genuine users' consent while countering manipulative design practices known as dark patterns. Despite the effectiveness of the GDPR in raising data protection standards and enforcing fines for breaches, the persistent use of exploitative tactics highlights the ongoing need for action. The GDPR has introduced crucial concepts like the "right to explanation" and "privacy by default," yet challenges arise from algorithmic decisions and inconsistent enforcement.

With the introduction of regulations such as the e-Privacy Regulation, DSA, and AI Act, the landscape is evolving to enhance transparency, safeguard user autonomy, and curb manipulative

[286] European Commission, 'Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation' (2022) Publications Office of the European Union < https://data.europa.eu/doi/10.2838/859030 > accessed 6 August 2023.

strategies. However, the full impact of these new regulations on reducing dark patterns and ensuring true consent is still unfolding. As technology and user behaviour evolve, refining and adapting regulations remains vital to cultivate an ethical digital realm that prioritises privacy and user empowerment.

CHAPTER 6: CONCLUSION

In conclusion, this research has navigated the intricate landscape of coerced consent within the digital services realm, drawing insights from various aspects of the European Union's regulatory framework. The journey embarked upon in this study has illuminated the multifaceted ethical, legal, and practical implications surrounding coerced consent, shedding light on the challenges posed by manipulation, limited choices, and deceptive practices.

In alignment with the research's overarching objectives, several key findings have emerged. Chapter 2 underscored the ethical and legal dimensions of consent, revealing the complexity and significance of this concept in the digital age. It became evident that the digital realm necessitates reevaluating the traditional understanding of consent to align with the contemporary digital landscape.

In Chapter 3, the focus shifted to the EU's legal framework for consent. Through an in-depth analysis of the GDPR and related legislations, this chapter scrutinised the requirements for valid consent, particularly in the context of data protection and cookies. Real-world case studies underscored the challenges of securing informed consent in the dynamic digital environment.

Chapter 4 delved into the intricacies of consent practices and identified loopholes within EU regulations. The examination extends to practices hindering personal autonomy, lacking transparency, and limiting user choices. Dark patterns and their implications are scrutinised, highlighting not only the ethical concerns but also the violation of regulations stemming from deceptive designs.

Chapter 5 underscored the importance of an adaptable regulatory framework to address the dynamics of rapidly advancing technology while preserving individual rights. This research observed that while regulatory measures are in place, continuous effort is required to ensure that evolving digital practices are met with suitable governance.

(6.1) Strengths and Contributions

This research embodies several strengths that enhance its credibility and value. A robust literature review forms the bedrock of the study, showcasing a deep understanding of consent, data privacy and regulatory frameworks. The research objectives are well-articulated, providing a clear

roadmap for the study. By adopting a multi-disciplinary approach, combining both doctrinal and socio-legal analyses, the research offers an extensive view of the subject matter. The incorporation of in-depth legal analysis, including regulations, case law and policy documents, bolsters the research's credibility. Additionally, the socio-legal insights, drawn from real-world cases and user experiences, provide a practical perspective on consent's impact. The structured framework, organised into distinct chapters, facilitates systematic exploration and comprehension. Ultimately, the research's contribution to the discourse on data privacy and consent lies in its critical examination of coerced consent's ethical, legal and societal dimensions.

(6.2) Limitations and Future Directions

However, this research is not without limitations. The complexity of the subject and word count constraints lead to a trade-off between depth and comprehensiveness. The novelty of regulations like the Digital Services Act, Digital Markets Act, proposed regulations of the Data Act and AI Act, coupled with their pending implementation, restricts a comprehensive evaluation of their functionality. Rapid developments in the digital landscape could impact the timeliness of findings. The EU-centric focus may limit the generalisability of findings to a global context, and while the research acknowledges ethical implications, it might benefit from deeper exploration. By acknowledging these strengths and weaknesses, the research paves the way for future improvements, suggesting avenues for more in-depth explorations, and a more global perspective on the challenges of coerced consent and data privacy. Looking ahead, these findings invite future avenues of exploration. For instance, the implications of coerced consent on specific digital contexts, such as social media, could warrant further investigation.

In summary, this research has charted a course through the intricate terrain of coerced consent, contributing insights that resonate with both the wider literature and practical concerns. By addressing the complexities of consent in the digital age and identifying challenges within regulatory frameworks, this study not only expands theoretical understanding but also guides practical policy considerations. As digital interactions continue to evolve, this research stands as a foundational cornerstone in the ongoing journey to ensure ethical, informed, and meaningful consent within the dynamic landscape of the digital era.

[19989 words]

BIBLIOGRAPHY

Primary sources:

European Union legal sources

Article 29 Data Protection Working Party, 'Cookie Sweep Combined Analysis – Report (Adopted on 3 February 2015) 14/EN WP 229 < https://ec.europa.eu/newsroom/article29/items/640605 > accessed 16 July 2023.

Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' 17/EN WP260 < https://ec.europa.eu/newsroom/article29/items/622227/en > accessed 8 August 2023.

Article 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)' (Adopted on 4 April 2017) 17/EN WP247 < https://ec.europa.eu/newsroom/article29/items/610140/en > accessed 5 August 2023.

Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption' (Adopted on 7 June 2012)00879/12/EN WP 194 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf > accessed 24 July 2023.

Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices' (adopted on 16 May 2011) 881/11/EN WP185 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf > accessed 29 July 2023.

Article 29 Data Protection Working Party, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (Adopted on 2 October 2013) 1676/13/EN WP 208 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf > accessed 8 August 2023.

Article 29 Data Protection Working Party, 'Working Document: Privacy on the Internet - An Integrated EU Approach to On-Line Data Protection' (adopted on 21 November 2000) 5063/00/EN/FINAL WP 37 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf > accessed 16 July 2023.

Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent', (adopted on 13 July 2011) 01197/11/EN WP 187 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf > accessed 8 August 2023.

Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent', (adopted on 13 July 2011) 01197/11/EN WP 187 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf > accessed 8 August 2023.

Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent', (adopted on 13 July 2011) 01197/11/EN WP 187 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf > accessed 8 August 2023.

Data Protection Commission welcomes latest successful prosecution of Marketing Offences' (Data Protection Commission, 5 December 2022) < https://www.dataprotection.ie/en/news-media/data-protection-commission-welcomes-latest-successful-prosecution-of-marketing-offences#:~:text=Guerin%20Media%20Limited%20pleaded%20guilty,Statutory%20Instrument%20336%20of%202011 > accessed 7 August 2023.

European Commission, 'Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation' (2022) Publications Office of the European Union < https://data.europa.eu/doi/10.2838/859030 > accessed 6 August 2023.

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 010 final < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 > accessed 5 August 2023.

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM (2021) 206 final < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 > accessed 6 August 2023.

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM (2022) 68 final < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN > accessed 6 August 2023.

European Data Protection Board (EDPB), 'Guidelines 05/2020 on consent under Regulation 2016/679' (Adopted on 4 May 2020) < https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf > accessed 10 July 2023.

European Data Protection Board, 'Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them' (Adopted on 14 March 2022) < https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf > accessed 1 August 2023.

European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (Adopted on 20 October 2020) < https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf > accessed 4 August 2022.

Organisation for Economic Co-operation and Development (OECD) Committee on Consumer Policy, 'Dark Commercial Patterns' (2022) 336 OECD Digital Economy Papers < https://www.oecd-ilibrary.org/deliver/44f5e846-en.pdf?itemId=/content/paper/44f5e846-en&mimeType=pdf > accessed 6 August 2023.

(EU legislation)

Charter of Fundamental Rights of the European Union, [2000] OJ C364/1.

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

Council of Europe Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L201/37.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L281/31.

European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, S.I. No. 336/2011.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119/1.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L265/1.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L277/1.

(Judgments of the European Court of Justice and General Court)

Case C-131/12 *Google Spain v Agencia Española de Protección de Datos and Mario Costeja González* [2014] ECR I-317.

Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] ECR I-388.

Case C-252/2 Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 22 April 2021 - *Meta Platforms Inc.and Others v Bundeskartellamt* [2021]

OJ C320/16 < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CN0252 > accessed 8 August 2023.

Case C-252/21 *Meta Platforms and Others v Bundeskartellamt* [2023] ECR I-537.

Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland* [2011] ECR I-3441.

Case C-61/19 *Orange Romania SA v Autoritatea Naţionala de Supraveghere a Prelucrarii Datelor cu Caracter Personal* [2020] ECR I-901.

Case C-61/19 *Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal* [2020] ECR I-158, Opinion of Advocate General Szpunar < https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62019CC0061 > accessed 31 July 2023.

Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019] ECR I-801.

Court of Justice of the European Union, 'Press Release No 137/20 Judgment in Case C-61/19 *Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării* Datelor cu Caracter Personal (ANSPDCP)' (11 November 2020) < https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-11/cp200137en.pdf > accessed 22 July 2023.

Cases, Legislation and legal sources (from other jurisdictions)

(Cases)

Agencia Española de Protección de Datos, Procedimiento PS/00187/2019 (Spain).

Datatilsynet, 2018-32-0357, *DMI's behandling af personoplysninger om hjemmesidebesøgende.* (Denmark).

Datatilsynet, Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS' behandling af personoplysninger om hjemmesidebesøgende, 2021-431-0125, 20 October 2021 (Denmark).

Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC (France).

Deliberation of the Restricted Committee SAN-2020-012 of 07 December 2020 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED (France).

Deliberation of the Restricted Committee SAN-2020-013 of 07 December 2020 concerning AMAZON EUROPE CORE. (France).

Deliberation of the Restricted Committee SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED. (France).

Gillick v West Norfolk and Wisbech Area Health Authority [1986] AC 112 (HL) (UK).

Landgericht Rostock, 3 O 762/19, 15 September 2020 (Germany).

(Legislation)

Data Protection Act 1984 (UK).

Federal Data Protection Act 1977 (Bundesdatenschutzgesetz, BDSG) (Germany).

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. (France).

(Legal sources)

Spanish Data Protection Authority (AEPD), 'Guidelines for Data Protection by Default' (2020) < https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto-en.pdf > accessed 4 August 2023. (Spain).

The President's Council of Advisors on Science and Technology (PCAST), 'Report to the President Big Data and Privacy: A Technological Perspective' (May 2014) < https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf > accessed 29 July 2023 (US).

Secondary sources

Books

Beauchamp T, 'Autonomy and consent' in Miller F and Wertheimer A, *The Ethics of Consent: Theory and Practice* (Oxford University Press 2009).

Beyleveld D and Brownsword R, *Consent in the Law* (Bloomsbury Publishing 2007).

Bloustein E J and Pallone N J, *Individual and Group Privacy* (Routledge 2017).

Borgesius F Z, *Behavioural Targeting', Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International 2015).

Collins H, *The Law of Contract* (Cambridge University Press 2003).

Cooter R and Ulen T, *Law and Economics* (6th edn, Pearson 2012).

Faden R R and Beauchamp T L, *A History and Theory of Informed Consent* (Oxford University Press 1986).

IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide* (4th edn, ITGP 2020).

Koulu R, *Dispute Resolution and Technology: Revisiting the Justification of Conflict Management* (COMI 2016).

Littman M and Ruck P C*, Privacy and the Law* (Stevens and Sons Limited 1970).

Markou C, 'Behavioural Advertising and the New "EU Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination' in Gutwirth S, Leenes R and P Hert P D, *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016).

Miller F and Wertheimer A, *The Ethics of Consent: Theory and Practice* (Oxford University Press 2009).

Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

Rawls J, *Political Liberalism* (Columbia University Press 2005).

Reed A and Bohlander M (eds), *Consent: Domestic and Comparative Perspectives* (Routledge 2017).

Reinhardt J, 'Realizing the Fundamental Right to Data Protection in a Digitized Society' in Albers M and Sarlet I W (eds), *Personality and Data Protection Rights on the Internet* (Springer 2022).

Siegel E, *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die* (Wiley 2013).

Voigt P and Bussche A V D, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (Springer 2017).

Journals and Articles

Acquisti A (eds), 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 50(3) ACM Computer Survey < https://dl.acm.org/doi/pdf/10.1145/3054926 > accessed 31 July 2023.

Acquisti A, Brandimarte L and Loewenstein G, 'Privacy and human behavior in the age of information' (2015) 347(6221) Science < https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.pdf > accessed 28 July 2023.

Alexander L, 'The ontology of consent. Analytic Philosophy' (2014) Legal Studies Research Paper 14/137.

Andreotta A J, Kirkham N and Rizzi M, 'AI, big data, and the future of consent' (2022) 37 AI and Society < https://doi.org/10.1007/s00146-021-01262-5 > accessed 27 July 2023.

Barocas S and Nissenbaum H, 'Big Data's End Run Around Procedural Privacy Protections' (2014) 57(11) Communications of the ACM.

Betzing J H (eds), 'The impact of transparency on mobile privacy decision making' (2019) 30(6) Electronic Markets < https://www.researchgate.net/publication/330936528_The_impact_of_transparency_on_mobile_privacy_decision_making > accessed 27 July 2023.

Borgesius F Z, 'Informed Consent: We Can Do Better to Defend Privacy' (2015) 13 IEEE Security Privacy.

Breen S, Ouazzane K and Patel P, 'GDPR: Is your consent valid?' (2020) 37(1) Business Information Review < https://doi.org/10.1177/0266382120903254 > accessed 13 June 2023.

Brkan M, Claes M and Rauchegger C, 'European fundamental rights and digitalization' (2020) 27(6) Maastricht Journal of European and Comparative Law < https://doi.org/10.1177/1023263X20983778 > accessed 7 July 2023.

Bygrave L A, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) Oslo Law Review < https://ssrn.com/abstract=3035164 > accessed 4 August 2023.

Carmi E, 'Review: Cookies – More than Meets the Eye' (2017) 34(7-8) Theory, Culture and Society < https://doi.org/10.1177/0263276417736367 > accessed 16 July 2023.

Cate F H, 'The Limits of Notice and Choice' (2010) 8(2) IEEE Security and Privacy.

Chartrand T L, 'The role of conscious awareness in consumer behavior. Journal of Consumer Psychology' (2005) 15(3) Journal of Consumer Psychology 203–210 < https://people.duke.edu/~tlc10/bio/TLC_articles/2005/Chartrand_2005.pdf > accessed 27 July 2023.

Clifford D, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the Crumbs of Online User Behaviour' (2014) 5 JIPITEC < https://www.jipitec.eu/issues/jipitec-5-3-2014/4095 > accessed 16 July 2023.

Cohen J E, 'Turning Privacy Inside Out' (2019) 20(1) Theoretical Inquiries in Law < https://www7.tau.ac.il/ojs/index.php/til/article/view/1607/1709 > accessed 8 July 2023.

Cranor L F, 'Necessary but not sufficient: Standardized mechanisms for privacy notice and choice' (2012) 10(2) Journal on Telecommunications and High Technology Law < http://www.jthtl.org/content/articles/V10I2/JTHTLv10i2_Cranor.PDF > accessed 27 June 2023.

Custers B (eds) 'Consent and Privacy' (2019) < https://ssrn.com/abstract=3383465 > accessed 7 July 2023.

Custers B (eds), 'Informed Consent in Social Media Use - The Gap between User Expectations and EU Personal Data Protection Law' (2013) 10(4) Scripted < https://ssrn.com/abstract=3047134 > accessed 8 July 2023.

Dougherty T, 'Yes Means Yes: Consent as Communication' (2011) 43(3) Philosophy and Public Affairs < https://philpapers.org/archive/DOUYMY.pdf > accessed 8 August 2023.

Ducuing C, Schroers J and Kindt E, 'The Wirtschaftsakademie Fan Page Decision: A Landmark on Joint Controllership - A Challenge for Supervisory Authorities Competences' (2018) 4(4) European Data Protection Law Review.

Dumortier J, 'Evaluation and Review of the ePrivacy Directive (2016) 2(2) European Data Protection Law Review.

Duque O V, 'Cookies and The Illusion of Informed Consent: The Framing of The Decision Environment as Digital Manipulation' (2021) < https://ssrn.com/abstract=3957528 > accessed 2 August 2023.

Eberlein B and Newman A, 'Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union' (2008) 21(1) < https://doi.org/10.1111/j.1468-0491.2007.00384.x > accessed 8 August 2023.

Edenberg E and Jones M L, 'Analyzing the legal roots and moral core of digital consent' (2019) 21(8) New Media and Society < https://journals.sagepub.com/doi/pdf/10.1177/1461444819831321 > accessed 27 June 2023.

Edwards L and Abel W, 'The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services' (2014) CREATe Working Paper 2014/15 < https://doi.org/10.5281/zenodo.12506 > accessed 3 August 2023.

Edwards L and Veale M, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (2018), 16(3) IEEE Security and Privacy < https://doi.org/10.1109/MSP.2018.2701152 > accessed 26 July 2023.

Edwards L and Veale M, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For' (2017) 16(1) Duke Law and Technology Review < https://scholarship.law.duke.edu/dltr/vol16/iss1/2 > accessed 3 August 2023.

Goicovici J, 'Granularity and Specificity of Consent and Implications Thereof for the Data Controller in the Light of the Principle of 'Purpose Limitation'' (2022) 9(2) InterEULawEast < https://hrcak.srce.hr/file/424613 > accessed 22 July 2023.

Goodman B and Flaxman S, 'European Union regulations on algorithmic decision-making and a ''Right to Explanation''' (2017) 38(3) AI Magazine < https://doi.org/10.1609/aimag.v38i3.2741 > accessed 3 August 2023.

Grafenstein M V (eds), 'Effective Regulation through Design - Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking Technologies in Personalised Internet Content and the Data Protection by Design Approach' (2021) < https://ssrn.com/abstract=3945471 > accessed 4 August 2023.

Hartzog W, 'The Case Against Idealising Control' (2018) 4 European Data Protection Law Review 425 < https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4050&context=faculty_scholarship > accessed 8 August 2023.

Hartzog W, 'The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?' (2010) 15(4) Communication Law and Policy < https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4539&context=faculty_scholarship > accessed 8 August 2023.

Hartzog W, 'Website Design as Contract'(2011) 60(6) American University Law Review < https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1617&context=aulr&httpsredir=1&referer= > accessed 4 July 2023.

Hilliard E, 'The GDPR: A Retrospective and Prospective Look at the First Two Years' (2022) 35 Berkeley Technology Law Journal 1288-1289 < https://btlj.org/wp-content/uploads/2022/01/0012-35-4-Hilliard.pdf > accessed 7 August 2023.

Hof S V D, 'I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2017) 34(2) Winsconsin International Law Journal < https://wilj.law.wisc.edu/wp-content/uploads/sites/1270/2017/12/van-der-Hof_Final.pdf > accessed 14 July 2023.

Hoofnagle C J and Urban J M, 'Alan Westin's Privacy Homo Economicus' (2014) 49 Wake Forest Law Review < https://ssrn.com/abstract=2434800 > accessed 3 August 2023.

Hoofnagle C J, Sloot B V D and Borgesius F Z, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28(1) Information & Communications Technology Law < https://ssrn.com/abstract=3254511 > accessed 8 August 2023.

Hopkins R, 'The CJEU's Facebook Fan Page Judgment: Joint Data Controllers, Cookies and Targeted Advertising' (2018) 2(5) International Journal for the Data Protection Officer, Privacy Officer & Privacy Counsel.

Hovinheimo S L, "Who controls our data? The legal reasoning of the European Court of Justice in Wirtschaftsakademie Schleswig-Holstein and Tietosuojavaltuutettu v Jehovan todistajat" (2019) 28 (2) Information and Communications Technology Law < https://doi.org/10.1080/13600834.2019.1623447 > accessed 22 July 2023.

Hurd H M, 'The moral magic of consent' (1996) 2(2) Legal Theory.

Hyams K, 'When Consent Doesn't Work: A Rights-Based Case for Limits to Consent's Capacity to Legitimise' (2011) 8(1) Journals of Moral Philosophy.

Jabtonowska A and Michatowicz A, 'Planet49: Pre-Ticked Checkboxes Are Not Sufficient to Convey User's Consent to the Storage of Cookies' (2020) 6(1) European Data Protection Law Review.

Jasmontaite L (eds), 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4(2) European Data Protection Law Review < https://par.nsf.gov/servlets/purl/10081980 > accessed 4 August 2023.

Jezova D, 'Principle of Privacy by Design and Privacy by Default' (2020) Regional Law Review < https://ssrn.com/abstract=3755514 > accessed 5 August 2023.

Kaiser E, 'The Concept of 'Freely Given, Specific and Informed' Consent under the Scrutiny of the European Court of Justice' (2020) 6(4) European Data Protection Law Review.

Korpisaari P, 'From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act' (2022) 14(2) Journal of Media Law < https://doi.org/10.1080/17577632.2022.2148335 > accessed 25 July 2023.

Kosta E, 'Peeking into the cookie jar: the European approach towards the regulation of cookies' (2013) 21(4) International Journal of Law and Information Technology < https://ssrn.com/abstract=2675810 > accessed 8 August 2023.

Leiser M R and Santos C, 'Dark Patterns, Enforcement, and the emerging Digital Design Acquis - Manipulation beneath the Interface' (2023) < https://ssrn.com/abstract=4431048 > accessed 6 August 2023.

Lynskey O, ‘Deconstructing data protection: The ‘‘added-value’’ of a right to data protection in the EU legal order’, (2014) 63(3) International and Comparative Law Quarterly, < http://eprints.lse.ac.uk/57713/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Lynskey%2C%20O_Lynskey_Deconstructing_data_protection_2014_Lynskey_Deconstructing_data_protection_2014.pdf > accessed 7 July 2023.

Mahieu R, Hoboken J V and Asghari H, ‘Responsibility for Data Protection in a Networked World: On the Question of the Controller, Effective and Complete Protection and Its Application to Data Access Rights in Europe’ (2019) 10(1) Journal of Intellectual Property, Information Technology and Electronic Commerce Law.

Manson N C, ‘Permissive consent: a robust reason-changing account’ (2016) Philosophical Studies: An International Journal for Philosophy in the Analytic Tradition.

Martínez D F M, ‘Unification of Personal Data Protection in the European Union: Challenges and Implications' (2018) 27(1) El profesional de la información < http://www.elprofesionaldelainformacion.com/contenidos/2018/ene/17_esp.pdf > accessed 8 July 2023.

McDonald A M and Cranor L F, ‘The Cost of Reading Privacy Policies’ (2008) 4(3) Journal of Law and Policy for the Information Society < https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1&isAllowed=y > accessed 28 July 2023.

Naithani P, ‘Curtailing the Cookie Monster through Data Protection by Default’ (2022) 27(1) Tilburg Law Review < https://doi.org/10.5334/tilr.311 > accessed 4 August 2023.

Nissenbaum H, ‘A Contextual Approach to Privacy Online’ (2011) 140(4) Daedalus < http://ssrn.com/abstract=2567042 > accessed 3 August 2023.

Ooijen I V and Vrabec H U, ‘Does the GDPR Enhance Consumers’ Control over Personal Data? An Analysis from a Behavioural Perspective’ (2019) 42 Journal of Consumer Policy < https://link.springer.com/article/10.1007/s10603-018-9399-7 > accessed 27 July 2023.

Park Y J, ‘Digital Literacy and Privacy Behavior Online’ (2011) 40(2) Communication Research < https://doi.org/10.1177/0093650211418338 > accessed 27 July 2023.

Pasha S B (eds), ‘EU Law Perspectives on Location Data Privacy in Smartphones’ (2016) 2(3) European Data Protection Law Review.

Richards N and Hartzog W, ‘Privacy's Trust Gap’ (2017) 126 The Yale Law Journal < https://ssrn.com/abstract=2899760 > accessed 8 August 2023.

Richards N and Hartzog W, 'The Pathologies of Digital Consent' (2019) 96 Washington University Law Review < https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview > accessed 13 June 2023.

Santos C, Bielova N, and Matte C, 'Are cookie banners Indeed Compliant with the Law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners' (2020) Technology and Regulation 72-73 < https://doi.org/10.26116/techreg.2020.009 > accessed 1 August 2023.

Schwartz A and Scott R E, 'Contract Theory and the Limits of Contract Law' (2003) 113 Yale Law Journal < https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1467&context=faculty_scholarship > accessed 2 August 2023.

Tsai J Y (eds), 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study' (2011) 22 Information Systems Research < https://www.researchgate.net/publication/220079706 > accessed 28 July 2023.

Veale M and Borgesius F Z, 'Demystifying the Draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22(4) Computer Law Review International < https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf > accessed 6 August 2023.

Westin A F, 'Privacy and Freedom' (1968) 25(1) Washington and Lee Law Review.

Working Paper

Ausloos J (eds), 'Guidelines for Privacy-Friendly Default Settings' ICRI Working Paper 12/2013 < https://dx.doi.org/10.2139/ssrn.2220454 > accessed 3 August 2023.

Conference Papers

Dimova Y (eds), 'Tracking the Evolution of Cookie-based Tracking on Facebook' (Proceedings of the 21st Workshop on Privacy in the Electronic Society, Los Angeles, November 2022) < https://lepoch.at/files/facebook-cookie-tracking-wpes22.pdf > accessed 1 August 2023.

Franklin M (eds), 'Missing Mechanisms of Manipulation in the EU AI Act' (2022) 35 The International FLAIRS Conference Proceedings < https://journals.flvc.org/FLAIRS/article/view/130723 > accessed 6 August 2023.

Gray C M (eds), 'Dark Paterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective' (Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, May 2021) < https://dl.acm.org/doi/pdf/10.1145/3411764.3445779 > accessed 30 July 2023.

Inglesant P and Sasse M A, 'The True Cost of Unusable Password Policies: Password Use in the Wild' (Proceedings of the 28th International Conference on Human Factors in Computing Systems, Atlanta, April 2010) < https://www.researchgate.net/publication/221517955_The_true_cost_of_unusable_password_policies > accessed 29 July 2023.

Jenson C and Potts C, 'Privacy policies as decision-making tools: An evaluation of online privacy notices' (Proceedings of the 2004 Conference on Human Factors in Computing Systems Vienna, April 2004) < https://www.researchgate.net/publication/221515790 > accessed 27 July 2023.

Kirkman D, Vaniea K and Woods D W, 'Dark Dialogs: Automated detection of 10 dark patterns on cookie dialogs' (2023 IEEE 8th European Symposium on Security and Privacy, Delft, July 2023) < https://www.danielwoods.info/assets/pdf/KVW_DarkDialogs_EuroSnP.pdf > accessed 30 July 2023.

Reding V, Vice President of the European Commission and EU Justice Commissioner, 'Your data, your rights: Safeguarding your privacy in a connected world' (Speech at the World Privacy Platform "The review of the EU data protection framework", Brussels, 16 March 2011) < https://europa.eu/rapid/press-release_SPEECH-11-183_en.pdf > accessed 8 July 2023.

Schaub F (eds), 'A Design Space for Effective Privacy Notices' (Symposium on Usable Privacy and Security, Ottawa, July 2015) < https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf > accessed 28 July 2023.

Schwartz P M and Solove D, 'Notice and Choice: Implications for Digital Marketing to Youth' (The Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children, Berkeley, June 2009) < https://www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf > accessed 29 July 2023.

Sorenson J and Kosta S, 'Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites' (Proceedings of the World Wide Web Conference, San Francisco, May 2019) < https://www.researchgate.net/publication/330997511_Before_and_After_GDPR_The_Changes_in_Third_Party_Presence_at_Public_and_Private_European_Websites > accessed 2 August 2023.

Tan J (eds), 'The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior' (Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, April 2014) < https://www.researchgate.net/publication/266655816 > accessed 28 July 2023.

Theses

From A, 'Cookie Consents and Notices under the EU Data Protection Framework' (Master's Thesis, University of Helsinki 2020) < https://helda.helsinki.fi/bitstream/handle/10138/317229/From_Alexandra_Thesis_2020.pdf?sequence=3&isAllowed=y > accessed 21 June 2023.

Kalaoja P, 'A Consent and Privacy Management Framework' (Master's Thesis, University of Applied Sciences 2022) < https://www.theseus.fi/bitstream/handle/10024/785039/Kalaoja_Petteri.pdf?sequence=2&isAllowed=y > accessed 25 July 2023.

Khandekar C, 'Cookie Security and its Implementation in the Light of GD-PR and E-Privacy Regulation' (Master's Thesis Tallinn University of Technology 2019) < https://digikogu.taltech.ee/en/Download/aaccb661-fa99-4c2b-9ecd-04f9df4c4a18 > accessed 17 July 2023.

Korpisaari P, 'From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act' (2022) 14(2) Journal of Media Law < https://doi.org/10.1080/17577632.2022.2148335 > accessed 25 July 2023.

Meskenaite G, 'An examination of the criteria for valid consent under the GDPR in the light of the rationale and technological neutrality'(Master's Thesis, Lund University 2022) < https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9096679&fileOId=9099573 > accessed 10 July 2023.

Oostveen M A A, 'Protecting Individuals Against the Negative Impact of Big Data: The Potential and Limitations of the Privacy and Data Protection Law Approach' (PHD Thesis, University of Amsterdam 2018). < https://pure.uva.nl/ws/files/21397315/Thesis_complete_.pdf > accessed 26 July 2023.

Rasilainen S, 'Valid Consent and Purpose Limitation Principle under the Eu General Data Protection Regulation' (Bachelor's Thesis, Tallinn University of Technology 2020) < https://digikogu.taltech.ee/en/Download/2c0349ba-4011-4b52-9ff0-3ab92736474d > accessed 10 July 2023.

Rossi J, 'Data Protection and Right to Privacy. Investigating the Contested Notion of "Personal Data"' (PhD thesis, Université de Technologie de Compiègne 2020) < http://julienrossi.com/these/Julien%20Rossi%20-%20PhD%20Summary%20FINAL.pdf > accessed 26 June 2023.

Varisco R A J, 'Cookies in the European Data Protection Framework' (Master's Thesis, University of Oslo 2018) < https://www.duo.uio.no/bitstream/handle/10852/67266/Thesis-Completed.pdf?sequence=1&isAllowed=y > accessed 16 July 2023.

Websites and blogs

Bitiukova N, 'Danish DPA zooms in on the cookie consent banner design and peeks into the ePrivacy and GDPR relationship' (*LinkedIn*, 18 February 2020) < https://www.linkedin.com/pulse/danish-dpa-zooms-cookie-consent-banner-design-peeks-bitiukova > accessed 7 August 2023.

Cordier T D and Dubuisson T, 'EU Court of Justice clarifies concept of "informed consent" for collection of personal data' (*Lexology*, 17 November 2020) < https://www.lexology.com/library/detail.aspx?g=6cf3217e-e687-4b5d-97f0-d2107e6ff7e7 > accessed 23 July 2023.

Dr Brignull H, Deceptive Patterns < https://www.deceptive.design/ > accessed 4 July 2023.

Gerlach N and Macher E, 'The Way the Cookie Crumbles: CJEU Clarifies European Data Protection Rules for the Use of Cookies' (*Clearly Gottlieb*, 10 December 2019) < https://www.clearycyberwatch.com/2019/12/the-way-the-cookie-crumbles-cjeu-clarifies-european-data-protection-rules-for-the-use-of-cookies/ > accessed 5 August 2023.

Lesen A D, 'A guide to the Digital Services Act, the EU's new law to rein in Big Tech' (*Algorithm Watch*, 21 September 2022) < https://algorithmwatch.org/en/dsa-explained/ > accessed 6 August 2023.

PEW Research Center, 'The State of Privacy in Post-Snowden America', (2016) < https://www.pewresearch.org/short-reads/2016/09/21/the-state-of-privacy-in-america/ > accessed 29 June 2023.

Sherman J, 'Privacy and Consent: The Heart of the Cambridge Analytica Scandal' (*Venafi*, 2 April 2018) < https://venafi.com/blog/privacy-and-consent-heart-cambridge-analytica-scandal/ > accessed 27 July 2023.

Shore J and Steinman J, 'Did You Really Agree to That? The Evolution of Facebook's Privacy Policy' (*Technology Science*, 10 August 2015) < https://techscience.org/a/2015081102/ > accessed 27 July 2023.

Tytunovich G, 'The Privacy Compliance Gap: How Lack Of Consent Enforcement Is Exposing Brands To Millions In Fines And Penalties' (*Forbes*, 19 December 2022) < https://www.forbes.com/sites/forbestechcouncil/2022/12/19/the-privacy-compliance-gap-how-lack-of-consent-enforcement-is-exposing-brands-to-millions-in-fines-and-penalties/ > accessed 29 July 2023.

Uuk R, 'Manipulation and the AI Act' (*The Future of Life Institute*, 18 January 2022) < https://futureoflife.org/wp-content/uploads/2022/08/FLI-Manipulation_AI_Act.pdf > accessed 6 August 2022.

What is a Flash Cookies?' (*CookiePro*, 2 June 2020) < https://www.cookiepro.com/knowledge/what-is-a-flash-cookie/ > accessed 8 August 2023.

Newspaper article

Palazzo C, 'Consumer campaigners read terms and conditions of their mobile phone apps... all 250,000 words' *The Telegraph* (Sydney, 26 May 2016) < https://www.telegraph.co.uk/technology/2016/05/26/consumer-campaigners-read-terms-and-conditions-of-their-mobile-p/ > accessed 27 July 2023.