Security, Privacy & Usability in Modern Web Services

A dissertation submitted for the degree of
Doctor of Philosophy

By:

Ashley Sheil

Under the supervision of:

Prof. David Malone

Department of Mathematics and Statistics
National University of Ireland Maynooth
Ollscoil na hÉireann, Má Nuad

December 2023

Declaration

I hereby declare that I have produced this manuscript without the prohibited assistance of any third parties and without making use of aids other than those specified.

This thesis has been prepared in accordance with the PhD regulations of Maynooth University and is subject to copyright. For more information see PhD Regulations (December 2022).

The thesis work was conducted from October 2019 to December 2023 under the supervision of Professor David Malone in the department of Mathematics and Statistics, Maynooth University. This research was conducted with the financial support of Science Foundation Ireland under Grant number 18/CRT/6222.

Maynooth, Ireland,

4th December 2023

Acknowledgement

Thanks first and foremost to my supervisor Professor David Malone. I am sure I am not the first PhD candidate to give you a glowing review of your mentorship and I won't be the last. I am so grateful for your guidance and confidence to allow me to meander slightly and find my own feet. You have a gift for knowing what my strengths and interests are. And I always enjoyed our weekly meetings, which I know not many PhD candidates can say.

Thanks to the SFI Advance CRT who provided huge support and enthusiasm for our progress as individual researchers. Being part of a cohort felt like having another family. It made the PhD experience less isolating and especially helped during the COVID-19 lockdown. Thanks also to Professor Deirdre Desmond who guided the Maynooth Advance cohort and was always available for navigating the complicated messy bits of being a PhD candidate.

My animal friends also helped during lockdown, I could not have coped without my daily dog walks and cat cuddles. A special thanks to the Maynooth library cat Seamus who was a welcome distraction on my daily campus walks.

I met some amazing new friends during my four years and this has resulted in pet-sitting opportunities, which in turn has resulted in many new furry friends. Thank you, Joan, Ita and all of the extended Advance family. Thanks to Grace, Dalal and TJ, my PhD support group. My family of course, who still may not understand what I am doing, but fully support me nonetheless.

Thanks to my examiners Ann O Shea and Donna O Shea, who have taken the time to read through my thesis.

Abstract

The overall aim of this thesis was to explore how user experience (UX) design can impact upon security, usability and privacy and the implications this has on the end user, in particular if that user is vulnerable. We aim to do this through three distinct projects.

Our first project was inspired by the question of whether a more complicated security mechanisms, that might challenge a vulnerable user, can always provide substantial extra security. We explore this question by attempting to guess PINs via their partial PINs (a random subset of the full PIN). This form of authentication is commonly used in banking in the UK and Ireland. We created four different guessing strategies in order to see which proved most efficient at guessing various sized PINs. Overall we discovered that you can recover a full PIN faster by guessing via its partial PIN, and that the partial PIN system is not as secure as using a full PIN at log in.

Our second project analyses Irish cookie banners in order to note style and compliance with GDPR regulations. Like partial PINs in our first project, cookie banners could be especially confusing and frustrating to a vulnerable user. This project is based on a study conducted in Greece which looked at their national cookie banners and banners in the UK. Comparatively Ireland fares slightly better in compliance, but otherwise similar results were noted. We note several dark patterns which manipulate users into sharing more data.

Our final project explores the strategies and dark patterns that are used to retain subscribers. We subscribe to four different countries' national news sites and compare subscription and cancellation flows. We also discuss recent regulatory

changes in each country. It was possible to cancel the majority of the subscriptions online. Despite this, it is not as straight forward to cancel and involves going through many barriers to eventually reach the goal of cancelling your subscription. Similar to the preceding two projects, dark patterns potentially can have a greater impact on the more vulnerable user.

Glossary

ACM Dutch Authority for Consumers and Markets

AIB Allied Irish Bank

ARL Automatic Renewal Law

ATM Automatic Teller Machine

BOI Bank of Ireland

CAPCHA A CAPTCHA test is designed to determine if an online user is really a human and not a bot. CAPTCHA is an acronym that stands for "Completely Automated Public Turing test to tell Computers and Humans Apart.

CDF Cumulative distribution function

CFR Charter of Fundamental Rights

CMA Competition and Markets Authority

CMP Consent Management Platform

CNIL Commision Nationale Informatique & Libertes

CPUT Consumer Protection from Unfair Trading Regulations

CSS Cascading Style Sheets

DES Data Encryption Standard

DPA Data Protection Agency

DPC Data Protection Commission

DSA Digital Services Act

ECDF Empirical Cumulative distribution function

EDPB European Data Protection Board

EEA European Economic Area

EU European Union

FCCA Fair Consumer Contracts Act

FIPP International Federation of Periodical Publishers

FTC Federal Trade Commission

GDPR General Data Protection Regulation

HCI Human Computer Interaction

HMAC Hash-Based Message Authentication Code

HOTP HMAC-Based One Time Password

HSBC Hong Kong and Shanghai Banking Corporation

HTML Hyper Text Markup Language

IAB Internet Advertising Bureau

IBAN International Bank Account Number

ICO Information Commissioner's Office

IP Internet Protocol; identifying number that is associated with a specific computer or computer network

ISP Internet Service Provider

MFA Multi Factor Authentication

NTA Network Address Translation

NTA Devices on a private network can interact with devices on a public network without requiring each device to possess a unique IP address

NOYB None of Your Business; European Centre for Digital Rights is a non-profit organisation founded my Max Schrems

NRCLex National Research Council Canada Lexicon

OpenWPM Open sourced web privacy measurement framework

OTP One Time Password

P2D2 The second Payment Services Directive

PAC Personal Authentication Code

PIN Personal Identification Number

PNG Portable Network Graphic

ROSCA Restore Online Confidence Act

SCA Strong Customer Authentication

SMS Short Message Service

TOTP Time Based One Time Password

TP Third Party

UX User Experience

VPN Virtual Private Network

Contents

List of Tables

List of Figures

CHAPTER 1

Introduction

This chapter outlines the objectives and motivation behind this thesis. We present a brief overview of the common threads linking the topics, namely dark patterns and the seven principles of universal design. Additionally, we provide a summary of the three separate studies that constitute this body of work. The chapter concludes with a discussion on the dissemination of the research findings from this thesis

1.1 Research Objectives

The objective of this thesis was to explore topics related to the privacy and security of online digital services while considering the seven principles of universal design (see Sec.1.3.1). We aimed to determine whether certain services might be less user-friendly for vulnerable users in the realms of security, privacy, and online shopping. This focus guided the selection of the thesis chapters.

We selected partial PINs for security and authentication as this method is relatively uncommon globally. We examined cookie banners in Ireland regarding privacy, as these banners often provoke strong reactions concerning privacy concerns. Finally, we investigated subscription services to analyse dark patterns and manipulative behaviours when shopping online. While this represents only a small subset of numerous online activities that can be scrutinised for similar purposes, we chose to highlight this particular subset in this thesis as a diverse lens through which to answer our questions. To achieve this, we aim to address the following questions:

1.1.1 Research Questions

- **Partial PIN Security**

    1. Can you guess a full PIN quicker by guessing its partial PIN?
    2. Is this system of authentication a viable system in terms of usability and security?
    3. Do partial PINs align with the seven principles of design?

- **Cookies Banners in Ireland**

    1. Do Irish cookie banners adhere to GDPR?
    2. What manipulative practices (dark patterns) and barriers are present (if any) in managing cookies.
    3. Do Irish cookie banners align with the seven principles of design?

- **Hard to Cancel Subscriptions**

    1. What barriers and dark patterns exist which can potentially impact cancelling subscriptions across the UK, Netherlands, Germany and American states Texas and California?
    2. Have regulations new or old, had any impact in cancelling subscriptions online across the countries mentioned above?
    3. Does subscription practices in these tested services, align with the seven principles of design?

All questions will be answered in detail in Chapters 2, 3 and 4, however, a brief overview of the chapters is given in Sec.1.4.

1.2 Motivation

In an increasingly digital age, individuals who can not effectively engage with the digital world risk being left behind. As technological change advances, digital skills become essential for connecting with others, accessing information and services, and meeting the evolving demands of the workplace and economy [266]. According to the United Nations, the number of adults over 65 will surpass the number of children aged 0-9 for the first time by 2030 [225]. The World Health Organisation (WHO) defines 'active aging' as the process of optimising opportunities for health, security, and participation to improve the quality of life as people age [241]. In an increasingly digital society, those who cannot avail of digital opportunities for any reason risk feeling excluded. As a result Ireland has drawn forth plans to make this nation the most digitally inclusive state of the European Union [117]. In the UK 2017 census, 56% of adult internet non-users were disabled. According to recent research from the National Council for the Blind of Ireland (NCBI), three-quarters of the country's top 100 websites are technically inaccessible to 600,000 people with disabilities [186, 300]. The report, prepared by NCBI's Inclusion and Accessibility (IA) Labs, also reveals that the vast majority of schools and universities have inaccessible websites, along with 17 of Ireland's top 20 public and private hospitals [186, 300].

Despite much research in the area of user friendly security [32, 290, 309], the user is mostly always taken as the mythical 'average human being'. Users are still almost an afterthought in online security and usability [148]. Disability can create difficulties when navigating the Internet, given that numerous individuals with disabilities struggle with tasks like writing, reading, and understanding textual content. This makes it challenging for them to grasp and employ fundamental security and privacy protocols, including passwords and CAPTCHAs[1] [308].

Jarovsky [162] notes that effective user experience[2] (UX) design can greatly reduce informational vulnerabilities. He emphasises the importance of clear communication regarding data practices, privacy policies, and user control options. By

[1] CAPTCHAS (Completely Automated Public Turing test to tell Computers and Humans Apart): https://www.cloudflare.com/en-gb/learning/bots/how-captchas-work/

[2] UX Design: https://www.interaction-design.org/literature/topics/ux-design

enhancing transparency and making information more accessible and understandable, UX design can empower users, protect their privacy, and build trust in digital interactions.

Johnson's book on designing user interfaces for an ageing population [163] highlights that digital services must be designed with accessibility in mind to be usable by individuals with intellectual disabilities. Continuous training and support are essential, and involving these individuals in the design process enhances inclusivity and effectiveness. Policies and regulations promoting digital inclusion are necessary to protect their rights. He adds that properly designed digital services can significantly improve their independence and quality of life. By focusing on these principles, the book advocates for universal design that enhances usability for older adults and benefits all users [163]. Zezulak et al. conducted a systematic literature review on 63 papers focusing on the privacy and security of web services for the disabled population. They note gaps in the current research, such as a lack of implementation of universal design methods and how solutions must focus on more subsections of the disabled population [308].

1.3 Foundational Themes: Universal Design & Dark Patterns

As dark patterns and the seven principles of design form a link for all topics in this thesis, we give a brief background on each here.

1.3.1 The Seven Principles of Universal Design

In 1997, a collaborative team consisting of architects, product designers, engineers, and researchers in environmental design, headed by the late Ronald Mace at North Carolina State University, formulated the Seven Principles of Universal Design [5].

1. **Equitable Use**: Whereby the design is useful and appeals to all people with diverse abilities. It should avoid stigmatising any users and the provisions for privacy and security should be available for all users.

2. **Flexibility in Use**: Whereby the design caters to a diverse array of individual preferences and abilities. This means the design should accommodate for example, right or left hand use and account for a person's accuracy and precision.

3. **Simple and Intuitive Use**: Whereby the design's usability is readily comprehensible, regardless of the user's experience, knowledge, language proficiency, or current level of focus. This means it should not be over complicated and be relatively intuitive. The interface should also provide feedback during tasks.

4. **Perceptible Information**: Whereby the design effectively conveys essential information to the user, regardless of surrounding conditions or the user's sensory abilities. This means it should use different methods of communicating, for example pictures and essential information should stand out.

5. **Tolerance for Error**: Whereby the design reduces risks and mitigates the negative outcomes of unintentional or accidental actions. The design should provide warnings for errors or risks and also provide fail safe features.

6. **Low Physical Effort**: Whereby the design enables efficient and comfortable use while minimising fatigue, it should also minimise repetitive actions.

7. **Size and Space for Approach and Use**: Whereby adequate size and space are ensured for approach, reach, manipulation and use, irrespective of the user's body size, posture, or mobility. For example, design should accommodate different hand and grip sizes and provide clear line of sight for seated or standing user.

1.3.2 Dark Patterns

The European Union Digital Services Act (DSA) describes dark patterns as:

> Practices on line that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade

> the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them [15].

Dark patterns cover a range of different manipulative design practices online including; *Fake Scarcity*, an example of this is when websites claim there is only a limited amount of the product the user is looking at. *Hidden Costs* occurs when the user, after being enticed by an attractive price, finds at checkout there are other charges added to the bill. Another example is *Visual Interference*, which is when information that is important to the user is hidden or disguised [66].

An observation noted in Mathur et al.'s [207] research, is that researchers can't seem to agree on how best to describe dark patterns. Are they 'manipulative', 'deceiving' or just 'tricks'? The term for dark patterns[3] is also changing, deceptive designs is the current politically correct term. However, it does not encompass all that dark patterns entails, dark patterns are not just about design. The term *Choice Architecture* was introduced by Thaler and Sunstein [288]. They define it as the "creation of various methods for presenting decisions to individuals who must make choices". Most dark patterns work by manipulating choice architecture [1]. According to the Federal Trade Commission (FTC) in the USA, a practice can be judged as deceptive from the viewpoint of a 'reasonable consumer'. In other words, does the practice create a false or misleading impression on the average consumer [207]?

Some researchers have raised doubts as to whether dark patterns are simply forceful marketing tactics, akin to the kind of cunning practices that have existed (and been accepted) in traditional offline businesses for a considerable duration [207]. Calo [74] asserts that digital marketplaces enhance the efficiency of market manipulation due to their extensive reach and advanced methods, enabling them to precisely focus on users. Unlike physical stores, digital marketplaces have the capability to tailor and refine manipulative strategies for each user, ultimately amplifying their overall impact on the entire population. The key differences including large scale, low cost, and unprecedented sophistication [206].

[3]As the term *dark patterns* is officially used in the Digital Services Act (DSA) [15], an EU regulation brought into law in November 2022 [13], we will use this term.

1.4 Thesis Overview

This thesis comprises a compilation of three distinct projects. Each project chapter contains background information and previous research on the topic. Additionally we include in each chapter a comparative literature table which lists prior work in each area and highlights the gap in each field to which our work contributes. In addition we discuss how, despite the fact that these projects are distinct, they have a common thread running through them. Additional work for each project is contained in Appendix A, B, C, D and E. The thesis concludes with Chapter 5, which gives an overall conclusion. This chapter also discusses further work and final thoughts.

1.4.1 Partial PIN Security

Our first project is covered in Chapter 2 and delves into the security of *partial PINs*. A partial PIN is a random subset from your full PIN requested at log in. An example of its use is commonly seen in banking app authentication. Recalling these digits can require some mental gymnastics. We therefore considered the question of how much additional security they added. We achieve this by creating four guessing strategies and running simulations to guess various sized PINs via various respective partial PINs. The results revealed that this form of authentication, which is still currently used in banking online, is not as secure as using full PINs. Examining the partial PIN system also highlighted usability issues. Recalling specific positions of a full PIN could be challenging to users with memory impairment. Further analysis on the mathematics behind guessing partial PINs is included in Appendix A, with extra figures displaying results from various sized PIN guessing simulations in Appendix B. In Appendix C, we consider how our methods used in guessing partial PINs can be applied to guessing time based one time passwords (TOTP). The background of this authentication method is also provided here.

1.4.2 Cookies Banners in Ireland

Chapter 3 investigates cookie banners on Irish websites, and how they comply with current GDPR regulations. Cookies are explained in more detail in the chapter, but, briefly, cookies are text files which websites use to serve multiple functions, including remembering user preferences and generating statistics [136]. This study was a comparative study based on a study of the same nature conducted on British and Greek cookie banners [168]. In analysing Irish cookie banners we uncovered several *Dark Patterns* and hurdles preventing ease of access to privacy friendly choices. In general GDPR regulations are unclear and easy to manipulate to benefit companies into collecting users data rather than protecting users privacy. This was evident with some websites interpreting GDPR Cookie banners come in numerous styles and are positioned in different locations on the page for different websites. Extra cookie banner images and data can be found in Appendix D.

1.4.3 Hard to Cancel Subscriptions

Chapter 4 looks into dark patterns in news website subscriptions. This project is a collaboration with Dr Gunes Acar, Dr Hanna Schraffenberger and Dr Raphaël Gellert from Radboud University. The project developed from a four month research placement in Radboud University, Nijmegen in the Netherlands. Over the course of this research placement, we explored different areas around the topic of dark patterns and one of which was *Subscription Traps* or *Roach Motel*. This is where it is easy to purchase a subscription but difficult to cancel it [66]. News sites appeared to be typically difficult to cancel, so we decided to focus on these, additionally news sites are also cheaper and more convenient to subscribe to in bulk compared to other types of subscriptions such as consumables or software. In this study we came across various usability issues regarding subscriptions. For example, cancelling for Daily Wire subscription required typing 'CONFIRM' into a box. For people with certain disabilities this could pose a challenge, dyslexia being one. Extra data and screenshots can be located in Appendix E.

1.4.4 Thesis Contribution

This thesis adds value to the discussion of usability for vulnerable populations especially in the context of Ireland's plans to make this country more user friendly for vulnerable populations [117]. Our research draws attention towards vulnerable users in specific areas of UX design, privacy and security. Each chapter offers a different perspective in the above mentioned areas in terms of design and usability.

Partial PINs (Sec. 1.4.1) potentially add extra complication in their use with no additional security benefits as recalling specific digits of a full PIN requires more cognitive effort. We demonstrate that we can guess a partial PIN in as little as a few hundred attempts, and as a result, for a 6-digit PIN with a 3-digit partial PIN, we can identify 50% of the full PIN. Figure 2.8 in Chapter 2 reveals how much longer it takes to guess a 6-digit PIN for all methods compared to a 3-digit partial PIN. We found that cookie banners (Sec. 1.4.2) in Ireland do not offer easy access to privacy-friendly options. Most employ dark patterns and positive language to nudge users toward accepting cookies, while making it difficult to find the option to decline unnecessary cookies. We submitted our findings to the Data Protection Commission in Ireland, who are the national independent authority responsible for ensuring the fundamental right of individuals in the EU to have their personal data protected[4]. And finally subscriptions (Sec. 1.4.3) can create problems for users who struggle to cancel them due to obstacles imposed by websites. We identify many websites who use dark patterns to elongate the cancelling process. This can cause frustration and financial hardship when a person is not able to successfully cancel a membership. From this study we submitted our findings to the Federal Trade Commission (FTC) in the USA. We also have provided a link to our data collected while subscribing and cancelling our subscriptions and steps on how we conducted our study to help future research in this area (see Chapter 4).

Additionally we highlight how regulations can be more clear and effective. In terms of GDPR, we can see how the vague guidelines can be manipulated with regards to cookie banners, however in our subscription study we note how effective Germany's strict regulation on cancelling subscriptions was in being able to cancel subscriptions online compared to other countries.

This thesis will also add a valuable contribution to further research in the area of universal design. Highlighting how many universal guidelines are not followed in all the topics we cover in this thesis. Each chapter highlights more detailed contributions for each topic covered in Sections 2.1.1, 3.1.1 and 4.1.1.

[4]Data Protection Commission in Ireland (DPC):`DataProtectionCommissioninIreland`

1.4.5 Thesis Limitations

Regarding the common thread linking all topics, vulnerable populations, we did not conduct research with vulnerable users and this is a obvious limitation. We anecdotally observe limitations in user design as they should adhere to the seven principles of universal design. Research involving vulnerable populations is difficult to conduct with regards to ethical approval [234]. We conduct this research as a guide to future work in this area that can further investigate these limitations as they apply to vulnerable users.

Conducting research with groups of people at risk of vulnerability is the exception rather than the norm and special consideration must be given [234]. This may explain why there is little research conducted on vulnerable populations and usability regarding the topics in this thesis.

1.5 Dissemination

All publications and talks are based on the work included in this thesis.

1.5.1 Peer Reviewed Publications

- Sheil, A. and Malone, D., 2022. *Guessing PINs, One Partial PIN at a Time*. Entropy, 24(9), p.1224. https://doi.org/10.3390/e24091224
- Sheil, A. and Malone, D., 2022. *Fianán, Cuacha: Irish Cookie Banners*. 2022 33rd Irish Signals and System Conference (ISSC) (pp. 1-8). IEEE. http://doi.org/10.1109/ISSC55427.2022.9826167
- Sheil, A., Acar, G., Schraffenberger, H., Gellert, R. and Malone, D., 2023. *Staying at the Roach Motel: Cross-Country Analysis of Manipulative Subscription and Cancellation Flows*. ACM CHI24 conference on Human Factors in Computing Systems https://dl.acm.org/doi/10.1145/3613904.3642881.

1.5.2 Media Publications

- **RTÉ Brainstorm**, Article on dark patterns in subscriptions, May 2024, https://www.rte.ie/brainstorm/2024/0509/1448035-dark-patterns-cancel-online-subscriptions/

1.5.3 Conferences Presentations & Other Talks

In addition to talks given for the Advance CRT cohort and the Maynooth Advance journal club, below lists all presentations and talks made during the PhD.

- **Hamilton Student Seminar**, Maynooth University. April 27th 2021. Virtual presentation of research paper *Guessing PINs, One Partial PIN at a Time*.
- **Famelab**. June 8th 2021. Virtual. Awarded a place in the Famelab competition which provided training in preparing and recording a three minute talk on research paper *Guessing PINs, One Partial PIN at a Time*.

- **SFI Science Summit**. November 4th–5th 2021. Virtual poster on research paper *Guessing PINs, One Partial PIN at a Time*.
- **HEAnet Tech Talk**. May 12th 2022. Virtual presentation of research paper *Guessing PINs, One Partial PIN at a Time*.
- **ISSC: Irish Signals and System Conference**, MTU, Co. Cork, Ireland. 9th–10th June 2022. Presentation of research paper *Fianán, Cuacha: Irish Cookie Banners*. Winner of best student paper.
- **TNC Lightning talk**, Trieste, Italy. June 13th–17th 2022. Awarded a place in the Future Talent programme sponsored by HEAnet to train for and present a lightning talk on research paper *Guessing PINs, One Partial PIN at a Time*.
- **Radboud University Lunchtime Talks**, Nijmegen, Netherlands. September 30th 2022 . Presentation of research paper *Guessing PINs, One Partial PIN at a Time*
- **PasswordCon**, Bergen, Norway. May 15th–18th 2023. Presentation of research paper *Guessing PINs, One Partial PIN at a Time*.
- **Three-minute thesis competition**, Maynooth University. October 25th 2023.

CHAPTER 2

Guessing PINs Via Partial PINs

Entering digits of a personal identification number (PIN) is a common form of authentication. One variant of this scheme is to request the digits from a random subset of positions, which is sometimes called a partial PIN. *This method is sometimes used in online banking, where different banks may vary the amount of digits requested. In this chapter we consider strategies for guessing the PIN when a partial PIN scheme is in use, which allows the quantification of the strength of this mechanism, and highlight how partial PINs may not be user friendly for vulnerable cohorts. We suggest several strategies for guessing the PIN under the assumption that the organisation assigns PINs randomly and requests random positions from the PIN at each login. We present analytic and simulation results from the different strategies and explore their performance when guessing different sizes of PIN and requested subset. We find that the most effective strategies have a reasonable chance of recovering a PIN in tens to hundreds of guesses.*

2.1 Introduction

PINs are generally associated with mobile phone unlocking and the financial market for use with ATMs and banking online, due to their convenience on number pads [78]. One variation of the simple PIN is to request a subset of digits from a longer PIN, known as a *partial PIN*. This scheme is commonly used by banks in some countries. This has the advantage that an eves-dropper who sees a single login does not learn the full PIN [36].

2.1.1 Objectives & Contributions

In this chapter, we pose the following three questions:

RQ1:1 Can you guess a full PIN quicker by guessing its partial PIN?

RQ1:2 Is this system of authentication a viable system in terms of usability and security?

RQ1:3 Do partial PINs align with the seven principles of design?

We address these question by exploring four strategies for guessing a full random PIN by guessing incrementally the partial PIN requested. Expanding on research conducted on user chosen PINs by Aspinal st al. [36] and their proposed future work utilising an adaptive projection dictionary[1]. We study the process via analysis and simulation to observe how these different strategies perform and to understand the effective strength of the partial-PIN mechanism.

This study is a notable contribution to both the mathematical and cybersecurity fields, as the detailed analysis of guessing random PINs via partial PINs has not been conducted to this extent before (see Table 2.2). The results we have found, and the graphs in Sec. 2.4, may be of use to security designers who wish to understand the strength of partial PIN schemes, either individually or as part of a multi-factor scheme. We developed novel guessing mechanisms for partial PINs, these can be used further in mathematical fields in the area of guesswork. This work also highlights a usability trade-of in partial PINs, there is no security gain in using partial PINs, however, inputting partial PINs can be unnecessarily cumbersome for vulnerable users. Password Complexity tends to increase both memory and motor errors [284].

[1] An adaptive dictionary attack is where the attacker utilises a continually updating list of probable password guesses to crack a password. Unlike a traditional dictionary attack that relies on a fixed list of common passwords, an adaptive dictionary attack adjusts its guesses based on feedback obtained throughout the attack process.

Digits	Top Ten PINs									
4	1234	0000	2580	1111	5555	5683	0852	2222	1212	1998
6	123456	654321	111111	000000	123123	666666	121212	112233	789456	159753

Table 2.1: Most popular four and six-digit PINs, data sourced from the RockYou password leak [204].

Sec. 2.2 reviews related work in this area. Sec. 2.3 describes our strategies, with Sec. 2.3.4 providing a mathematical analysis of the strategies. Sec. 2.4 demonstrates the guessing performance of the strategies and Sec. 2.5 discusses these results in context. Finally, Sec. 2.6 concludes and discusses further work in the area. More in depth mathematical analysis of the strategies can be found in Appendix A, with additional graphs in Appendix B. In Appendix C we explore how our partial PIN guessing methods can be theoretically applied to guessing time based one-time-passwords.

2.1.2 PINs & Partial PINs Background

PINs in banking were first introduced in the Barclays-De La Rue system in 1967, initially with 6 digits. The number was later reduced to 4 digits after the wife of John Shepard Barron, the leader of the engineering team, reportedly struggled to remember six random digits [61]. Banks began allowing customer-chosen PINs in the 1980s as a marketing initiative [61]. Some banks subsequently took on the user-chosen PIN idea, but have since discovered security flaws in this, Markert et al. demonstrate the flaw in their paper: humans tend to use patterns of numbers to make their PINs easier to recall [204]. The top ten user-chosen PINs for four-digit and six-digit PINs can be seen in Table 2.1, here you can see patterns, such as the last 6-digit PIN, the numbers 159753 are an x shape pattern on the number pad from 1 down to 9 and 7 up to 3.

In some jurisdictions, rather than requesting the full PIN, banks often ask for a random subset of a customer's PIN when banking online. This is known as the partial PIN system. The Partial PINs origin story is not easy to source. Initially they were used in phone banking, to prevent the operator from seeing your whole PIN [36], but why they migrated to online banking is not so clear. One speculative theory could be, as partial PINs were approved by regulators for phone banking, banks may have felt that this then also gave them some level of approval to use as a second factor online. Dr Junade Ali, believes partial PINs were a measure to reduce screen scraping of banking information—adding complexity rather than stopping it[2]. Different banks may use different sized PINs and request different

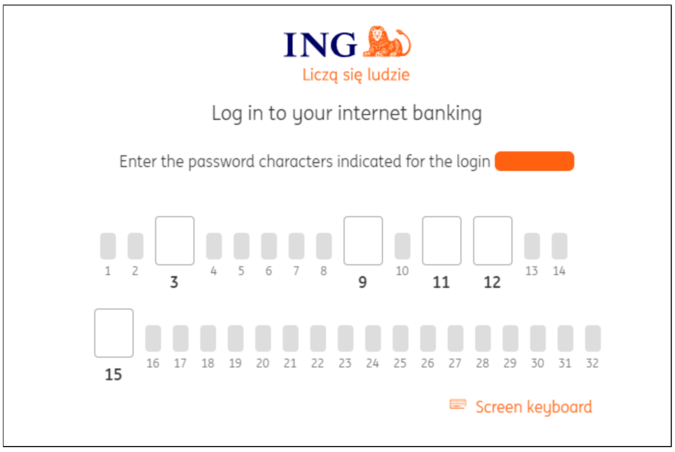


Figure 2.1: Online partial password login for ING bank in Poland [2].

sized subsets. The partial PIN system is believed to be predominantly used in the UK and Ireland. It is also utilised in South Africa, Canada, Poland, Croatia, and Kuwait[3]. Fig. 2.1 shows the partial PIN log in for the bank ING in Poland, which is based in the Netherlands. ING stopped their partial PIN system in April 2022, to log into online banking, you either call or request a one time password (OTP) [40].

With the development of strong authentication, partial PINs are being combined with other forms of authentication. The second Payment Services Directive, or PSD2, is a European law that came into effect in September 2019. This law aims to make online banking more secure by adding strong customer authentication (SCA) [41, 305]. Some banks are changing their login procedures, which depending on the individual bank may vary for e.g. Allied Irish Bank (AIB) will now require their customers to log in online with their full personal access code (PAC),

[2]Information obtained while attending PasswordCon23 from Dr Junade Ali, a British Computer scientist and Fellow of IET, https://junade.com/.

[3]Based on discussions with fellow participants at PasswordCon23.

where previously, you were required to input a subset of your PAC. AIB appear to be the only Irish bank that have abandoned partial PIN outright however, other banks like Bank of Ireland (BOI) have kept their partial PIN but added other forms of authentication. The Credit Union and the Permanent TSB also require a partial PIN for their banking apps along with 2FA. Adding a second factor of authentication might be sufficient to mitigate any security vulnerabilities associated with partial PINs. In the UK the Hongkong and Shanghai Banking Corporation (HSBC) use a partial password and a question, Santander uses partial PIN and a partial password. When banking online via a laptop, your smart phone provides second factor authentication. For online purchasing you are required to authenticate with a second factor SMS or your banking app. Others require bio-authentication like facial recognition or a third verification such as a personal question.

There is no particular reason why partial PINs or passwords should be restricted to banking. Indeed, Symantec's Advanced Authentication product, which provides authentication support for mobile and web applications, includes support for partial passwords[4]. However, in practice, common examples of its use seem to be in the banking sector.

2.1.3 Partial PINs & Security

A potential security advantage of partial PINs is their ability to thwart *shoulder surfing* attacks[5], where an observer tries to capture your full PIN. With partial PINs or passwords, observing a single input does not provide sufficient information to access an account, unless the exact same characters are requested again. However, as we demonstrate in this chapter, this protection is not foolproof. The second Payment Services Directive mentioned Sec.2.1.2, may change the use of partial PINs for a number of reasons. These include the availability of multi-factor authentication methods (MFA) and challenges in storing hashed partial

[4] See, for example, `https://techdocs.broadcom.com/us/en/symantec-security-software/identity-security/advanced-authentication/9-1/release-notes-9-1.html`.

[5] A technique employed to acquire sensitive information, such as personal identification numbers (PINs), passwords, and other confidential data, by covertly observing the victim's actions. Unauthorised individuals may observe the keystrokes entered on a device or eavesdrop on sensitive information being spoken to gather the data they seek [6].

passwords [217]. Websites that request partial password or PIN Validation, cannot ensure secure storage of passwords through robust algorithms such as BCrypt[6] or Argon2[7], which are both password hashing algorithms designed to enhance the security of stored passwords. Typically, passwords are stored on the server in an irreversible hashed format, which protects them in case of a data breach. But for partial passwords, this seems impractical — a hash cannot reveal individual characters of a password, as all information is destroyed in the hashing process if it is truly a cyptographic one-way function. The entire password would need to be stored in a recoverable form to compare individual characters [193]. PINs for partial PIN retrieval, could be stored encrypted in a hardware security module (HSM)[8] [193]. Individual digits then can be presented to the HSM, which then gives a yes/no answer. This increases the risk of decrypted passwords being extracted as HSMs are not invulnerable [193]. In the event of a breach, where the service provider's security is compromised, these exposed passwords in plain text could be exploited to access other websites if the account holder employs the same password, resulting in a potential *Credential Stuffing*[9] attack [167]. This implies, that even if the bank PIN is not user chosen, a person may reuse their PIN in other authentications as it is easy to remember [78, 172]. In short these PINs could be used in dictionary attacks for other accounts. As noted in Sec. 2.2, there is minimal research on the security of random partial PINs, and the storing of partial PINs and obtaining this information from banks is challenging.

[6]Bcrypt is a password hashing algorithm designed to be slow to resist brute-force attacks and uses a salt to protect against rainbow table attacks (a rainbow table is a pre-computed table used to reverse cryptographic hash functions, primarily for cracking password hashes). It hashes passwords with a 128-bit salt, resulting in a unique 192-bit hash for each password. The hashes and salts are base-64 encoded, producing 31-character and 22-character strings, respectively. This approach enhances security by increasing computational effort and ensuring unique hashes [44].

[7]Argon2 addresses several key aspects of security, including resistance to brute-force attacks, memory-hardness, and adaptability to future hardware improvements. It is a modern password-hashing algorithm designed to be secure, efficient, and resistant to various attacks. It won the Password Hashing Competition (PHC) in 2015 and has since become a recommended standard for password hashing. `https://github.com/P-H-C/phc-winner-argon2`

[8]A hardware security module (HSM) is a physical device that provides secure storage and management of cryptographic keys and sensitive data.

[9]Credential stuffing is a cyberattack technique where attackers use lists of compromised user credentials to gain unauthorised access to a system [160].

2.1.4 Partial PINs & Vulnerable Users

Superficially it is more efficient to enter three digits than six. However, it can be quite difficult to remember specific positions of a long PIN. This potentially could be much more difficult for people who have some impairment to their memory. To recall certain digits a person may have to write out their full PIN, as recalling incorrectly more than two times results in being temporarily locked out of your account and if it is a banking account this can be frustrating. This can also apply when using password managers, it is often necessary to copy the password from your vault and paste it somewhere in order to see the required digits [167].

Helkala [156] demonstrates how individuals with Parkinson's disease, dyslexia, vision impairment, and upper extremity disabilities impact the security and usability of existing authentication methods, such as static PIN codes, textual passwords, and one-time codes generated by code generators or received via SMS. Helkala discusses how each disability can impact different authentication methods and compares them to the average person. In terms of PIN use with these disabilities a person with dementia has a higher chance of forgetting PINs than the average user. A summary of her results can be seen in Fig. 2.2 taken from the paper. As we our focusing on PINs, we have concentrated on the PIN section of her study. The terms standard, slightly lower, or lower describe the search space entropy[10] and circumvention difficulty to reflect the impact of disabilities. For transaction time and human delay, the terms standard, slightly longer, or longer are used. For PINs we can see that circumvention difficulty is lower for users with Parkinson's, vision impairment and upper extremity disabilities than the average user. Transaction time and time caused by human delay are slightly longer for users with Parkinson's, dysleksia and vision impairment. As can be seen in Table 2.2, there is limited research on partial PINs, and, to the best of our knowledge, none on the usability of partial PINs. In terms of memory and PINs, Moncur et al. discusses the challenges individuals face in remembering PINs and passwords, highlighting the cognitive burden associated with these security measures [213], this study was conducted in 2009. Huh et al. showed that there was no statistically significant

[10]Search space entropy measures the unpredictability of possible values an attacker must guess, such as passwords or encryption keys. Higher entropy means a larger, more complex search space, making unauthorised access more difficult.

difference in the difficulty in recalling 6, 7, and 8-digit PINs. Therefore considering 7 and 8-digit PINs as options when increasing the length from the commonly used 4-digits can enhance security [159]. This same study suggests clunking sections of numbers together in a long PIN in order to remember better, people remember their mobile number for this reason also (Irish mobile numbers are ten digits long). This could be one way to remember partial PINs better without resorting to writing them down.

	Group	Search Sapce Entropy	Circumvention Difficulty	Transaction Time	Time caused by Human Delay
PIN	Parkinson	Standard	**Lower**	*Slightly Longer*	*Slightly Longer*
	Dysleksia	Standard	*Slightly Lower*	*Slightly Longer*	*Slightly Longer*
	Vision Impaired	Standard	**Lower**	*Slightly Longer*	*Slightly Longer*
	Upper Extremity	Standard	**Lower**	*Slightly Longer*	Standard

Figure 2.2: PIN section of Table 1, taken from [156], standard equating to the average user, lower/longer at the opposite end of the scale and slightly longer/lower the middle.

2.1.5 Why Study Partial PINs?

We are motivated to study guessing such PINs for two reasons. First, there are situations where in-the-wild attacks using such guessing is practical. An example scenario sees an attacker, Craig who has access to Alice's phone and attempts to gain access to her online banking account, which is protected by a partial-PIN scheme. Craig is going to be patient and play the long game. He will attempt to guess Alice's banking full PIN by guessing the partial PIN; he has a few attempts each day in which he tries to guess the correct partial PIN and stops before being locked out. The next day he tries again and so on, each time he is ruling out incorrect guesses and crosses them of the list of all possible combinations. If he gains access with a correct partial PIN guess he now has those digits of the full PIN and can eliminate all combinations which do not have those numbers in order. Eventually, with enough patience, Craig will guess the whole PIN.

In this case, Craig has access to Alice's device, which might be possible if Craig is, for example, a co-worker or is caring for Alice. Hence, any blocking mechanism based on device, location or IP (Internet Protocol)[11] address is unlikely to be effective. Distinguishing between a low-rate attack consisting of a few guesses per day from typographical errors or accidental activation of a banking app (e.g., when someone takes their phone out of their pocket) will be extremely difficult. However, we can also consider weaker versions of the attack, where Craig does not have regular access to the device but might share accommodation with Alice, and so still shares a location and IP address. In this scenario, the bank has slightly more information, but unless logins are tied to a specific device, the attack will still be feasible.

A weaker attack still might see Craig attacking a pool of users after an online leak of information, and with access to a large pool of IP addresses to make guesses from; here no one IP address has a high guessing rate. In each of these cases, the number of guesses required is an important factor in the success of the attack,implementing a blocklist or rate limit based simply on IP address would incur significant practical issues, and it would be challenging to differentiate low-rate guessing from accidentally misentered digits. If web-based logins are permitted (which is the case for many banks, even if in modern systems, subsequent transactions require authorisation from a specific device), this attack will also remain possible, at least for determining the PIN.

While the environment a web browser runs in is often easier for a user to manipulate, the environment for an app on a phone is much more constrained. Banking apps themselves can be vulnerable [83, 84, 155, 267]. Kellner et al. [170] Looks

[11] IP-based blocklisting is a method used to restrict or block access to a particular network, system, or service based on the IP address of the incoming connection. It involves maintaining a list of IP addresses that are known or suspected to be associated with malicious activity, unauthorised access attempts, or other undesirable behaviour. It is worth noting however, that implementing any form of simple IP-based blocklisting poses significant challenges in modern networks. Many users share IP addresses due to household NAT (Network Address Translation), Carrier-Grade NAT, or transparent proxies operated by ISPs (Internet Service Providers), which are all techniques used to manage and conserve IP addresses in computer networks. This means that IPs cannot simply be blocked or rate limited without causing significant problems for customers. Additionally, there are numerous opportunities for determined attackers to gain access to other IP addresses through natural address rotation, VPN services, cloud services, and so on.

at jailbreak attacks[12] on banking apps and demonstrated that only 18 out of 34 banking apps downloaded from the Apple App Store employ jailbreak detection mechanisms, leaving the rest vulnerable to attacks. They emphasise the urgent need for enhanced jailbreak detection mechanisms to safeguard against eavesdropping and data theft, especially in two-factor authentication scenarios commonly employed in banking applications. This another possible way of gaining log in information.

Of course, it might be possible to authenticate by a device ID instead of a IP address, particularly on a mobile device. While mobile devices often have a hardware identifier that can be accessed by a mobile application, the situation for those accessing banking through a traditional browser is different. Here, there is no standardised hardware identifier and they could be easily faked as the software is under control of the user. In fact, proposals to add such attestation to browsers in general, such as Google's Web Environment Integrity, have been resisted by users and developers as harmful to the openness of the web [304]. In cases where the device ID is not available, the IP address could be used to track or rate-limit users, as is common with countermeasures for spam e-mail. On mobile devices with device identifiers, the attack scenario would be slightly different, or when both a mobile and desktop device are available.

Admittedly, with the addition of second factor authentication, the above scenarios are far less realistic. However, we feel it is important to quantify the strength of this form of authentication as it has not been done before for random partial passwords (see Table 2.2).

Second, we believe the theoretical strength of these partial-PIN mechanisms has not been quantified (see Table 2.2), and we aim to do this in terms of number of guesses required to determine the secret (i.e., the full PIN). This is analogous to characterising the number of guesses required to identify user-chosen passwords or machine chosen secrets [202]. We believe it is important to offer some insight into the security of these partial PINs, as they remain in use as a factor in banking

[12]Jailbreak attacks exploit vulnerabilities to bypass a device's security restrictions, granting unauthorised root access. This allows for the installation of unapproved software and customisation but also increases security risks by compromising built-in protections.

authentication, and some countries noted in Sec. 2.1.2. We choose the number of guesses to recover the full PIN as the metric of interest, as the use of partial PINs is motivated by protecting the full PIN from an attacker. However, similar techniques can be applied to study the number guesses before the first successful login.

2.2 Related Work

Password guessing is a popular research topic in the area of banking and online security, however most research is aimed at user-chosen PINs. Bonneau et al. investigate the security implications of human selection and management of PINs [63], based on the leaked data set 'RockYou', from which they discovered that 1234 was the most common user-chosen four-digit PIN. Markert et al. also availed of this data set when investigating user-chosen PINs [204]. Birth dates were discovered to also be a popular choice for PINs (especially for four and six-digit PINs), as were repeated digits, for example, 1111. Bonneau et al., advise users not to use PINs based on date of birth [63]. Bentley and Mallows postulate that "Humans tend to choose secrets in nonrandom and repeated patterns" [48].

In light of this research, randomly assigned PINs appear to be a more logical approach for security, and some banks appear to follow this approach. Research in the area of guessing sets of random numbers, such as PINs, is harder to find. The closest previous work done in this area is by Markus G Kuhn where he uses probability to guess randomly generated PINs for ATM cards [183]. Donald E. Knuth focuses on the game Mastermind, where rather then numbers, you are guessing colours in a sequence of four coloured pegs out of six possible colours, hence there are $6^4 = 1296$ possible combinations [177]. Comparing this case to our scenario, we have 10 digits to choose from, here they have 6 (colours), their full PIN (or peg sequence in this case) size is 4, therefore they only focus on this PIN size. In our paper the lowest PIN size we look at is $10^4 = 10000$, which has a much bigger list of combinations, we also explore much bigger sizes up to 10^6.

Focardi et al. follow on Knuth's idea of solving the Generalized Mastermind Game problem and link it with guessing bank PINs [133]. From Focardi et al.'s study, we repurposed their guessing protocol for our banking scenario. They set out a framework for guessing games which we will use to describe our problem. In terms of exhaustive guessing methods, which we explore in our paper, Chiasson and Van Oorschot explore methods of guessing passwords relating to password expiration policies [87].

Aspinal and Just also investigate partial passwords, both character and numerical [36]. They concede that this is an area that has seen less attention than others, and it has not been addressed since their work in 2013, which can be also noted in Table 2.2. This study also addresses user-chosen passwords and PINs. Like Bonneau et al. [63], they avail of the RockYou data set in their study, where they find that with "6 guesses, an attacker can respond correctly to 2-place challenges on 6-digit PINs with a success rate of 30%" and "Recording up to 4 runs, an attacker can succeed over 60% of the time". The study also indicates that the likelihood of an attacker successfully reconstructing the entire password grows with the number of partial password entries they collect. For instance, if a password is eight characters long and an attacker can observe four different partial requests, the chances of them deducing the complete password are significantly high [36].

In this chapter, we look at how quickly a randomly assigned PIN can be guessed, which is similar to what Aspinal et al. [36] consider, with a key difference being that we consider the possibility of tracking all information learned by guessing, which is important in the effective guessing of uniformly assigned random PINs. In their terms, it corresponds to an *adaptive projection dictionary* attack suggested in their future work. This means that in our case we have a list of all possible combinations for a PIN, as opposed to a list of leaked passwords to guess from such as the RockYou dataset.

Table 2.2 shows a comparative literature review highlighting the research gap which our study (highlighted in grey) addresses, which includes whether or not the research addressed vulnerable users.

Table 2.2: Comparative literature table on PIN and Partial PIN guessing. Highlighting our contribution in this area.

Title	Year	Vulnerable Users	Full PIN	Partial PIN	Random	User Chosen	Snooped Info
Protecting poorly chosen secrets from guessing attacks [144]	1993		✓			✓	✓
Decimalisation table attacks for PIN cracking [59]	2003		✓				✓
A PIN-entry method resilient against shoulder surfing [259]	2004		✓		✓		✓
How Much Assurance Does a PIN Provide? [48]	2005		✓			✓	✓
Formal analysis of PIN block attacks [280]	2006		✓		✓		✓
ColorPIN: securing PIN entry through indirect input [115]	2010		✓		✓		
Guessing bank pins by winning a mastermind game [133]	2012		✓		✓		
A birthday present every eleven wallets? the security of customer-chosen banking pins [63]	2012		✓			✓	✓
Analysis of dictionary methods for PIN selection [279]	2012		✓			✓	✓
PIN selection policies: Are they really effective? [173]	2012		✓			✓	

Table 2.2: Comparative literature table on PIN and Partial PIN guessing. – continued from previous page.

Title	Year	Vulnerable Users	Full PIN	Partial PIN	Random	User Chosen	Snooped Info
Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry [56]	2012		✓		✓		
Guessing human-chosen secrets [61]	2012		✓			✓	✓
On the Practicality of Motion Based Keystroke Inference Attack [72]	2012		✓		✓		✓
"Give me letters 2, 3 and 6!": Partial password implementations and attacks [36]	2012			✓		✓	✓
PIN skimmer: inferring PINs through the camera and microphone [272]	2013		✓		✓		✓
PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices [276]	2014		✓		✓		✓
Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry [188]	2014		✓		✓		✓
Beware, Your Hands Reveal Your Secrets! [271]	2014		✓		✓		
Learning Assigned Secrets for Unlocking Mobile Devices [264]	2015		✓		✓	✓	

Table 2.2: Comparative literature table on PIN and Partial PIN guessing. – continued from previous page.

Title	Year	Vulnerable Users	Full PIN	Partial PIN	Random	User Chosen	Snooped Info
WiPING: Wi-Fi signal-based PIN Guessing attack [80]	2016		✓		✓		
On The Security Evaluation of Partial Password Implementations [217]	2016			✓		✓	✓
Understanding Human-Chosen PINs: Characteristics, Distribution and Security [298]	2017		✓			✓	
Guessing your PIN right: Unlocking smartphones with publicly available sensor data [50]	2018		✓		✓		
DragPIN: A Secured PIN Entry Scheme to Avert Attacks [277]	2018		✓		✓		
Two-Thumbs-Up: Physical protection for PIN entry secure against recording attacks [229]	2018		✓		✓		✓
There Goes Your PIN: Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting [49]	2018		✓		✓		
When Human cognitive modelling meets PINs: User-independent inter-keystroke timing attacks [192]	2019		✓		✓		✓

Table 2.2: Comparative literature table on PIN and Partial PIN guessing. – continued from previous page.

Title	Year	Vulnerable Users	Full PIN	Partial PIN	Random	User Chosen	Snooped Info
Your PIN Sounds Good! Augmentation of PIN Guessing Strategies via Audio Leakage [76]	2020		✓		✓		
This pin can be easily guessed: Analysing the security of smartphone unlock pins [204]	2020		✓			✓	
Hand Me Your PIN! Inferring ATM PINs of Users Typing with a Covered Hand [75]	2022		✓		✓		✓
PIN Scrambler: Assessing the Impact of Randomised Layouts on the Usability and Security of PINs [176]	2022		✓		✓		
Secure PIN-Entry Method Using One-Time PIN (OTP) [57]	2023		✓		✓		
Guessing PINs, One Partial PIN at a Time [270]	2023	✓		✓	✓		

2.3 Attacker Strategies

We denote a full PIN and their partial PIN subset as ${}^{n}C_{m}$, we use the mathematical notation used for a binomial coefficient[13]. This notation reads as n choose m and indicates the number of ways one can choose m items from a collection of n items. We do not use it mathematically the same way but only to show that the full PIN

[13] A Binomial coefficient represents the number of ways to choose k items from a set of n distinct items without regard to the order of selection and is calculated using the formula

is represented by n and it's subset or partial PIN is represented as m, it provides a shorthand representation of the partial PIN. When we refer to full PINs with no partial PINs we say ${}^{n}C_{n}$.

Assume that the bank chooses an n-digit PIN for a user uniformly at random. For simplicity of exposition, we will use $n = 4$ for our examples in this section, so there are 10,000 possible PINs [14]. This PIN is assigned to the user for future logins.

When a user (or attacker) attempts to log in, the bank picks m positions from the n digits of the PIN. In these examples, we work with $m = 2$. The user must provide these digits. If they provide them correctly, they are given access to the system. If they do not provide them correctly, they are refused access. We assume that repeated login attempts results in a new random selection of positions from the PIN. In real systems, login attempts are often throttled or rate-limited, but here we assume that many guesses can be made in order to assess how quickly attacks can be practical.

We assume that the attacker begins with a list of all possible PINs, which we call the PIN list. The attacker will use this list to inform their choice of guess, and we call this a strategy. After each guess, the attacker updates the PIN list. If the attacker correctly guesses the two chosen positions (which will be revealed upon gaining access to the account), all four-digit numbers that do not have this combination of digits in the requested positions are deleted from the PIN list. If the guess is wrong, then all PINs with this combination of digits are deleted from the PIN list. In this way, if the PIN list reduces in length at each guess, the attacker will eventually find the correct PIN.

[14]There are 10 possible values for each digit of the PIN $(0-9)$, so there are $10 * 10 * 10 * 10 = 10^4 = 10000$ total possible PIN numbers.

2.3.1 Partial PIN Guessing Algorithm

In abstract terms, following the notation for a general guessing game in [133], guessing the PIN can be described as follows:

- The bank chooses the secret s, which in our case is the PIN.
- The set of possibilities, S, ranges from 0000 to 9999.
- A guess g, in our case a subset of the PIN, is for two random positions in the PIN.
- Response to guess $= r_s(g)$ depends on the secret s and the guess g. In our case, this is a successful login or not.
- After guessing the list of remaining numbers from our PIN list:
  $S_i = \{v \in S : r_v(g) = r_s(g)\}$.
- The secret s must be in the intersection of the sets S_i.

Note, an attacker can incorporate additional information, such as an eavesdropped login attempt, by starting with a different S. The above example uses a PIN size of 4-dgits with a partial PIN of 2, but any m or n can be used. Examples of results using different m and n sizes can be seen in Appendix B.

2.3.2 The Four Strategies

We consider the following four strategies for choosing the guesses:

Max At each guess, this method uses the PIN list to find the frequency of combinations of digits in the positions requested by the bank. The combination with the highest frequency is guessed, with ties broken randomly.

Educated Guess This method looks at the distribution of digit combinations for the positions requested by the bank, and chooses a combination according to this distribution. For example, if the second and third digit are requested and 50% of PINS remaining have 77 in this position, while 25% have 78 and

25% have 79, then 77 will be chosen 50% of the time, etc. In practice, this can be achieved by choosing one PIN at random from the remaining PIN list and using the requested digits.

Round Robin The Round Robin method starts by trying 0 for each position. On the next guess requesting this position, it will guess 1, then 2 and so on, wrapping at 9. This method does not use the PIN list to choose its digits. Note, in the ${}^{n}C_{n}$ case it will usually not succeed; for example, if guessing 4 digits from 4, it will only guess 0000, 1111, ..., 9999. For ${}^{n}C_{m}$ problems where $m < n$ and random (strict) subsets of digits are being selected, it will eventually guess every combination. However, it will usually fail on ${}^{n}C_{n}$ problems.

Random The random method chooses random numbers for each of its guesses. It will eventually guess all combinations with probability converging to 1. As with Round Robin, it does not use the PIN list to guess.

Each of these strategies was coded in Python, to allow the assessment of its performance. We created pseudocode (see Alg. 1) based on our Python code, to summarise the operations performed by the code for each strategy. We expect that the last two strategies will not usually be competitive, as both methods do not avail of the information from the all possible combinations PIN list. Guessing randomly means wrong partial PINs can be repeatedly guessed again and round robin is an iterative process, each digit has to go through guessing from 0 to 9. However we include them for two reasons; First, they offer a useful comparison. Second, since they do not use the PIN list to make choices, they avoid many operations on the PIN list which is initially of size 10^n. For large n, maintaining this list might be prohibitive. In some cases, these strategies act in the same way, which can be seen in Sec. A.1.

Algorithm 1 Pseudocode for Strategies for ^nC_m problems

```
PIN[i] ← i^th remaining PIN
bank[i] ← i^th position requested

procedure Max
    count ← zero(10^m)
    for each p in PIN[] do
        v ← digits of p at bank
        count[v]++
    end for
    return arg max_v count[v]
end procedure

procedure EducatedGuess
    p ← random PIN from PIN[]
    v ← digits of p at bank
    return v
end procedure

procedure Random
    p ← random from 0 – 10^n − 1
    v ← digits of p at bank
    return v
end procedure

Init:
    RRdigit ← zero(n)
procedure RoundRobin
    v ← 0
    for each d in bank[] do
        v ← 10 × v + RRdigit[d]
        RRdigit[d]++ mod 10
    end for
    return v
end procedure
```

2.3.3 Computational Complexity

In this section we look at the computational complexity for each strategy. Namely this means looking at how much work each guessing step does. Later in this chapter we observe how many guesses are garnered in these steps.

The **Max method** must:

1. Walk through each item in the pinlist, extract the m digits and then increment the frequency of each — this is $O(PINLISTLEN * m)$.
2. It must then find the most frequent combination — this can actually be done in parallel with step one.
3. Then the m digits must be extracted and sent to the bank — this is $O(m)$.
4. Finally the pinlist must be updated by filtering on each of the m digits based on the bank's response — this is $O(PINLISTLEN * m)$.

The total is $O((2 * PINLISTLEN + 1) * m)$.

The **Educated Guess** method must:

1. Pick a random item from the pinlist, which if the length is tracked can be done close to $O(\log(PINLISTLEN)) \approx O(1)$.
2. Then it must extract the m digits.
3. Finally it updates the pinlist based on the response.

The total will be $O(1+(PINLISTLEN+1)*m)$, so slightly faster than the Max strategy.

For **Round Robin**;

1. m digits must be incremented and then m digits sent to the bank.

Maintaining the pinlist is not necessary, so $O(2m)$, considerably faster than the smarter strategy.

For the **Random** strategy;

1. m random digits must be selected and sent to the bank.

Like Round Robin, it will be $O(2m)$ (or $O(n+m)$ if you choose to generate a full set of random digits).

From looking at each method we note that Max and Educated method require more effort per step, but, as we shall see later, this amounts to more reward for this effort with more guesses. Equally for Random and Round Robin method, these do not require much effort but as a result do not guess as efficiently.

2.3.4 The Mathematics Behind The Strategies

In this section, we briefly consider some analysis that can be carried out on the PIN guessing strategies.

2.3.4.1 Stepwise Optimality of Max Strategy

It is possible to analyse the guessing process at each step. Suppose we are at a point in the guessing process where N entries remain on the PIN list. The bank asks about m positions in the PIN. We let $N_{d_1 \dots d_m}$ be the number of entries in the PIN list with the digit d_1 in the first requested position, digit d_2 in the second requested position, and so on. If PINs are initially assigned uniformly at random, then the chance of guessing the digits $d_1 \dots d_m$ correctly will be

$$p_{d_1 \dots d_m} = N_{d_1 \dots d_m}/N.$$

Using this probability, we can aim to choose the digits that maximise the chance of particular outcomes. For example, to aim to maximise the chance of a successful login on the next guess, we choose the digits $d_1 \dots d_m$ with the highest frequency, corresponding exactly to our Max strategy.

One might also aim to minimise the expected number of entries that remain on the PIN list, thus reducing its size as quickly as possible. If we choose $d_1 \dots d_m$ and we are correct, then just $N_{d_1 \dots d_m}$ will remain after this guess. If we are incorrect, then all combinations not matching these digits will remain, i.e. $N - N_{d_1 \dots d_m}$ combinations. Thus, to achieve this aim we choose the digits to minimise

$$p_{d_1 \dots d_m} N_{d_1 \dots d_m} + (1 - p_{d_1 \dots d_m})(N - N_{d_1 \dots d_m}) = N \left(p_{d_1 \dots d_m}^2 + (1 - p_{d_1 \dots d_m})^2 \right).$$

Note that this function is quadratic in $p_{d_1 \dots d_m}$ with a minimum at 0.5. Thus, to minimise the size of the remaining PIN list, we should choose the combination of digits that has frequency closest to half the number of remaining PINs. As it is unusual to have one combination of digits to be the majority of the PIN list, this aim will also usually correspond to the Max strategy.

A slightly more cautious aim might be to select the digits that minimise the remaining size of PIN list in the worst case, regardless of whether it is a correct guess or not. Here, we choose the digits that minimise

$$\max(N_{d_1 \dots d_m}, N - N_{d_1 \dots d_m}).$$

This is a piecewise linear function in $N_{d_1 \dots d_m}$, with a minimum at $N/2$. So again, we should choose the combination of digits that is closest to half the remaining digits. As noted above, this aim usually corresponds to the Max strategy.

Interestingly, the three above aims usually result in the same action as our Max strategy, providing no single combination of digits is in the majority. Consequently, we expect that the Max strategy should perform well in terms of both reducing the size of the PIN list and achieving successful logins. Note that each of these aims are greedy, in the sense that they optimise gains one step ahead.

2.4 Results

We chose our PIN and partial PIN sizes based on the fact that most banks use PINs ranging from 4 to 6 digits, while partial PINs typically range from 2 to 3 digits. This information was identified through online searches relating to Banks and PIN sizes along with research conducted by Aspinall et al. [36], who documented banks and their respective PIN and partial PIN sizes. PINs longer than 6 digits would require substantial computing power and time to guess. Additionally, the number of runs for PIN guessing was determined based on time constraints and necessity. Bigger PIN numbers required longer times for more runs, therefore we experimented with run sizes. For example, 1000 runs did not provide significantly more information than 500 runs, aside from improving the visual appearance of our waterfall graphs.

As an initial example, consider a single run of the ${}^4C_2$ problem using each strategy. In Fig. 2.3 the y-axis displays the remaining number of entries on the PIN list (log scale), and the number of guesses taken is shown on the x-axis. We see that for each strategy, the number of entries on the PIN list gradually decreases, with occasional sudden drops. These drops correspond to a successful login attempt, which typically removes many entries from the PIN list. Looking at the Max strategy, this happens quite quickly at around 70 guesses, followed by the Educated Guess method, and then the Round Robin method. Lastly the Random method has a success after about 300 guesses. When the lines reach $y = 1$, the full PIN has been discovered, which occurs in the same order as the drops: Max, Educated Guess, Round Robin and finally Random.

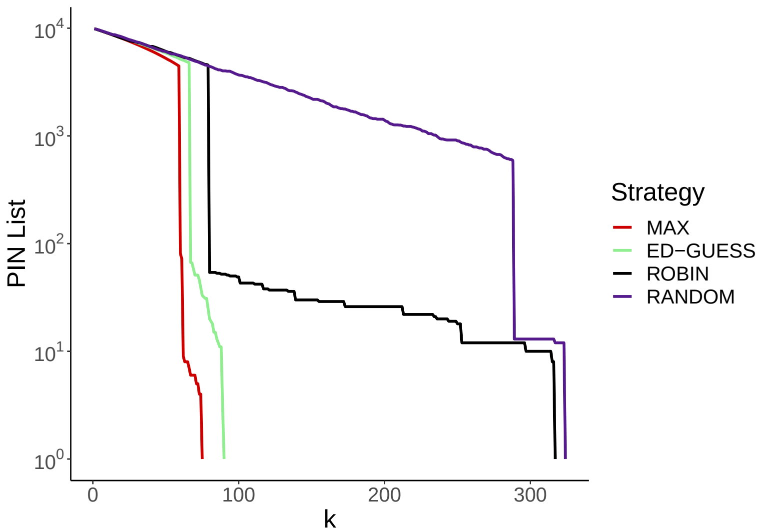


Figure 2.3: The number of remaining entries (log scale) in the PIN list after each guess k for guessing $m = 2$ digits from $n = 4$.

As we will see, this ordering is typical of the general case, as is the larger gap between the Max/Educated Guess and the Random/Round Robin strategies. As mentioned in Sec.2.3.2, the reason for this gap can be explained by the fact that the Max Method and Educated Guess method both avail of a list of all possible PIN combinations to make informed guessing choices where as random and round robin make their guesses independently of this list and therefore take much longer to make correct guesses.

The statistics in Table 2.3 show the smallest, 1st quartile, median, mean, 3rd quartile and maximum number of guesses required by each method to determine the full PIN. These results were gathered from the data collected from running the guessing process for each method 1000 times in Python. The programme documented how many guesses it took to guess a full PIN for each run and directly loaded the information into an Excel sheet which we uploaded to R to create a statistical table. Apart from the minimum and the maximum, which we expect to be influenced by outliers, each of these statistics ranks the guessing methods in the same order as before. We note that the Round Robin and Random methods actually perform quite similarly in these statistics. While Max and Educated Guess perform better, there does seem to be a gap between their performance, as we expect. The average amount of guesses for Max and Educated Guess methods combined is around 85 guesses, while the average for Round Robin and Random method combined is 645 guesses, a difference of 560 guesses.

	Max	**EdGuess**	**RRobin**	**Rand**
Min	4.00	5.00	13.00	5.00
1st Qu	42.00	43.75	196.00	201.00
Median	68.00	80.00	299.00	303.50
Mean	74.59	95.93	318.20	326.60
3rd Qu	103.00	134.00	422.20	429.20
Max	171.00	309.00	1098.00	996.00

Table 2.3: Statistical summary of number of guesses required for determination of the full PIN. 1000 runs for guessing $m = 2$ digits from $n = 4$.

In Fig. 2.4 , we have plotted 100 different runs for each strategy. Each path represents a different PIN and combination of requested positions. If we take a closer look at the Max strategy graph, each path drops quite sharply once the first pair of digits has been guessed, with a similar pattern evident for the Educated Guess strategy. This is explained by the fact that large portions of the PIN list are being deleted when a partial PIN guess is correct. When the guess is wrong, one number is deleted, but when a guess is correct, the list deletes all numbers from the list that do not have that requested partial PIN in those positions. We do see a similar pattern for the Round Robin and Random strategies, however the times at which these two digits are guessed is typically later, and so the gain is delayed. We also note that before these jumps, the Round Robin and Random strategies seem to be decreasing at a log-linear scale, whereas the Max and Educated Guess strategies seem to be reducing it at a super-log-linear rate. Log linear refers to the mathematical relationship between the x and y axis, so in this case; the guesses and the PIN list. It highlights the dependence on the PIN list for the Max and Educated Guess methods which utilise the PIN list and thus the list reduces at a super-log-linear rate. Compared to the Random and Round Robin method which does decrease at a log linear scale but less so, as they do not utilise the list and are therefore not dependent on it and as a result the relationship is not as strong as the former two methods.

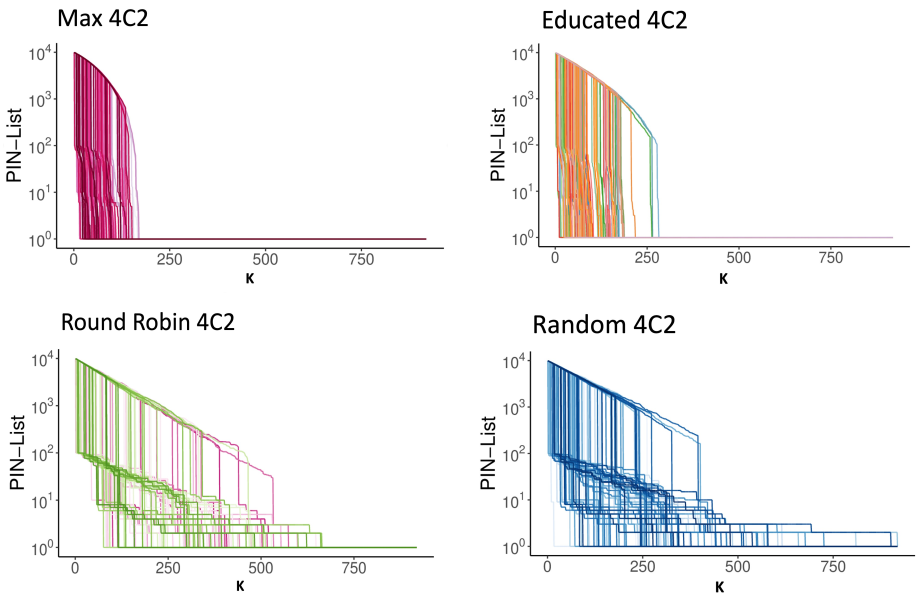


Figure 2.4: Number of remaining entries (log scale) in PIN list after each guess (k) for guessing $m = 2$ digits from $n = 4$. Each line represents an individual run for one random PIN, totalling in a 100 runs of each strategy.

While the paths shown in Fig. 2.4 are quite useful for understanding the details of the performance of each strategy, it is useful to summarise their performance. In Fig. 2.6 and Table 2.3, we display results for 1000 runs of each method, in other words, 1000 different PINs are guessed using each strategy, with different combinations of random positions being selected each time. The box plots in Fig. 2.6 reveals the summary of the data collected for both the number of guesses for the successful login (partial PIN guessed correctly), and the number of guesses where all four digits of the PIN have been guessed. The box plot displays how the

Max method is the most efficient for both measures (first and final log in), with smaller medians and also less spread. The Educated Guess strategy is almost as effective, with slightly more spread (more guesses). The Round Robin and Random methods have higher medians and more outliers, again behaving similarly.

2.4.1 Results for Various Partial PIN

In the previous example, we considered a single ${}^4C_2$ problem, where we provided two digits from four. In this section, we look at the performance of the strategies on other PIN sizes over many trials.

Fig. 2.7 summarises the results for 500 runs of each ${}^nC_m$ problem, using a box plot[15] to show the number of guesses for different strategies and different values of n and m. The first column displays different PIN sizes for the Max method, each individual box in this column then displays results for different partial PINs for that full PIN size. For example starting at the top, we have Max ${}^3C_m$ and this graph displays partial PIN (m) sizes ranging from $m = 1$ to $m = 3$. At the end of this column is results for the Max method ${}^6C_m$ with partial PIN (m) sizes ranging from $m = 1$ to $m = 6$. Moving to the right we display results for Educated Guess and the Random method in the same manner. The size of the PIN and partial PIN is depicted on the y axis and the number of guesses is depicted on the x axis. Each 'box' represents the amount of guesses needed for that PIN and partial PIN size. As can be seen in the graph the bigger the partial PIN gets the further right the box moves. The top row (row A) shows results for $n = 3$ and the bottom row (row D) shows results for $n = 6$. Within the plot for each n value, results for subsets of size $m \leq n$ are shown. We show results for each of the Max, Educated Guess and Random strategies.

For example, consider the ${}^3C_m$ guessing problem in the top row (row A). It becomes harder to guess the PIN as m increases for all strategies. In other words, the bigger the partial PIN the harder it is to guess. We can also see that the performance

[15] A box plot (also known as a box-and-whisker plot) visually represents the distribution of numeric data across one or more groups. The box shows the central 50% of the data, with a line inside marking the median. Lines (whiskers) extend from the box to represent the range of the remaining data, and dots beyond the whiskers indicate outliers [307].

of the Max and Educated Guess strategies is broadly similar, with Max having a slight edge. The Random strategy lags, with the smallest relative gap for ${}^{3}C_{3}$.

Round Robin results are similar to Random except in the ${}^{n}C_{1}$, where it follows Max/Educated Guess (as discussed in Sec. A.1) and the ${}^{n}C_{n}$ case, where it usually fails (as discussed in Sec. 2.3 and why we have shown results separately from Fig. 2.7). Each dot represents the number of guesses required to find the full PIN for a single run, with boxes showing the first and third quartile. Notches give a 95% confidence interval for the median. A line joining the means has also been included to highlight how the mean changes as m increases see Fig. 2.5.

If we look at the Random method it is visually evident the uniformity of difficulty in guessing from the linear progression of PIN and partial PIN sizes. However moving from right to left looking at Educated Guess and Max method, we can see full PINs are much more difficult to guess compared to their partial PIN counterparts. For example ${}^{3}C_{1}$ and ${}^{3}C_{2}$ are guessed quicker than the full PIN of ${}^{3}C_{3}$. These graphs highlight how much more secure full PINs are compared to partial PINs.

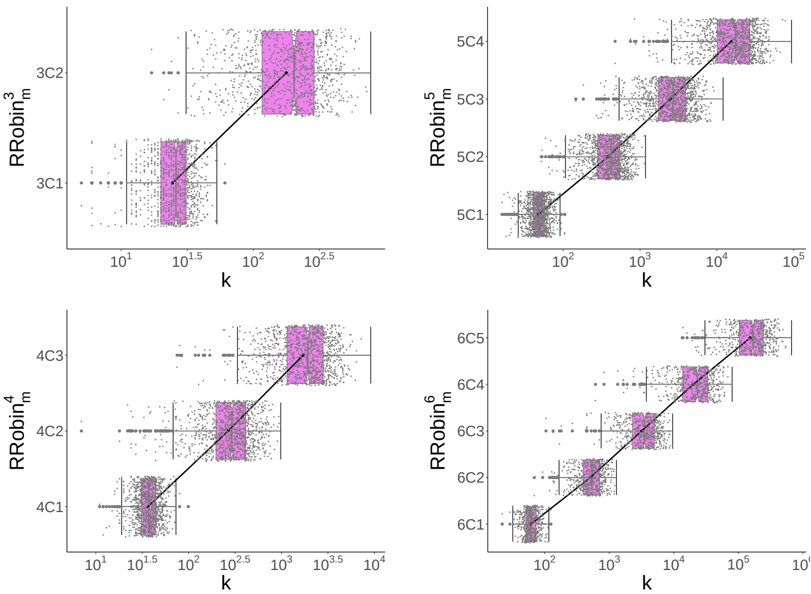


Figure 2.5: Summary of number of guesses (k) for Round Robin strategies, $n = 3$ for $m = 1, 2$, $n = 4$ for $m = 1, 2, 3$, $n = 5$ for $m = 1, 2, 3, 4$ and $n = 6$ for $m = 1, 2, 3, 4, 5$. 500 runs (Box 1st/3rd quartile, whisker ± 1.5IQR).

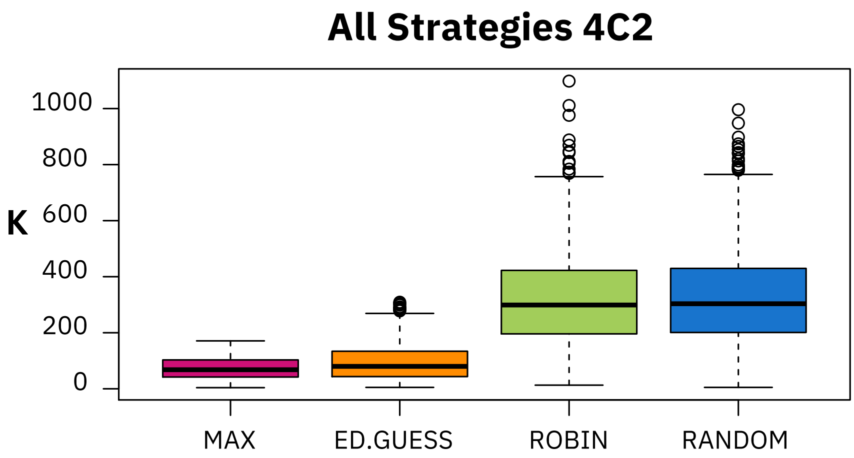


Figure 2.6: Box plots showing summary of number of guesses (k) required for determination of full PIN. 1000 runs for guessing $m = 2$ digits from $n = 4$ for all strategies (Box $1^{\text{st}}/3^{\text{rd}}$ quartile, whisker $\pm$ 1.5IQR).

Looking at the left edge of the box gives the number of guesses required for a 25% success rate in determining the full PIN. With the Max strategy, we obtain the PIN with a 25% success rate with approximately 20, 30 and 250 guesses for ${}^3C_1$, ${}^3C_2$ and ${}^3C_3$ respectively.

Similar results are presented for ${}^nC_m$ for $n = 4, 5, 6$ in rows B, C and D, respectively. We see that the ordering of the schemes and increase with m is broadly maintained. Interestingly, for the Max strategy, if we keep m fixed and increase n, we see a relatively small increase in the median number of guesses. We also see that the number of guesses required for a 25% chance to obtain the full PIN can be surprisingly small. For example, in the ${}^4C_2$ case it is between 45 and 50 guesses and the ${}^6C_3$ it is between 290 and 300 guesses.

2.4.2 Comparison of Strategies

To allow a comparison of the performance of different strategies, Fig. 2.8 shows the results for ${}^6C_m$ problems, plotting the cumulative distribution function (CDF)[16] for the strategies on a single graph. The x axis displays again the amount of guesses needed to guess the full PIN and the y axis shows the probability of guessing the full PIN. The strategies (lines) which are further left on the graph, are more likely to recover the full PIN quickly. These graphs show several interesting features that are observed in our results for ${}^nC_m$ for other values of n.

First, observe that as expected in the ${}^6C_1$ case, we see that Max, Educated Guess and Round Robin all have similar performance, with a 50% chance of recovering the PIN in around 60 guesses. Random slows down considerably once more than a handful of guesses are made. Like Fig. 2.7, this graph also shows how full PINs are safer as each method is performing the same for ${}^6C_6$.

Again, as expected from Sec. A.1, we see that Max and Educated Guess perform equally well for ${}^6C_6$ problems, always guessing the pin in less than 1,000,000 guesses. The Random scheme lags slightly initially, with a long tail where it is unlucky and repeatedly makes incorrect guesses.

Between the extremes of ${}^6C_1$ and ${}^6C_6$, we see that Round Robin and Random perform similarly, both lagging behind Max and Educated Guess considerably. For smaller numbers of guesses, Educated Guess and Max behave similarly. However, Max makes more efficient use of what it has learned if the number of guesses is large.

2.4.3 Varying n and m in ${}^nC_m$

In the previous subsection, we compared the performance of our strategies. However, it is also reasonable to ask how the difficulty in the guessing problem changes as we vary n and m in more detail. If we fix m and increase n, the impact seems clear: increasing n increases the number of initially unknown digits without chang-

[16]The cumulative distribution function (CDF) describes the probability distribution of random variables. It applies to discrete, continuous, or mixed variables and is obtained by summing the probability density function to get the cumulative probability for a random variable.

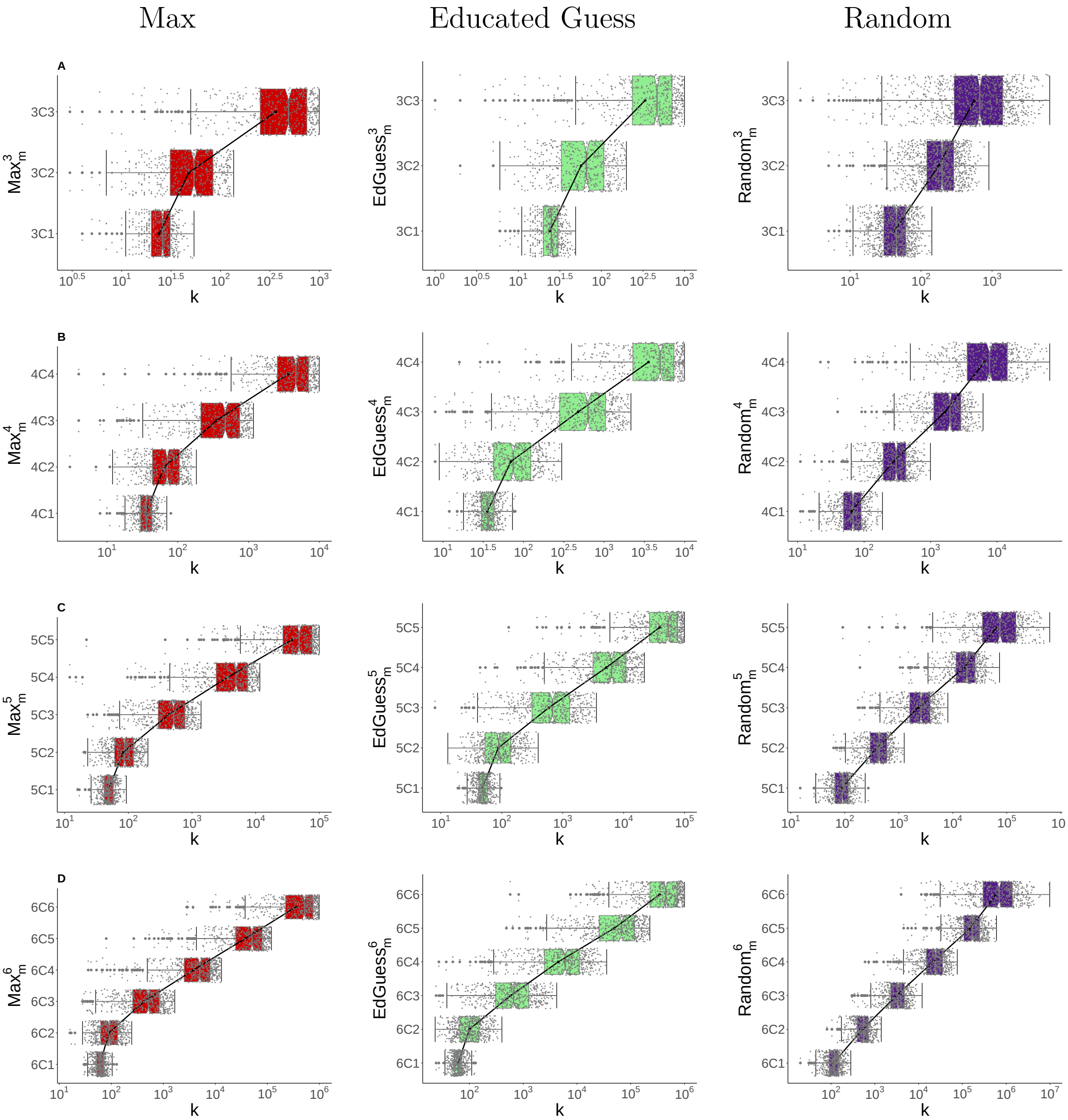


Figure 2.7: Summary of number of guesses (k) required for Max/Educated Guess/Random strategies, Row A: $n = 3$ for $m = 1, 2, 3$, Row B: $n = 4$ for $m = 1, 2, 3, 4$, Row C: $n = 5$ for $m = 1, 2, 3, 4, 5$ and Row D: $n = 6$ for $m = 1, 2, 3, 4, 5, 6$, 500 runs (Box $1^{\text{st}}/3^{\text{rd}}$ quartile, whisker $\pm$ 1.5IQR).

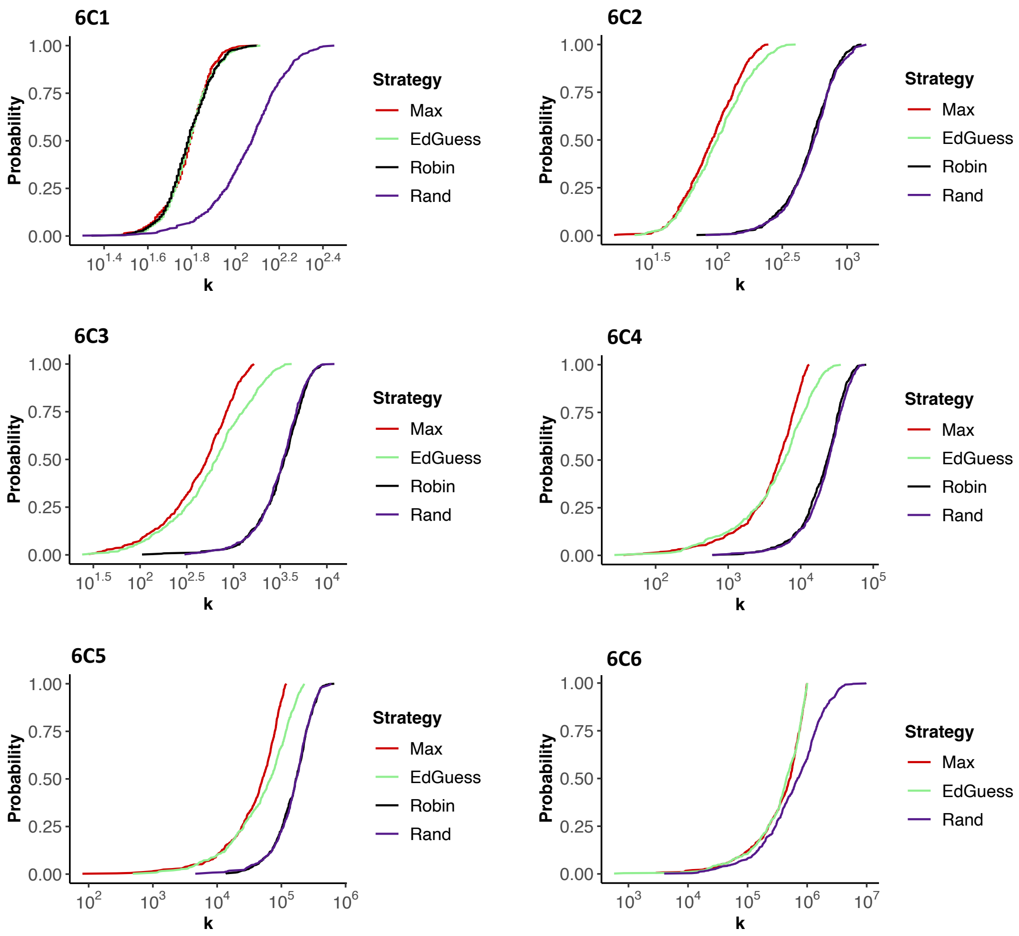


Figure 2.8: The empirical CDF for the number of guesses (k) required to recover a PIN for a ${}^6C_m$ problem for each strategy. Top row $m = 1, 2, 3$. Bottom row $m = 4, 5, 6$. 500 runs.

ing the difficulty of the individual guesses. Indeed, this matches what we see in practice.

If we fix n and increase m, the situation is more complex. Increasing m increases how much we learn on each step, while also making the probability of a successful guess less likely. This is because the bigger m gets the more PINs are deleted from the PIN list after each correct guess. The bigger m gets however, also makes the chances of guessing this partial PIN correctly less likely than if it were smaller. As a successful guess usually provides the most information, it is not immediately obvious how these factors trade off against one another for different measures of difficulty. In other words, the benefits don't cancel out the difficulty in guessing this larger partial PIN.

Fig. 2.11 shows the results of fixing $n = 6$ while varying m for each of our four strategies. We present the ECDF for various values of m on a single graph for each strategy. We see that as m increases, the graphs move to the right. This indicates that an increase in the number of guesses required to achieve any particular success rate, indicating stochastic dominance[17]. We conclude that increasing m increases the difficulty of recovering the PIN by guessing.

Additional graphs displaying the results of guessing different sized PINs and partial PINs using each strategy can be found in Appendix B. This appendix also includes CDF graphs comparing the empirical and theoretical results of the various strategies.

2.4.4 First & Last Successful Log In

Up until now, our focus has been to compare our methods in discovering the full PIN via its partial PIN. But what about the scenario where Craig is satisfied with accessing Eve's banking app just once? In this section, we examine the relative efficiency of our methods in determining the initial correct login, versus attempting to guess the complete PIN. As we discovered in Sec. 2.3.4, the Max method is the

[17] Stochastic dominance is a way to compare random variables, often used in decision theory. It ranks one gamble as better than another for many decision-makers, based on shared preferences for outcomes and their probabilities. Limited knowledge of preferences is needed to determine dominance. Risk aversion is relevant only in second-order stochastic dominance [301].

most effective in optimising the chance of a successful login at each step. From this analysis, it is likely that it would also be the most efficient at guessing the first successful log in before other methods would. Fig. 2.9 depicts simulations for guessing a full PIN of 6 with a partial PIN of 3, which is the size of Bank of Ireland's partial PIN system. We can see, that for a 25% chance of guessing the first partial PIN, Max method requires around 250 guesses. Educated Guess, Robin and Random all requiring over 300 guesses. For a 100% chance, Max requires roughly 2500 guesses, Educated Guess, Robin and Random between 4000 and 5000. Fig.2.10 displays first log in success for all strategies using the most commonly found partial PIN sizes. As seen in previous graphs in this chapter, Educated Guess follows relatively closely behind Max with Round Robin and Random lagging behind, Robin always fairing slightly better than Random. Comparing the methods for guessing the final log in after guessing the first log in, we can see that the Max and Educated guess method, guess the final full PIN relatively shortly after guessing first log in. Round Robin and Random both have significant gaps in-between guessing first log in and final log in. Additional results for various PIN sizes and their respective partial PIN sizes for first and final log in can be seen in Appendix B.4.

2.5 Discussion

In designing our strategies, our analysis indicated that the Max strategy should be effective in discovering the PIN most quickly, and this has been borne out. However, the performance of the Educated Guess strategy can approach the Max strategy. By consulting Alg. 1, we can see that while Educated Guess also uses a PIN list, its implementation is simpler and so less computationally complex than the Max strategy. This was noted in the time taken for each method to run. The Round Robin and Random strategies do not require a PIN list to generate guesses, however their performance is significantly worse in most cases.

If n is fixed and m is increased, the difficulty of guessing increases. Going back to Fig. 2.7, we observe approximately convex behaviour for the mean/median of the strategies on a log scale. In fact, if we restrict our attention to the ${}^{n}C_{m}$ problems with $m > 1$, the observed pattern is almost (log-)linear. We conjecture the existence of this convex behaviour in general. If confirmed, this behaviour

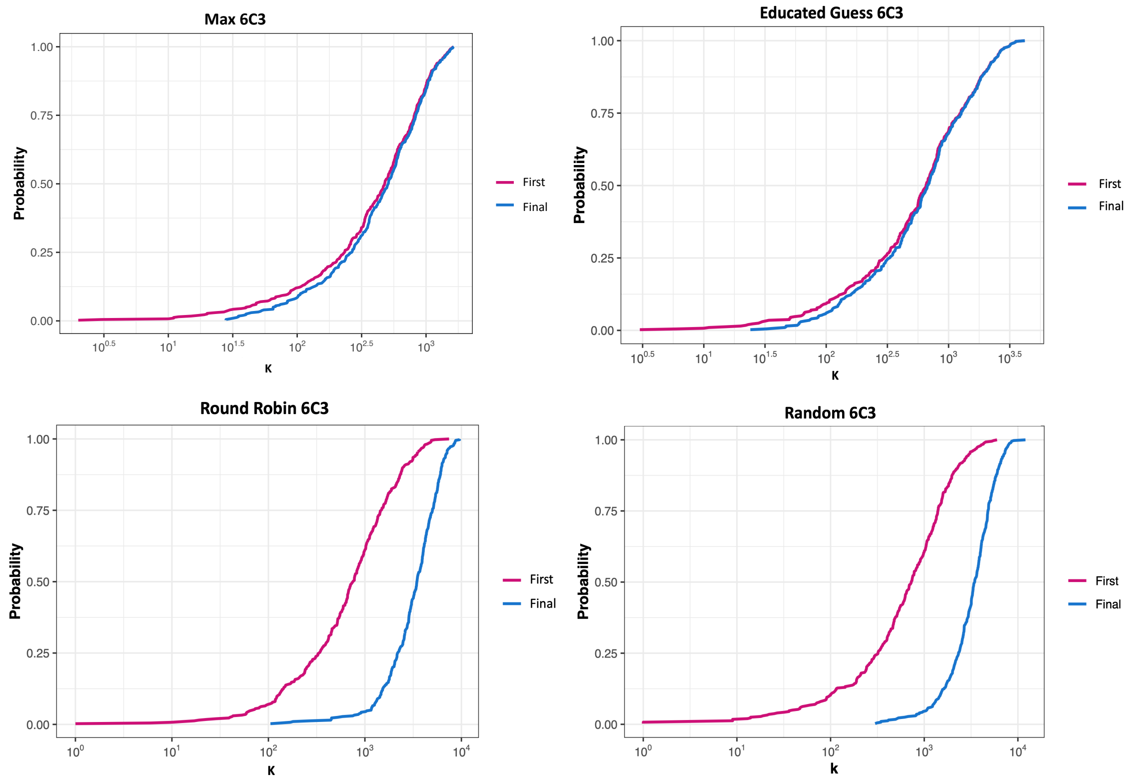


Figure 2.9: Empirical cumulative distribution frequency graphs for all strategies showing first & final successful guesses (log in) for ${}^6C_3$, k representing number of guesses made.

could be used to bound the guessing cost of ${}^nC_m$. We have provided an analysis of ${}^nC_n$ and ${}^nC_1$ in Appendix A. Alternatively, techniques such as Large Deviations might be used to give asymptotic estimates, as they have been for the guesswork of various distributions [89, 121, 189].

The Max strategy seems to require relatively little extra effort to guess a ${}^nC_m$ as n increases and m is fixed. This possibly indicates efficient use of cross-position information learned as guesses are made.

Increasing m, the number of digits requested, results in more guesses being required to identify the full PIN. This might be considered counter-intuitive, as partial PINs are intended to make it harder to reuse snooped PIN information. We have also seen that with moderate numbers of guesses ($10s-100s$) it is possible to recover a

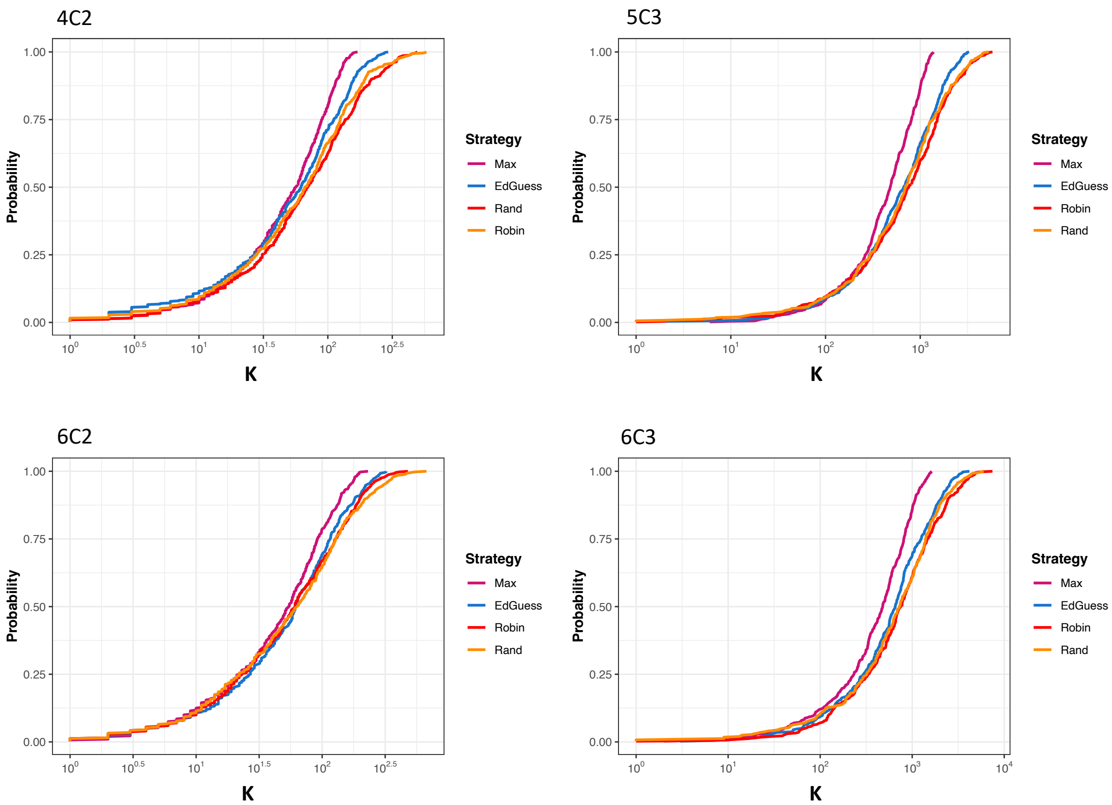


Figure 2.10: Empirical CDF for all strategies' first log in for most used partial PIN ratios ${}^{n}C_{m}$, where k = guess.

reasonable fraction of PINs when using the more efficient strategies. At one guess per day, a 25% success rate is possible for ${}^{4}C_{2}$ in under two months and for ${}^{6}C_{3}$ in under a year.

In this chapter, we have mainly focused on strategies for an attacker for guessing a PIN that was assigned uniformly at random. However, PINs might be non-uniformly assigned. For example, the method of assignment of 4-digit (non-partial) PINs to ATM cards analysed by Kuhn is non-uniform and allows an attacker to identify particular PINs that have higher probability giving an approximately 0.7% chance of guessing the PIN in three guesses [183]. In this case, the non-uniformity arises from the mapping of the output from the DES cipher to decimal digits.

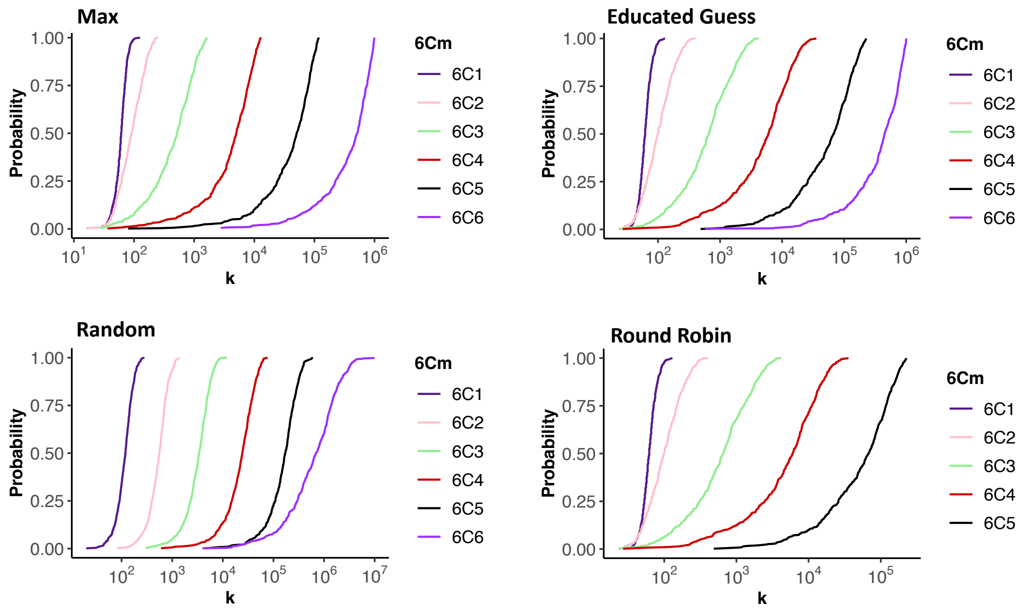


Figure 2.11: The empirical CDF for the number of guesses (k) required to recover a PIN for a ${}^6C_m$. Top row Max, Educated guess. Bottom row Random and Round Robin. 500 runs.

Aspinall and Just also exploit non-uniformity in the context of partial passwords [36], however they are more focused on the situation where the non-uniformity arises because of factors such as user choice, where it is known that password choices are non-uniform [202]. In this situation, non-uniformity can provide a huge advantage. Using synthetic data based on the RockYou leak, Aspinall and Just are able to achieve over 10% coverage in a single guess! Hence the importance of advice to implement blocklists of common PINs where user-selected PINs are permitted [63].

In the introduction, we noted that our attacks correspond to an adaptive projection dictionary attack proposed in Aspinall and Just's future work. Here *dictionary* corresponds to our PIN list, *projection* means that we use the PIN list by summarising the information at the requested digit positions and *adaptive* means that we prune the PIN list after each guess. Our results show that both Max and Educated Guess are effective, even in the case where PINs are uniformly assigned, if a moderate number of guesses are possible. We expect the advantage from these strategies can be combined with the advantages of non-uniformity. Indeed, our Max and Educated Guess strategies can actually be easily extended to the non-uniform situation by weighting each PIN with any prior information, requiring small modifications to the procedures in Alg. 1.

We note that other attacks are possible, for example, an attacker might evesdrop on the communication and try to determine the full PIN by observing multiple successful logins. In this case, the analysis is the same as when a dictionary of passwords is available, and the distribution of successes has been calculated (see the *pure recording attack* [36]). As observed previously, incomplete information gained by evesdropping can easily be used as input to our guessing strategies via the initial set S.

2.5.1 Partial PINs & The Seven Principles of Universal Design

As we note in the Chapter 1, we aimed to examine how each topic in this thesis aligns with the seven principles of universal design [5]. For partial PINs we feel that they fail in respect to principle one with regards to equitable use. In Sec.2.1.4 we noted that recalling PINs can be difficult at the best of times for people with memory issues and we feel that partial PINs can add to this cognitive burden. Principle one states that the provisions for privacy and security should be available for all users. We also feel that partial PINs fall short on principle five, tolerance for error, where the design reduces risks and mitigates the negative outcomes of unintentional or accidental actions. For users with memory issues inputting wrong digits can cause banking apps to lock them out, which in turn can potentially cause anxiety.

2.5.2 Future Work & Limitations

For this chapter we acknowledge that the 'in the wild' scenarios mentioned could be considered unrealistic, which include guessing a persons bank PIN in the presence of 2FA. However we feel it is necessary to highlight any potential limitation in this method of authentication. As noted previously, research is limited surrounding partial PINs in general, therefore the storing of partial PINs or password is also limited. Investigation into the storing and hashing of partial passwords could be explored.

While we have shown that our Max strategy is, in some senses, stepwise optimal, it is not clear if more effective overall strategies may exist. In addition, there may also be defensive strategies, for example adapting the digit positions requested when it is believed that an attack is ongoing. The simplest version of such a strategy might involve requesting the same digit positions until a successful login occurs. In these cases the design choices around our Max and Educated Guess strategy still hold, though the details of the performance analysis will be changed. We leave the performance and design of such defensive strategies as future work. Further work could also explore longer PINs and probabilistic analysis to predict the performance of our strategies.

In terms of usability, further work could focus on how usable partial PINs are in comparison with full PINs especially for people with disabilities. Memory could also be addressed in comparing partial and full PINs.

2.6 Conclusion

We have looked at strategies for guessing a PIN in a system where m digits from n are requested at login. We have identified two efficient strategies that make use of a PIN list. We have evaluated these strategies in the case where the PIN has 3–6 digits, providing curves that show the success rate after a number of guesses. The number of guesses increases with both n and m, though more slowly for n. Our results indicate it is often possible to have a moderate chance of recovering the full PIN with tens to hundreds of guesses. While we have shown that our Max strategy is stepwise optimal, it is not clear of more effective strategies may exist.

As physical banks are rapidly closing all over Ireland [294], older adults have to adapt to digital banking which can be challenging [31], and adding complexity to the process offers no benefit. Considering that passwords and PINs already present challenges for vulnerable users such as the older generation [250], our findings show that partial PINs potentially add more complexity than security.

CHAPTER 3

The Landscape of Irish Cookie Banners

Kampanos and Shahandashti extended the OpenWPM software to analyse Greek and English cookie banners, concluding their paper by encouraging others to use their code for similar studies in different countries. We accepted this challenge and extend it to observe how cookie banners could potentially impact vulnerable cohorts. We compare our findings to theirs, as well as the Data Protection Commission (DPC) of Ireland's report on Irish cookie banners. Our study revealed similar patterns, with some improvement in banner prevalence and other metrics reported by the DPC. We also identified invisible banners, where the HTML for a banner exists but is not displayed. Additionally, the Irish word for cookies is interchangeably referred to as Fianán or Cuacha and was not commonly found on Irish websites.

3.1 Introduction

Cookie banners are mostly unavoidable in modern web browsing, however they are useful in how they make perusing the Internet easier; allowing websites to remember what is in our online shopping carts and to remember we have already authenticated. These are known as *session cookies* and *authentication cookies* and are the sort of cookies that many people want permitted, perhaps depending on the lifetime of that cookie. The rejection rate of cookies however, is quite high, which shows that customers are being put off by cookies [247]. This rejection rate is likely caused by *third-party* cookies, which are cookies set by websites other than the one you appear to be visiting. These cookies can be traced back as far as 1996 [275] and are significant when regarding users' privacy online, as they allow a user to be tracked as they visit multiple websites.

We conducted a casual Twitter survey which revealed that 55% of participants hit the most obvious button on a cookie banner, 31% carefully chose an option, 7% left the website, with 6% choosing other. The comments following the survey were particularly interesting. Some participants had a procedure, where they will click 'accept all' and eventually clear cookies at a later date. Others choose based on the website itself, where given an all or nothing choice they may leave, depending on whether a website is deemed to be 'trustworthy'. This choice based on perceived 'trustworthiness' was also noted in a user study on cookie banners conducted by Kulyk et al. [184]. However, for the most part, it appeared participants did not put much thought into cookies.

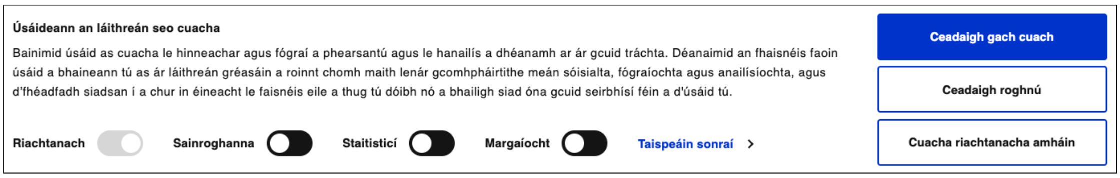


Figure 3.1: One of the few cookie banners in the Irish language found in this study from `tg4.ie`.

The combination of cookie usage creates a challenge for users in deciding what cookies they should accept, this can be extra challenging for a vulnerable user. In general what a person needs to consider when faced with a cookie banner is "...what purpose they serve, how long they endure, and their provenance." [178].

Cookie banners (or consent notifications) were created with the intention of informing the user of their rights and full disclosure of what data is being used, while allowing control over what data is stored. The reality may seem to be otherwise: cookies are more of an annoying chore for both website owners and users [184].

The problem appears to be that either people seem less concerned about their privacy or are just ignorant of what is happening to their data [223].

From a user's point of view, the perception of cookies is overall negative, with studies showing users to be annoyed about cookies and the lack of information surrounding them [184]. Trust in the website itself seemed to have more influence over the user than the banner, which we also observed in our casual Twitter survey.

3.1.1 Objectives & Contributions

In this chapter, our objective is explore the landscape of Irish cookie banners. Our research questions being:

RQ2:1 Do Irish cookie banners adhere to GDPR?

RQ2:2 What manipulative practices (dark patterns) and barriers are present (if any) in managing cookies.

RQ2:3 Do Irish cookie banners align with the seven principles of design?

In answering some of these questions we can also note how banners can potentially impact more vulnerable users.

To address these questions, we adapted Kampanos's OpenWPM framework to accommodate the nuances of Irish cookie language and compiled our own list of Irish websites [245,246]. Combined with the Tranco[1] list of websites, four thousand Irish websites were identified to investigate. Most cookie studies take the most popular websites to analyse, however our list also takes into account lower traffic websites. The data from the crawl was analysed to identify banner and cookie prevalence along with language and visual differences of Irish banners as well as *dark patterns*.

We submitted our findings to the Data Protection Committee as a contribution to their existing research on Irish cookie banner GDPR compliance. We note

[1]Tranco is a ranking service which provides up to date lists of popular domains `https://tranco-list.eu/`

an improvement in compliance regarding GDPR since the DPCs report regarding pre-ticked banners mentioned in Sec. 3.6.2

An additional contribution from this study is the presence of invisible banners, where it appears that there is code for a banner in the HTML but is not visible on the website. This highlights lack of attention to websites where the code may be broken and therefore the banner is not visible which is effectively not abiding by GDPR.

This chapter is laid out as follows; Sec. 3.2 explores the background on GDPR and cookies with regard to vulnerable users and privacy. Related research is discussed in Sec. 3.3. Our method for surveying cookies is described in Sec. 3.4. The results of this survey are presented in Sec. 3.5 and then discussed and compared to prior work in Sec. 3.6. We discuss cookies in the context of the seven principles of universal design in Sec. 3.6.3. Our conclusion is given in Sec. 3.7.

3.2 Background

3.2.1 Regulatory Situation

The EU formulated the General Data Protection Regulation (GDPR) for data protection and privacy in the European Union [237]. Its aim is to enhance an individual's control and rights over their personal data. Apart from *strictly necessary* cookies, a person has the right to control what data is shared and must give consent. In the EU, if a website stores a person's data as cookies, then they must display a cookie banner that clearly states what data is stored, how long it is stored and whether third-party cookies are used. A user must be able to decline data storage and accept any cookie that is used. As stated in the EU Charter of Fundamental Rights (CFR), everyone has the right to protect their personal data [93] and Recital 30 of the GDPR acknowledges that a person can be identified by their devices [237]. Associated tools and protocols can, when combined, be used to create a profile.

The GDPR is enforced by various national authorities. The Data Protection Commission (DPC) for Ireland is responsible for the enforcement of the GDPR and also ePrivacy laws, which are separate but complement the GDPR [289]. As several large companies have European headquarters in Ireland, they come under the bailiwick of the Irish DPC. The various national authorities are under pressure to uphold these laws, with some complaints claiming investigations can be ineffective and privacy is being abused [69]. Despite this, in 2021, Amazon was issued with a hefty fine of 746M euros for violating GDP regulations [287]. In fact, that same year documented some of the highest GDPR-related fines since its commencement in 2018 [287]. Amazon is a well known company and much in the spotlight however, there are many smaller websites that may be flying under the radar while violating regulations. According to online privacy activist Schrems, one reason why tech giants such as Google or Meta, along with smaller companies, opt not to abide by the GDPR is because bypassing them proves to be more profitable [46].

Consent for the use of cookies is usually sought by a cookie banner. According to article 4[11] in the GDPR, consent means any "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" [104]. Consent, however, is an abstract concept and seems to be interpreted in different ways. Krisam et al. refer to the difficulty in fulfilling GDPR requirements with cookie banners, given the architecture of the web and lack of standards [182] .

In January 2023, the European Data Protection Board (EDPB) released a report [58] specifically addressing non-essential cookies. This report addresses many of the deceptive practices seen in our study such as links to pages to change cookie settings and deceptive button colours. Regarding button colours in banners, the task force agreed that this would have to be judged on a case by case basis, as it should not be up to the data controllers to make these choices [58]. The members of the cookie banner task force asserted that pre-selected tick boxes for opt-in purposes do not result in valid consent. This conclusion is supported by references in both the GDPR, particularly recital 32, which states that "Silence, pre-ticked boxes, or inactivity should not be considered as consent", and Article 5(3) of the ePrivacy Directive [58]. Among European privacy advocates, there remains a difference of opinion regarding specific aspects, such as the necessity of including a 'reject all' button. Some regulators refer to Article 5(3) of the 2002 E-Privacy Directive, which does not require it [285].

3.2.2 The Privacy Paradox

When discussing cookie banners and GDPR compliance, *The Privacy Paradox* is an unavoidable issue. This term was first coined in 2001 [68], to describe the contradictions between user attitudes and their actions online. Despite expressing high levels of concern about their privacy, users take minimal steps to safeguard their personal information [43]. The illusion of control is a cognitive bias which is being taken advantage of online. This can be seen to be demonstrated in a study which found that it was easier to get people to donate money when presented with the phrase "but you are free to accept or refuse" [149]. The suggestion of choice can effectively alleviate the sense of mistrust triggered by perceived threats to our freedom. In psychological terms, this phenomenon is referred to as 'reactance' [239]. Alessandro Acquisti notes that as a result of our cognitive bias, we share personal data without taking full stock of the situation and the implications of our actions [30]. This is likely what is happening with cookies, under the illusion of choice as to what data we share, we happily accept all cookies. Helen Nissenbaum, a professor of information sciences at Cornell Tech, refers to this in her own terms as the "farce of consent", which deceives users into believing they have genuine control over their data [239]. According to her perspective, even well-meaning companies remain unaware of the actual fate of the data they gather [239].

Another factor that may contribute to the privacy paradox is our tendency to prioritise the importance of immediate events over possible future outcomes. Consequently, the immediate advantage of accessing an article takes precedence over the future, and potentially unsettling, consequences of sharing personal data with the relevant website [239].

When it comes to data privacy, cookie banners appear to create more of an illusion of choice. Similar in fact to *security theatre*, a term coined by computer security specialist Bruce Schneier, which describes the practice of taking security measures that provide the feeling of improved security while doing little or nothing to achieve it [4].

Design seems to be of great impact on how people choose their privacy settings and psychology and sociology play a big part in this. Thaler and Sunstein emphasise that individuals have a natural inclination to opt for the path of least resistance in decision-making [288]. They suggest this tendency arises from factors such as laziness, fear, or distraction, leading people to select options requiring minimal effort or encountering the least obstacles. Consequently, individuals often revert to the 'default' option, irrespective of its quality or consequences [288]. This makes sense in terms of clicking 'Accept All' for cookie banners when the alternative means going through several levels of options to reject cookies.

Max Schrems, an Austrian attorney, along with his privacy campaign NOYB (None of Your Business) is managing a total of 800 complaints in different jurisdictions on behalf of Internet users. According to Schrems, despite NOYB filing numerous complaints that have resulted in hundreds of millions of euros in fines, the enforcement of GDPR remains infrequent [236]. This is for numerous reasons, funding, lack of a uniform approach across different countries and the influence of big tech who have significant resources to fight and pay fines [191]. In 2021 the Irish Council for Civil Liberties reported that 98% of major GDPR cases referred to the Data Protection Commission in Ireland remain unresolved [191].

In some countries in Europe, websites use a system known as 'consent or pay' or 'cookie paywalls', which allows users to access a website for free by consenting to the use of cookies. Alternatively, users who choose not to consent can access the website by making a payment, usually in the form of a subscription [108]. The Austrian Data Protection Authority however, has declared that cookie paywalls are not GDPR compliant [16]. Schrems claims that the subscriptions with cookie paywalls, generates profits that are approximately 10 to 100 times greater than those derived from online advertising [25].

3.2.3 Consent Management Platforms

A consent management platform (CMP)[2] is software designed to help collect and manage personal information and consent in compliance with data protection laws and regulations [224]. As the GDPR can be quite complicated, many websites employ these platforms to obtain and manage consent for them and to ensure they are compliant with local regulations [261]. This means that these companies need to be up to date with GDPR. Individual European countries have their own adjustments to GDPR, which different CMPs can adjust for. Other factors that can differ among various CMPs include their data management practices and tracking methods [224]. In light of this, we take note of what websites in our subset avail of these platforms, to observe if these platforms do indeed comply with GDPR. Experte.com checked 5 million websites and found that Osano, Quantcast Choice, OneTrust, Cookiebot and Iubenda, were the top five consent management platforms for in 2023 [185]. We will see that the following CMPs are used most by Irish websites analysed in this study: CookieBot, OneTrust and CookiePro.

3.2.4 Cookies & Vulnerable Users

Regarding privacy online, Schaub and Cranor argue that simply meeting regulatory requirements is inadequate. They outline four key components necessary for effective privacy interfaces: findability, understandability, usability, and usefulness [263]. Habib et al. examine the usability of various privacy choice mechanisms designed to help users manage their privacy settings and consent to data collection practices. They demonstrate that the usability of privacy tools significantly impacts user engagement and compliance. Their findings highlight the importance of designing intuitive and accessible privacy choice mechanisms to enhance user control over personal data and privacy settings [153]. Clarke et al. evaluate the accessibility of cookie notices for users with visual impairments, focusing on visibility, readability, and audibility [94]. Their findings highlight that poor design choices, such as low contrast and small fonts, further hinder visibility. Overall, they discover that a significant number of cookie notices fail to meet basic web accessibility guidelines [94]. Carlsson et al. investigate data leaks to third parties

[2] https://www.consentmanager.net/

through web services designed for vulnerable groups. They highlight the risks and implications of such breaches, especially concerning sensitive information related to health, personal circumstances, and other protected data. Their analysis underscores the critical need for robust data protection measures in web services for vulnerable populations to safeguard their sensitive information and uphold their privacy rights [77]. Soe et al. argue that cookie consent banners without a negative option to deny consent, adds an extra cognitive burden on the user. Without the direct option to reject cookies they have to navigate more levels of the banner or manually clear cookies after [273]. In Ireland Reynolds et al. examine the cookie practices of Irish homecare companies, assessing their compliance with the General Data Protection Regulation (GDPR). They find that many homecare companies do not fully adhere to GDPR requirements, concluding that these companies must ensure proper cookie compliance to enhance user trust and data protection [252] .

The British privacy regulator Information Commissioner's Office (ICO) is taking action against dark patterns in cookie banners. Stephen Almond of the ICO notes that dark patterns can have adverse effects on people, as an example, he describes the scenario of a recovering gambling addict being nudged to accept all cookies and as a result being targeted with gambling advertisements [175].

An observation we note in collecting cookie banners, was the amount of information presented to the user. The many different options one could choose in relation to their data. Psychologist Barry Schwartz, believes that while autonomy and freedom of choice are crucial human values, an abundance of options and excessive control can overwhelm us and steer us away from making optimal decisions [265]. This could also potentially be problematic for users who are cognitively impaired or suffer from mental illness.

3.3 Related Research

Studies in this area focus mainly on GDPR compliance, how users interact with and understand cookies, cookie design and dark patterns. We review papers that look at cookie banners in different EU countries with regards to GDPR compliance and dark patterns. The web's open nature, coupled with the GDPR being complex and open to interpretation, mean that ascertaining whether websites are 100% compliant with GDPR is difficult [261]. Dark patterns however, are easier to observe and note with more confidence.

3.3.0.1 Cookie Compliance

Englehardt and Narayana employed an automated OpenWPM script to crawl one million websites and found that news websites contained the most third-party cookies [125]. Kampanos and Shahandashti discovered that banners were not universal, just 48% of Greek and 44% of the UK websites included a cookie notice [168]. They also found that, direct opt-outs were rare and that the majority of banners were positively phrased leading people to think that they can trust the website. They also note that, compared to previous similar studies on Greek and British cookies, banner prevalence had decreased. This is contrary to what might be expected with GDPR compliance. Kampanos and Shahandashti point out that this is likely to do with their large sample size, which would include smaller and less popular websites. In a study undertaken in Spain, 500 websites were examined, revealing that the top websites in the country fail to implement proper consent mechanisms and engage in user tracking. Only 8.91% of websites which obtain users' consent as required apply this consent successfully in practice [205]. Santos et al. studied 407 banners from the most visited English speaking websites in the EU and found that 89% violated at least one legal requirement [262]. Other identified issues included misleading statements, technical jargon, and vagueness. They observe another common pattern in banners: 'necessary vs unnecessary' cookies. The lack of clarity around what is strictly necessary, can leave the user to assume all cookies are necessary [262]. Degeling et al. analysed 500 websites and noted that since GDPR's enforcement, rather than helping people with their actual privacy choices, it has led to more of a sense of false security [116]. Fouad et al. investigate the legal compliance of 20,218 third-party cookies [137]. Of these cookie banners, 12.85% have a corresponding cookie policy where the word cookie is not even mentioned. They found that 95% of cookies do not have an explicitly declared purpose and are therefore impossible to audit for compliance. They also stress the need for policy makers to agree on unified requirements surrounding cookies and tracking in their definitions for purpose.

Papadogiannakis et al. point out issues with consent management platforms (CMPs) with regards to GDPR compliance [243]. Their crawling mechanism identifies CMPs but do not name any particular brands of CMPs. They also identify "a disparity between (i) what the users perceive about the collection of their data, and (ii) what some websites implement with respect to data processing". They observe that some websites collect and share data with third parties before the user has a chance to register a privacy choices. On some occasions, even if they do decline, data collection increased [243]. Matte et al. studied CMPs by crawling 1426 websites to monitor Internet Advertising Bureau (IAB) Europe's Transparency and Consent Framework [208]. They observe that 141 websites note positive consent before the user has interacted with the banner, 236 websites had pre-ticked options and 27 websites registered positive consent despite the user opting out. They detected at least one violation in 54% of their collected websites. Matte et al.'s study is the only study we noted which identifies individual countries in their European crawl [208]. They look at 25 Irish websites out of a total of 1426 using Consent Management Platforms (CMP) in their European crawl.

ZeShi Li et al. state that more research is needed in educating software developers with regards to the GDPR [190]. Lack of knowledge was also highlighted in the DPC's report, where websites were unaware of certain violations [113].

3.3.0.2 Cookie Banner Design & Dark Patterns

The CNIL[3] released a report in 2019 on dark patterns and data protection in UX/UI design. They classify dark pattern practices related to data collection online into four categories which include different design tactics. From the *Diverting the Individual* category they describe the *Bait and Change* tactic as a setting or a choice made by the user which produces a different result than desired. For instance, giving the impression that clicking x means "close and move on", when in fact you are accepting all cookies [239].

[3]The CNIL, Commission Nationale Informatique & Libertés, is the French Data Protection Agency, `https://www.cnil.fr/en`.

The Data Protection Commission Ireland conducted their own study into Irish cookie banners [113]. In this study they requested information from 38 website cookie controllers to examine the deployment of cookie technologies. Their study was prompted by complaints made about some of the websites they investigated. This report highlights examples of dark patterns, one of which comes in the form of *cookie bundling*. Here, users are asked to accept cookies, with an explanation stating that cookies are necessary for the website, so unless you look further (and often you can not), you must agree to marketing and tracking cookies. The DPC report also found that 26% of their banners displayed pre-ticked options. Our study differs from the DPC report by focusing on a direct analysis of the websites themselves. In comparison, our study is on a much larger scale, examining 3,735 websites and offering more detailed insights into the number of first and third-party cookies collected, along with specific information on each banner.

Bauer et al., found that design had an impact on user interaction with banners [45]. They tested a banner with a green accept button, hidden details for opting out and positive framing. They compared this to a banner with equal access to opting out and neutral framing. They found that dark patterns, such as highlighted buttons, have a significant effect on users' interactions. The former banner style is still prevalent and was also observed in this study. Mathur et al. refers to this type of dark pattern as an *Asymmetric* dark pattern. These types of patterns place unequal burdens on the user's selection possibilities [207] . The choices that serve the company's interests receive prominent placement, while options that are advantageous for the user are often concealed behind multiple clicks or obscured by manipulating the style and positioning of the choice. Asymmetrical dark patterns are particularly widespread in consent interfaces [207].

Machuletz and Böhme also found that users were more likely to click on highlighted buttons over neutral buttons and to subsequently regret their choices: "... users accept more data collection purposes when consent dialogues integrate a highlighted default button that selects all purposes at once" [197]. Another interesting observation from the same study discusses *multiple choice designs*. When presented with multiple choice, users found they were less likely to recall their choices and also regret them afterwards. This highlights that these multiple choices may cause confusion.

Utz et al., found that users interacted more with left-hand corner banners and, given a binary choice, were more likely to allow tracking compared to banners with options [295]. They found that overall, nudging[4] has a big impact to users' choices in online tracking. According to Bermejo Fernandez et al., the position of the banner does not affect users' participation with cookie consent, but buttons that were highlighted did have an impact on users' interactions with banners [52].

After analysing 300 consent banners from Scandinavian and English language news outlets, Soe et al. found that all utilise varying degrees of unethical tactics [273]. They argue that "any regulation of a computational systems that aims to protect the users' rights should be accompanied by a regulation of user interface design" [273].

More recent work on dark patterns in cookie banners comes from Krisham et al., who looked at 500 websites in Germany [182]. They sorted their list into categories based on the options available to the user, for example an 'Accept All' button. They found a strong prevalence towards nudging users into accepting cookies.

Graßl et al. point out that "The use of dark patterns can be problematic for legal as well as ethical reasons [145] . While the GDPR (2016) does not explicitly ban all dark patterns, they do breach the spirit of the GDPR". They refer to three common dark patterns in banners as 'Default' (pre-ticked options), 'Aesthetic Manipulation' (accept button is highlighted) and 'Obstruction' (where it is difficult to opt for more privacy friendly options). They found that dark patterns did not effect users choosing data-unfriendly options but rather it is a conditioned response for users to choose these options. A possible reason for this is that non-EU websites sometimes will not allow access to a page without consenting to tracking.

Habib et al. found in their review of 150 websites, that, although privacy choices were commonly available, they are sometimes difficult to find and understand [152]. They go on to say that privacy-choice text requires a university education to decipher and privacy policies do not do much better. McDonald et al., estimated

[4] Nudging guides users behaviours by way of interface and design in digital environments [242].

that the time needed to read the privacy policies you encountered in a year would necessitate 76 working days [210].

A report commissioned by Schillings[5] and published April 2013, revealed that measures intended to empower consumers in managing their online information actually led them to disclose more of their personal data. The study found that cookie banners' design often employed tactics aimed at discouraging users from modifying their data permissions. They used nudges to incentivise users to agree to the most permissive settings instead [165].

Many studies have focused on consent management platforms (CMPs) alone [197, 227, 273, 295]. Nouwens et al., found that dark patterns and implied consent were ubiquitous [227]. From their survey they note that people ignore controls placed below the first layer in a banner. According to Nouwens et al., consent management platforms are considered compliant with the GDPR if the consent obtained through their interface is explicit, easily customisable to accept or deny, and devoid of preselected checkboxes . Failure to meet these criteria renders the consent interface susceptible to being categorised as an unlawful dark pattern [227].

Soe et al. outline a set of eight criteria that would classify a consent management platform interface as a dark pattern under the provisions of the GDPR [273]. These include *Does not count*, where data is collected before or even when you deny cookies and *No Choice* where you are directed to different links which explain how to change browser settings to get rid of cookies. The latter we also came across in this study.

The studies mentioned in this section have analysed European websites, where they look at English speaking websites in Europe generally. Our study to the best of our knowledge is the only one to focus on Irish websites solely. The only exception to this is the study looking specifically at Irish homecare website cookies mentioned in Sec.3.2.4.

A summary of related work can be seen in Table 3.1, highlighting how our study differs from others.

[5]Legal experts on privacy and security https://www.schillingspartners.com/about/.

Table 3.1: Comparative Literature table on Cookie Banners. Highlighting the gap our study addresses in this area.

Title	**Year**	**Vulnerable Users**	**Dark Patterns**	**Ireland Only**	**GDPR Compliance**	**Web Crawl**	**Manual Crawl**
Online tracking: A 1-million-site measurement and analysis [125]	2016					✓	
Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners [261]	2019		✓		✓		✓
We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy [116]	2019				✓	✓	✓
Multiple purposes, multiple problems: A user study of consent dialogs after GDPR [197]	2019		✓		✓		
(Un) informed consent: Studying GDPR consent notices in the field [295]	2019		✓		✓		
An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites [152]	2019		✓		✓		✓

Table 3.1: Comparative literature on cookie banners. – continued from previous page.

Title	Year	Vulnerable Users	Dark Patterns	Ireland Only	GDPR Compliance	Web Crawled	Manual Crawl
Multiple purposes, multiple problems: A user study of consent dialogs after GDPR [197]	2019		✓		✓		
On compliance of cookie purposes with the purpose specification principle [137]	2020			✓	✓		
Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework [208]	2020		✓		✓	✓	✓
GDPR compliance in the context of continuous integration [190]	2020				✓		✓
Circumvention by design-dark patterns in cookie consent for online news outlets [273]	2020		✓		✓		✓
Accept all: The landscape of cookie banners in Greece and the UK [168]	2021		✓		✓	✓	✓

Table 3.1: Comparative literature on cookie banners. – continued from previous page.

Title	Year	Vulnerable Users	Dark Patterns	Ireland Only	GDPR Compliance	Web Crawled	Manual Crawl
Cookie banners, whats the purpose? Analysing cookie banner text through a legal lens [262]	2021		✓		✓		✓
User tracking in the post-cookie era: How websites bypass GDPR consent to track users [243]	2021				✓	✓	
Are you sure, you want a cookie? – The effects of choice architecture on users' decisions about sharing private online data [45]	2021		✓		✓		
This website uses nudging: Mturk workers' behaviour on cookie consent notices [52]	2021		✓		✓		
Dark patterns in the wild: Review of cookie disclaimer designs on top 500 German websites [182]	2021		✓		✓		✓
Dark and bright patterns in cookie consent requests [145]	2021		✓		✓		

Table 3.1: Comparative literature on cookie banners. – continued from previous page.

Title	Year	Vulnerable Users	Dark Patterns	Ireland Only	GDPR Compliance	Web Crawled	Manual Crawl
Web-tracking compliance: websites' level of confidence in the use of information-gathering technologies [205]	2022				✓	✓	
Fianán, Cuacha: Irish Cookie Banners [269]	2022	✓	✓	✓	✓	✓	✓

3.4 Methodology

As we are following in the footsteps of Kampanos and Shahandashti's study on cookie banners in Greece and the UK [168], to more accurately compare Ireland with Greece and the UK, we decided to also use the same tools. Kampanos et al.'s code is available on GitHub[6].

3.4.0.1 Tools Used For Crawling

OpenWPM[7] is a web privacy measurement framework, available as open source software, that can scrape websites for relevant information [126]. It is designed to use the automation features of the Mozilla Firefox browser to simulate website visits. Different browsers may function slightly differently, but the purpose of cookie banners remains the same. Therefore, we do not expect that using an alternative browser would yield different results. There are many other webcrawlers available, such as Scrapy[8] and Mechanical Soup[9] [129]. OpenWPM can be scripted, allowing it to be easily tailored for specific research questions. Consequently, it has been

[6]Kampanos and Shahandashti GitHub repo: `https://github.com/kampanosg/i-like-cookies`

[7]OpenWPM GitHub repo: `https://github.com/openwpm/OpenWPM`

[8]Scrapy web crawler: `https://scrapy.org/`

[9]Mechanical Soup:`https://pypi.org/project/MechanicalSoup/`

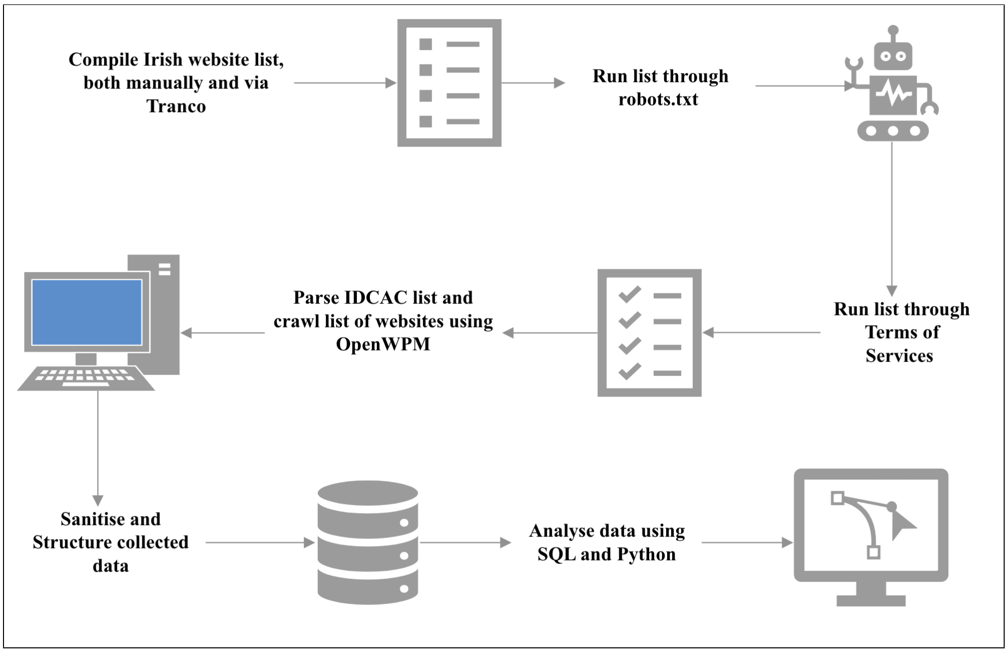


Figure 3.2: Methodology for analysing Irish cookie banners.

used in many research studies. For example, Sørenson and Kosta used OpenWPM to explore the cookie landscape before and after GDPRs activation [275].

CSS selectors[10] Are used in the design of websites to change style and layout. Kampanos et al. made modifications to OpenWPM to identify cookie banners by referring to a list of cascading style sheets [168]. These are used as a reference to identify what commands are used for cookie banners so that OpenWPM can identify the location on the page etc. The framework takes a screenshot of the banner using these selectors, and saves this as a PNG along with the HyperText Markup Language (HTML)[11] of the banner. Unfortunately, these modifications no longer apply cleanly to OpenWPM. Subsequent versions of OpenWPM include a more flexible extension framework to make these sort of modifications less intrusive. Porting Kampanos's modifications to this new framework, allowed the use of

[10] CSS selectors are a key part of Cascading Style Sheets (CSS), which is used to style HTML documents. Selectors specify which elements on a web page will be styled according to the CSS rules.

[11] HTML (HyperText Markup Language) is the standard language used to create and design web pages. It provides the structure of a webpage by using a system of tags and attributes to define elements and their content.

current versions of OpenWPM and Firefox.

Tranco provides a list of the current top one million most popular websites. Research conducted by LePochat et al. show that Tranco offers improved resilience against manipulation compared to traditional rankings, making it a valuable tool for researchers studying the web [187]. For this reason and as Kampanos et al. also availed of Tranco for their list of websites, we decided to follow suit. We also compiled our own list of Irish websites manually, by amalgamating several lists of top Irish websites, such as Irish shopping websites, found via web search. This was done to capture Irish websites outside the `.ie` domain. Websites are included in the candidate list for crawling if they are on the Tranco list, in the `.ie` domain or are on our list of Irish websites.

I don't care about cookies[12] is a browser extension that automatically removes cookie consent pop-ups. With this extension, users can browse the web without interruptions from these consent requests. It works by accepting or hiding cookie banners based on predefined rules, eliminating the need for users to interact with them manually. Kampanos et al. use this list of predefined rules in combination with some additional selectors they identify for cookies. We adjusted this list also to address specific Irish cookie banners such as language.

`robots.txt`[13], also known as the Robots Exclusion Protocol, is a text file that websites use to communicate with web crawlers and robots. It defines which parts of the site should not be crawled or indexed by search engines and is located in the root directory.

[12] I Don't Care About Cookies: https://www.i-dont-care-about-cookies.eu/.

[13] `robots.txt`: https://www.cloudflare.com/en-gb/learning/bots/what-is-robots-txt/

3.4.0.2 Steps For Cookie Crawling

The steps for running the crawl are similar to those in Kampanos's original study (see Fig. 3.2):

- **Step One**
  - Download list of 1M top websites via TRANCO.
  - Manually compile list of Irish websites.
  - Parse Tranco website list for `.ie` websites.
  - Merge the Tranco `.ie` list and the manual Irish to run through OpenWPM.
- **Step Two - using OpenWPM**
  - Check `robots.txt` compliance.
  - Check Terms of Services (ToS) compliance.
  - Using *I don't Care about Cookies* (IDCAC) list crawl all websites on the list.
  - Collect cookie data.
- **Step Three**
  - Sanitise collected data.
  - Structure collected data.
- **Step Four**
  - Analyse data using SQL and Python.

By inspecting the data recorded by OpenWPM, the automated analysis was able to identify cookies set during the crawl. It counted the number of cookies set for each site and checked if these cookies were third-party cookies. The identification of third-party cookies was achieved by comparing the site URL recorded by OpenWPM with the domain of the cookie stored.

3.4.1 Manual Crawl Methodology

In order to perform a manual inspection of a subset of the overall list of websites, a sample size of 362 was calculated using Cochran's formula, to provide a 90% confidence level with 4% margin of error. Cochran's formula for sample size determination is vital for ensuring statistical power, precision, and reliability in research. Helping balance accuracy, cost, and time while considering different types of variables. The formula adjusts sample sizes for large populations and extends to confidence intervals using the Studentized[14] sample mean, making it useful for various statistical analyses [180, 221, 282, 286, 306].

The 362 websites were randomly chosen using Excel from the list of websites identified as containing banners. The manual inspection allowed us to identify if different phrases may have been used in cookie banners, for example if they were in a different language. This in turn allowed for adjustment to the list of phrases that was used in searching for banners. The manual inspection was also used to address other questions, for example regarding the design or placement of the cookie banner. In the undertaking of this manual subset check, a lot of false positive and a number of false negatives were noted. It was also noted that many CSS selectors on the *I don't care about cookies* list that were intended to only be applied to websites in a specific domain were actually being applied to all websites by the system developed by Kampanos. The system was adjusted to ignore CSS selectors that were intended to be more specific. New CSS selectors were discovered and added to a list of extra CSS selectors used to identify banners and the main crawl was re-run.

3.5 Results

The results of the overall crawl are first considered, followed by the results of the manually inspected subset. The results of the full crawl are based on our improved run, which ignores the overly-specific CSS rules. Our manual results are based on the first crawl, but omitting false positive banners. We manually checked the results and we visually documented the banners appearance and the details they contained.

[14]Wikipedia Studentization: https://en.wikipedia.org/wiki/Studentization

Websites visited	3735	Total options found	3542
Websites with cookies	3373	Average options per banner	1.93
Websites setting no cookies	362	Total affirmative options	1531
Websites setting only 3rd party cookies	220	Total non-affirmative options	322
Websites setting only 1st party cookies	1239	Total managerial options	557
Websites setting both 1st & 3rd party cookies	1914	Total informational options	1132
Automatically identified banners	1835	Average word count per banner	249.4
Manually identified banners	234	Banners with no options	124
Websites without banners	1666	Banners with only info option	158
Total third-party cookies set	22724	Banners with only accept option	210
Total first-party cookies set	58129	Banners with only reject option	1

Table 3.2: Summary of crawl results.

3.5.1 OpenWPM Crawl Results

The total number of candidate websites was 4528. The framework tested the `robots.txt` for each of these websites and found 4003 suitable for crawling. The framework also checks for terms of service for each of the remaining websites to check if they are for personal use only. After this check, 3782 websites remain. The framework then crawls these websites and obtained results for 3735 of them.

To rule out false negatives, we manually check our list of websites where they are marked as not containing banners. From this list we find an extra 234 websites which do in fact display banners, so while the framework documents 1835 websites with banners, the total number is actually 2069.

A summary of the results for these 3735 websites are provided in Table 3.2. During the crawl, a total of 58129 first-party cookies were set, an average of around 15.6 cookies per visit and a total of 22724 third-party cookies, with an average of 6 third-party cookies per visit. Third-party cookies appeared on 2134 of the websites and of all crawled websites approximately 10% had not set any cookies by the time the crawl of that site was completed. Fig. 3.3 shows the overlap of websites with first/third party cookies.

We note the framework does not consent to any cookies being set and although 90% of Irish websites set cookies, only 55% were identified as displaying banners. However, compared to Kampanos's findings, we see a small improvement with regards to third-party cookies; with 57% hosting third-party cookies. Kampanos

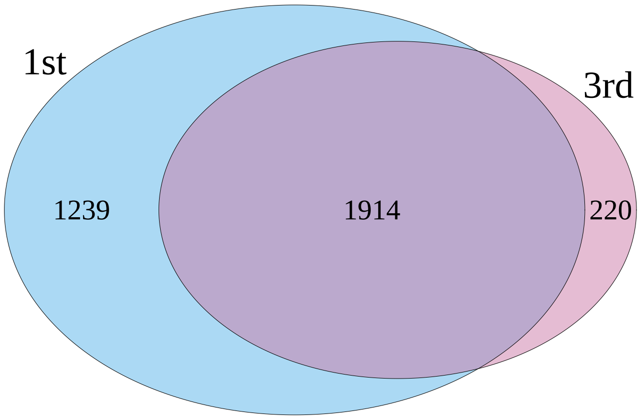


Figure 3.3: Websites hosting first & third-party cookies.

reports 48% of Greek websites containing banners with 61% of these hosting third-party cookies and 44% of British websites displaying banners with 70% of these containing third-party cookies. The website sample we collected is similar in size to the Greek sample.

Considering options (or call to actions) presented by the banners, there are, on average, just under two options identified per banner. The framework classifies these options as affirmative, non-affirmative, managerial and informational, with affirmative and informational being the most common. We take percentage of each option type, from the total banners processed, which can be seen in Fig. 3.4. A small number of banners had just one or no options. Comparatively, Kampanos documents no websites with reject only, we find one banner with a reject only option. A summary of the text found in each different type of option is shown in Table 3.3.

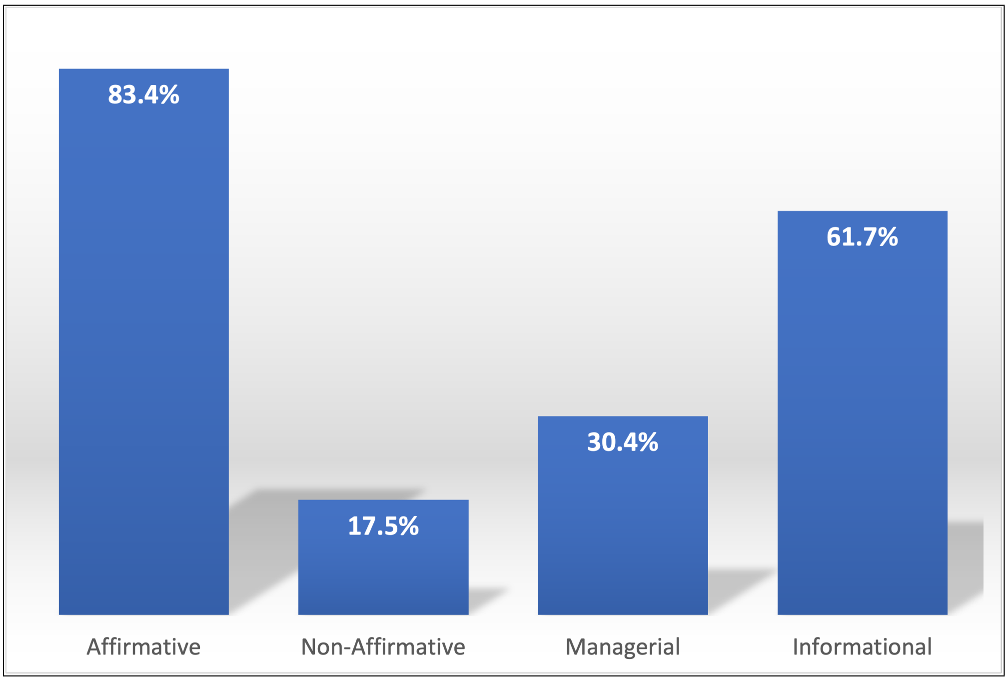


Figure 3.4: Irish cookie banner Call to Actions, percentages taken from total banners processed.

Accept	%	**Decline**	%	**Options**	%	**Info**	%
Accept	26	Reject all	48	Cookie settings	48	Cookie policy	22
Accept all cookies	16	Reject	27	Manage cookies	16	Privacy policy	15
Ok	10	Decline	13	More Options	11	Read more	13
Accept all	10	Disagree	5	Settings	10	Learn more	10
Allow all cookies	9	No	4	Manage	1	Cookie declaration	10
Got it!	5	Decline All	2	Cookie Preferences	0.4	More information	4
I accept	4	Revoke Cookies	0.6	Change Preferences	0.4	Cookie details	4
Allow All	4	Disable Cookies	0.6	Change Settings	0.2	More info	2

Table 3.3: Call to Action, percentages taken from total in each category.

Figure 3.5: Cookie banner word frequency.

Fig. 3.5 shows a word cloud based on the text observed in banners. It contains words suggesting positive framing. We performed automated sentiment analysis on the words used in the banners using NRCLex. NRCLex assesses emotional affect in a text corpus. It utilises a dictionary which comprises of around 27,000 words and is derived from the National Research Council Canada (NRC) affect lexicon. The NRC Emotion Lexicon is a list of English words and their associations with eight basic emotions (anger, fear, anticipation, trust, surprise, sadness, joy, and disgust) and two sentiments (negative and positive). The annotations were manually done by crowdsourcing [39].

The words NRCLex isolated from the banners to judge sentiment were 'Relevant', 'Provide', 'Agreeing', 'Happy', 'Improve','Continue' and 'Agree'. The code assigns each word to a sentiment category, some words are included in more than one sentiment category. For example all words were included in the positive category (see Fig. 3.4).

No negative emotion was registered in the text, which contrasted Kampanos's findings where they recorded 14% negative sentiment present in their banner text [168].

	Positive	Trust	Anticipation	Joy
Agree	✓			
Provide	✓	✓		
Agreeing	✓	✓		
Relevant	✓	✓		
Continue	✓	✓	✓	
Improve	✓	✓	✓	✓
Happy	✓	✓	✓	✓

Table 3.4: Sentiment analysis performed on words identified from banners using NRCLex.

3.5.2 Manual Crawl Results

From the list of websites we randomly chose to manually crawl, we noted 6 false positives; websites that did not exist or were down. We also discovered 19 (5%) websites that contained HTML for banners but had no visible banner. Our total, therefore, is 337 visible banners and not the full sample of 362. Considering pages including visible or invisible banners ($n = 356$), the fraction of websites containing third-party cookies amounts to 55%. We documented position of banners, whether you could decline cookies directly and consent management platforms. We looked at the design of the banners and took note of unusual banners and dark designs. We did not record individual dark patterns such as highlighted accept buttons.

A benefit to working with a smaller subset, which has been used in the past [113, 152, 182, 262], is being able look at banners in detail. Fig. 3.6 displays the most common positions for banners on the page, the bottom of the website position being the clear winner.

We also are able to identify cookie banners in the Irish language of which we found only two (see Fig. 3.1). These were located on Irish language websites for example the Irish TV station TG4, Google also tends to translate cookie banners to English. We can also identify dark patterns and issues considered in the DPC's report. We noted several similarities. For example, a number of websites declare all cookies to be 'necessary' for the website to function, while not specifying what cookies are indeed 'strictly necessary'. The DPC considered this a form of cookie

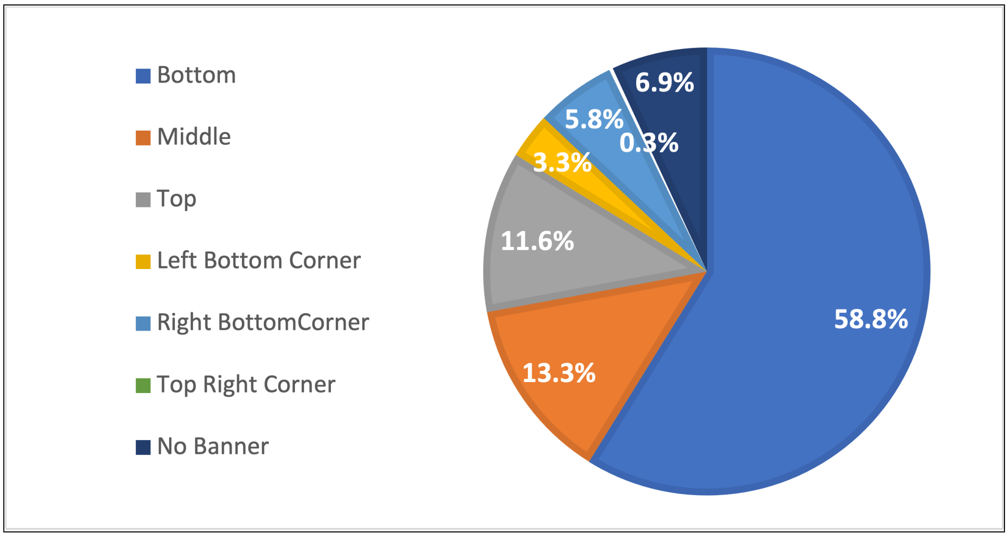


Figure 3.6: Subset banners positions.

Pre-ticked	8%	CMP**	25%
Direct Opt-Out	19%	TP*+CMP**	14%
Preferences	53%	TP*+Pre-ticked	4%
No Info	10%	CMP**+Pre-ticked	1.7%
Accept Only	76%		

Table 3.5: Feature summary of manually inspected subset, *TP–Third-party cookies, **CMP–consent management platform banner.

bundling [113] and was also observed in Santos et al. cookie banner analysis [262]. Tab. 3.5 summarise some of these features.

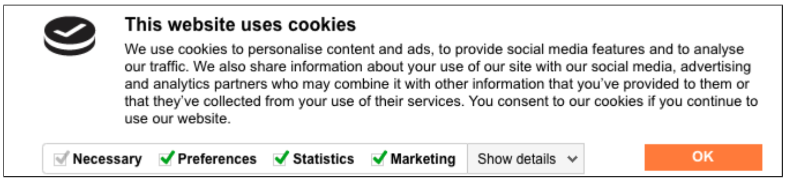
Another practice, which was also noted in the DPC's report, were websites who assume that informing the user that they can change their privacy settings in-browser implies consent. The GDPR highlights that a person's consent to cookies should be "freely given, specific, informed and unambiguous" [104], merely directing them to alternatives to changing privacy choices, such as changing privacy setting in your own browser, does not imply consent to cookies. Other observations noted were: (1) highlighted accept buttons, in one case a decline button was opaque. (2) The colour green for accept buttons and red for decline, which is a dark pattern nudging technique (green being a colour synonymous with Go!) [52]. The two above cases can affect visually impaired users, as Clarke et al. note, banners with low contrast further hinder visibility [94]. Green and red are also problematic colours for colour blind users [253]. (3) Of the websites recorded in the manual crawl 63% had banners on the bottom. We did observe some banners were almost invisible at the bottom or top of the website. Many of these assumed consent by scrolling through the website, which is easier to do with a thin banner at the top or bottom of the page. It might be argued that these websites have discrete banners to avoid annoying their users while also complying with regulations. (4) Some websites included links for more information that did not work or redirected to the same page (also observed by the DPC).

There is a stark difference between the style of banners found. On one end of the scale we have a barely visible sliver on the top or bottom of a page containing only an 'Accept' button. On the other end a large banner in the middle or side with all options and information visible and direct opt-out buttons. Only 19% of the banners were observed to have both an 'Accept' and 'Decline' option, with 76% of banners containing 'Accept' only. We found 8% of the banners had pre-ticked options where the less private options were already chosen (e.g. Fig. 3.7a), 56% of these contained third-party cookies.

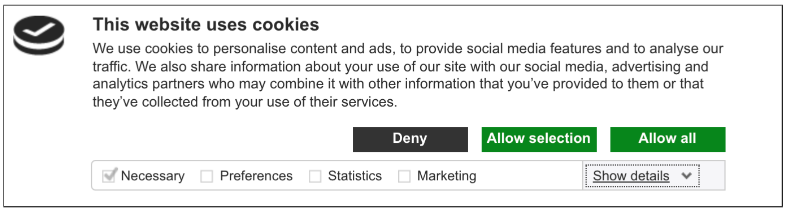
As noted in Sec 3.2.3, websites use CMP's to manage their cookies for them and as such should be up to date with GDPR. The majority of banners with pre-ticked options did not have a CMP logo attached. Of the manually inspected websites, 25% employed a CMP (see Fig. 3.7). Matte et al. identify 25 Irish websites out of 1426 European crawled websites with CMPs. Three of the 25 Irish websites displayed the OneTrust CMP, who for all 3, stored cookies before consent and 2 of the 3 had pre-selected options [208]. OneTrust is the only CMP from their list of Irish CMPs which we also identified. This CMP appeared most in our subset (36) and interestingly did not have pre-ticked options. This is likely due to the change in the GDPR in 2019 regarding pre-ticked banners [111]. Our list of CMPs found can be seen in Table 3.6.

CMP	TOTAL	%
CookiePro	16	19.05
CookieYes	4	4.76
OneTrust	36	42.86
wordpress.org	5	5.95
Privado	1	1.19
Cookiebot	21	25
Trustarc	1	1.19

Table 3.6: Consent Management Platforms brands and their percentage from total (84) CMPs found in our manual subset.



(a) Pre-ticked options



(b) Direct opt-out

Figure 3.7: Examples of consent management platform (CMPs) banners, with different options. Often these are preticked like (a), (b) has the option to deny cookies.

Three websites redirected to a link explaining cookies 'cookiesandyou.com' and 'allaboutcookies.org'. On one policy redirect, the banner popped up again in the middle and you could not scroll down to read the cookie information unless you clicked accept. One website's banner contained a 'more info' link which directed you to the cookies Wikipedia page. A few page's 'Learn More' button led to nothing, which might be a fault in the consent management platform (CMP) tool of which the website itself may not be aware of. The same fault applied to some banners, where on clicking 'preferences' results in nothing happening.

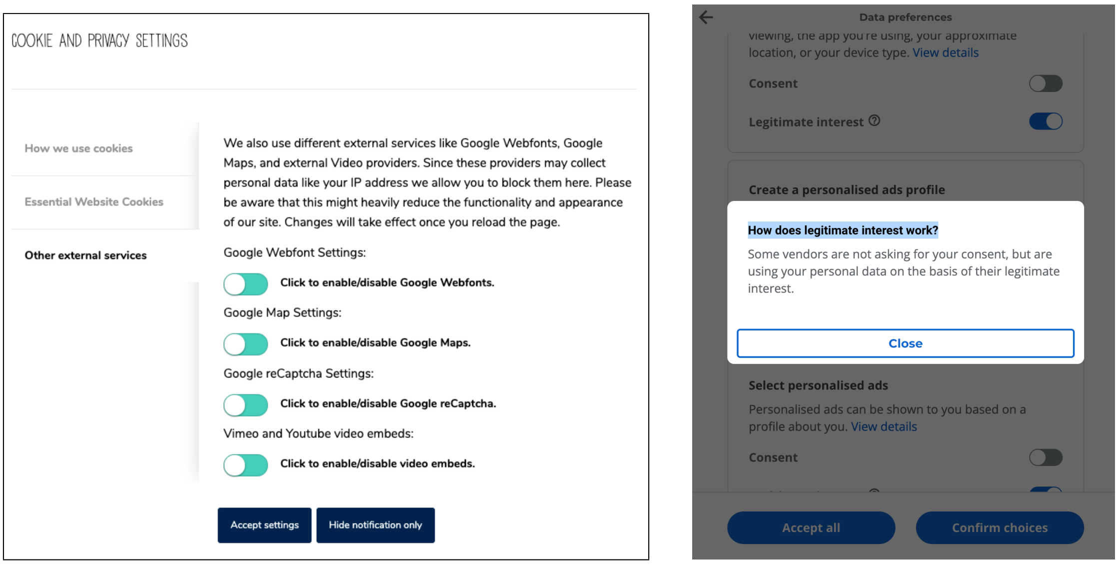


Figure 3.8: Banner with vague instructions and pre-ticked buttons (left) and 'Legitimate Interests' banner (right).

(5) Other vague banners included an 'Accept' button along with 'Dismiss', which can be misleading, in that you may assume 'Dismiss' means 'Deny Cookies', when in fact you are dismissing the banner and accepting cookies.

One website with third-party cookies used a bottom banner which displayed "This site uses cookies. By continuing to browse the site, you are agreeing to our use of cookies' with a highlighted 'ok' button and a 'learn more' button". When the 'learn more' button is clicked, you are directed to the banner shown left in Fig. 3.8. It is not clear whether the buttons are already ticked; the colouring suggests that they are. However, more commonly pre-ticked buttons will have the coloured part to the left which suggests it has already been ticked, the line beside the button says 'click to enable/disable' suggesting then, that these buttons are in the 'enable' position.

Two CMP banners, after clicking preferences, contained just the option to enable or disable 'strictly necessary' cookies with no other options. The website in question included third-party cookies, and it was not clear if they were all necessary. A cybersecurity and data protection website, also containing third-party cookies, displayed no cookie banner.

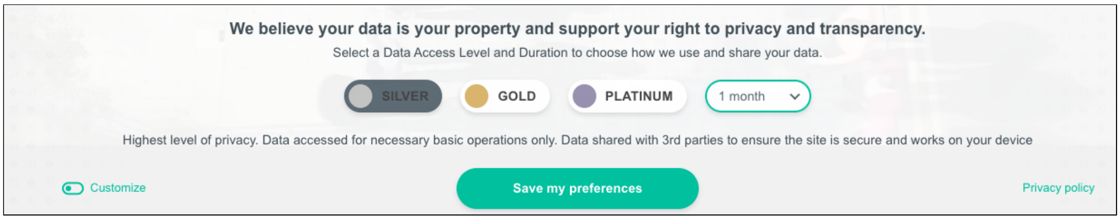


Figure 3.9: Data choices represented by precious metals on `lensmen.ie`.

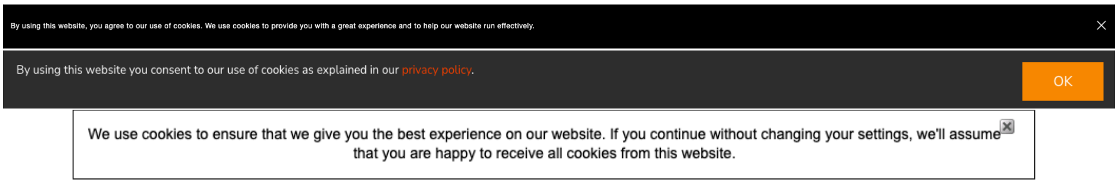


Figure 3.10: Example of some poor cookie banners from the top: (1) `cococontent.ie`, (2) `budget.ie`, (3) `ecigarettesworld.ie`.

Some banner policies mention that other websites have access to their information via third-party cookies but they do not have responsibility over what that third party website does with this data and thus the onus is on the user to investigate this. Another banner's preference list consisted of consent buttons for certain data collation. Beneath this there was a pre-ticked 'legitimate interests' button. When you click on 'more information' relating to 'legitimate interest' it states: "How does legitimate interest work? Some vendors are not asking for your consent, but are using your personal data on the basis of their legitimate interest." This does not explain what constitutes as their 'legitimate interests', (e.g. Fig. 3.8 (right)).

One novel example of a dark pattern noted was data choices represented by silver, gold and platinum (see Fig. 3.9), where platinum is, as they say, the "Highest level of personalisation. Data accessed to make ads and media more relevant. Data shared with 3rd parties may be use to track you on this site and other sites you visit". This is the only example we have seen that represents the choice in this way. It is likely that people will associate platinum to be the best choice.

3.6 Discussion

This study aimed to provide a comprehensive overview of cookie banners in Ireland and to analyse their visual characteristics, including any dark patterns. Additionally, we sought to determine if Irish cookie banners adhere to the seven principles of universal design and to compare our findings with similar studies conducted in other European countries.

3.6.1 OpenWPM Crawl Discussion

At a high level, there is similarity between the Irish, Greek and English cookie landscape. One difference is that the proportion of websites in Ireland containing third-party cookies without banners is smaller than UK or Greece. While one reason for this may be better compliance in Ireland, it might also be explained by a more effective list of CSS selectors used to identify banners or improved compliance over time, possibly motivated by fines issued for non-compliance.

Strong positive sentiments were recorded in banner language where it is often presented as being in your best interest to accept cookies. This could be interpreted as a variation on *confirm shaming*[15]. For many websites, advertising is a source of income and allowing people to easily opt out of cookies could reduce their earning power [260]. Consequently, enticing people to choose cookies using positive language is one way to seek financial advantage.

In some cases, choice of cookies appears to be an illusion, particularly for banners which declare they use cookies and only display an 'OK' button. If there are any cookies that are not strictly necessary then there should be a choice or information on how to opt out. While some websites may be technically complying with GDPR, this type of behaviour seems to be prevalent. Certain characteristics which act as barriers to protecting your data fall under the heading of dark patterns, which are difficult to outlaw.

[15] The act of making the user feel guilty to have them agree into opting into something. The option to decline is worded in such a way as to shame the user into compliance. [216]

3.6.2 Manual Crawl Discussion

We found that opting out of cookies is quite difficult, as noted in other studies [168]. Many websites necessitate going to a second level or more, in order to opt out of cookies or expect you to change your cookie settings in your browser. It has been observed that “placing controls or information below the first layer renders it effectively ignored” [227].

Similar dark patterns emerge in Irish banners as are observed in studies on German banners [182]. Other classifications of dark patterns such as those mentioned in Graßl et al.’s study on dark patterns in cookie banners, were also observed and make it apparent that dark patterns are in use in Irish banners [145]. When it comes to dark patterns and cookie banners it has been observed that there is a “lack of identification of the ways in which particular dark patterns might be connected to legal requirements and the user experience” [146]. Whether banners are intentionally designed to influence users into allowing their data to be easily collected or if it is down to lack of understanding on the part of website creators, is not easy to identify.

Strong similarities to the DPC study were also observed, although the DPC’s study was performed on a small hand-picked group of 38 websites. The DPC report highlights examples of bad cookie banners, most notably thin banners such as the ones shown in Fig. 3.10. This also appeared to be the most common banner in our manual sweep.

Note that the percentage of pre-ticked options dropped significantly compared to the DPC’s findings of 26%. This could be explained by the fact that in 2019 the Court of Justice of the European Union delivered a judgment in the Planet49 case [113]. This ruling stated that pre-ticked options do not constitute valid consent under the e-Privacy Directive [111]. The DPC acknowledges that their study was conducted before this judgement. However, pre-selected choices were always a violation of GDPR (since 2016) in a direct violation of the requirement of unambiguous consent from article 4(11) [8].

The DPC’s report noted that some websites were not aware of their breaches when using an external CMP [113]. As regulations can differ between countries, these banners may be legal in some countries but not others. We observed that the majority of banners with pre-ticked options did not have a CMP logo attached. This suggests that the recent clarifications regarding pre-ticked cookies are being followed, particularly by CMPs.

Another feature, which was also noted in the DPC's report, was the presence of websites who assume that informing the user that they can change their privacy settings in-browser implies consent. This may arise because regulations may appear vague, especially regulation 5(4) of the ePrivacy regulations:

> Where it is technically possible and effective, having regard to the relevant provisions of the Data Protection Acts, the user's consent to the storing of information or to gaining access to information already stored may be given by the use of appropriate browser settings or other technological application by means of which the user can be considered to have given his or her consent [113].

Without a legal background, one might assume that this means you can gain consent by notifying the user that they can change their settings. However, this has been clarified as not an exception to regulation 5(3), which states a person cannot store information unless the user has given clear consent [113].

Finally, we identified a number of invisible banners, a finding that has not been addressed in previous studies. Without manual inspection, it is difficult to know if a banner is actually displayed, and some often only appear once you scroll down to the bottom of the page. This leads to the question of websites functioning as intended, regardless of whether cookies have been accepted or not. Some website's cookie banners, while not invisible, are so discrete you have to actively search for them. These banners may have a decline button, but a person can peruse the website without noticing it.

3.6.3 Irish Cookie Banners & The Seven Principles of Universal Design

In terms of usability and the seven principles of design, we feel Irish cookie banners fail to align with five of the principles. Principle one equitable use; "the provisions for privacy and security should be available for all users", for example, older adults with parkinson's disease may potentially find it difficult to navigate layers of banners to attain more private options. The banner options in themselves are for the most part not equitable, as in they do not have equal options, 'accept' and 'reject'. This also applies to principle three; simple and intuitive use, unless an accept and reject button are available it is often not intuitive as to where to get more privacy friendly features. We also feel Irish cookie banners do not align with principle four; perceptible information, banners can be confusing and mean different things in one banner and not the other, such as necessary cookies. The law itself can be very confusing with regards to GDPR, with paragraphs of information regarding data that is not easy to understand. We feel principle five also applies here, as it relates to no warnings as to the real impacts of sharing data. And lastly principle seven with regards to size and space for approach and use, cookie banners were for the most part barely visible on the webpage.

3.6.4 Future Work & Limitations

Regardless of whether websites adhere to GDPR, the effectiveness of cookie banners comes into question if a person does not comprehend its content and purpose. Future work could study vulnerable populations and how they understand or navigate cookie banners. A possible 'one size fits all' banner could be designed and tested, one that adheres to all seven principles of universal design (explained in Chapter 1).

We acknowledge the following limitations, we did not document quantitative results for dark patterns for all websites. Additionally OpenWPM did not accurately screenshot each websites banner, this resulted in the necessity of manually looking at a small subset.

3.7 Conclusion

In this chapter, our aim was to investigate the utilisation of cookie banners in Irish websites. We employed the use of an automated mechanism, similar to Kampanos [168], and also inspected a subset of banners manually. Comparatively, our automated results are broadly similar to Kampanos study with an improvement in terms of websites hosting third-party cookies and displaying banners. Our manual inspection of banners identified the use of a number of common dark patterns identified with some banners displaying confusing and misleading language and instructions. Our findings also highlight usability issues with regards to the seven principles of universal design. In addition to our findings via the adjusted OpenWPM framework we suggest banner detection could be improved by more careful interpretation of specific CSS selectors. We would also suggest regular crawls over multiple countries to monitor changes over time and location.

CHAPTER 4

Cross-Country Analysis of Subscription Traps

Subscribing to online services is typically a straightforward process, but cancelling them can be arduous and confusing — causing many to resign and continue paying for services they no longer use. Making the cancellation intentionally difficult is recognised as a dark pattern called Roach Motel. This chapter characterises the subscription and cancellation flows of popular news websites from four different countries, and discusses them in the context of recent regulatory changes. We study the design features that make it difficult to cancel a subscription and find several cancellation flows that feature intentional barriers, such as forcing users to type in a phrase or call a representative. Further, we find many subscription flows that do not adequately inform users about recurring charges and can be harmful to vulnerable users. Our results point to a growing need for effective regulation of designs that trick, coerce, or manipulate users into paying for subscriptions they do not want.

4.1 Introduction

In 2023, internal documents leaked to Business Insider revealed that Amazon had deliberately designed the process of cancelling Prime subscriptions in an arduous

Figure 4.1: A 2023 tweet by comedian Trevor Noah ridiculing the difficulties of cancelling subscriptions [27].

and prolonged manner [293]. It was also revealed that Amazon were aware of consumers being involuntarily enrolled in their service [98].

While Amazon's practices also prompted complaints by consumer organisations in Europe [99, 109], the practice of building obstacles to keep users subscribed is not limited to a single company [10, 14, 195, 254]. In fact, a 2022 survey of 2,500 Americans showed that one-third of Americans are paying for subscriptions they do not use, with 42% feeling 'locked in' to their current subscription plans [201]. Frustrated users including celebrities (see Fig. 4.1) turn to social media and online forums such as Reddit[1] to complain about these manipulative practices [19,33,105]. Responding to Nieman Journalism Lab's[2] call in 2021, several users listed unexpected credit card charges as a reason to cancel their newspaper subscriptions [19]. In 2022, hundreds of one-star reviews left on the customer review site ConsumerAffairs complained about subscription-related practices in industries such as dating sites, software subscriptions, radio/TV services, and weight loss and health club memberships [158].

New laws and regulations across the globe have been recently passed or proposed to better protect consumers against these unfair practices [12, 97, 103]. A notable example of these new laws is the German Fair Consumers Act which requires a 'termination button' to make it easy to cancel subscriptions [181]. In the US, the

[1] Reddit threads mentioning "cancel subscription", https://www.reddit.com/r/assholedesign/search/?q=cancel%2Fsubscription

[2] Nieman Journalism Lab was published by Nieman Foundation at Harvard to investigate future models with the aim to support quality journalism [19]

Federal Trade Commission propose a 'Click to Cancel' option for cancelling [97]. Finally, the UK by 2024, aim to "ensure, consumers can easily exit contracts without any unnecessary steps (ideally one click)" [122].

4.1.1 Objectives & Contributions

Motivated by user complaints, the recent and upcoming regulatory changes, and the surge of subscriptions as a business model, this chapter investigates problematic practices in the context of online news subscriptions. Existing research typically focuses on dark pattern taxonomies and/or user studies [51, 60, 119, 200, 206], however these studies do not shine a light on individual dark patterns, such as we do with the *Roach Motel* dark pattern. We characterise the subscription and cancellation paths to news sites from five different locations. Specifically, we posed as a German, Dutch, English, Texan and Californian consumer and subscribed to a list of up to ten news sites for each persona's country.

We aim to address the following questions in this chapter:

RQ3:1 What barriers and dark patterns exist which can potentially impact cancelling subscriptions across the UK, Netherlands, Germany and American states Texas and California?

RQ3:2 Have regulations new or old, had any impact in cancelling subscriptions online across the countries mentioned above?

RQ3:3 Does subscription practices in these tested services, align with the seven principles of design?

We chose news websites over other industries (e.g., streaming, games, beauty, makeup) and subscriptions types (e.g., physical) to avoid ethical problems surrounding collecting physical products and waste. News sites are widely used, reasonably priced, and available in each country, making them more feasible for our comparative study.

We choose these locations to study practices in countries and states with different regulations. Germany was chosen because, as we noted, they have implemented a strict cancel subscription regulation, as well as the fact that one of the co-authors for this paper is German and therefore her knowledge of the German language could prove useful. As this project was conducted in collaboration with a research group in Radboud University in the Netherlands, we chose the Netherlands as one of our countries. The country has a larger number of national news sites and presents a more intriguing case from a regulatory perspective. Additionally we wanted another country from the EU to compare to Germany's strict regulations. We chose the UK as it is now not in the EU yet still has to comply with GDPR, and we were curious to note if this had may impact on subscribing to British news sites. Finally we chose the US because their regulations are quite different from Europe and have recently seen some changes in their subscription laws as will be discussed in Sec.4.3. State laws vary greatly in the US, so we chose two American personas; a Texan whose state has no subscription law as yet and a Californian who have recently changed their regulations pertaining to subscriptions (see Sec.4.3). In addition, our European personas also subscribed to the same American news sites to observe any differences in subscribing and cancelling based on subscribers' location.

The main contribution of this work, is a systematic cross-country comparison of subscription and cancellation flow designs of popular news websites. We study these flows through the lens of requirements imposed by the relevant existing and upcoming regulations and also through the lens of requirements imposed by the seven principles of universal design. In addition, we provide a comparison of subscription and cancellation flows in terms of efforts necessary to achieve the two respective goals. We show that in all the jurisdictions studied, the *Roach Motel* is still present, though to varying degrees. Finally we contribute a dataset of over 100 screen recordings of subscribing and cancelling[3]. This comprehensive dataset serves as a valuable resource for researchers studying subscription-based services from various perspectives.

The chapter is laid out as follows; in the next section (Sec. 4.2) we look at the general background of subscriptions and dark patterns associated with them. We also look at related work in this area. This section is further split into subsections.

[3]Cancellation videos of our dataset can be viewed on `https://github.com/roach-motel/chi-24`

In Sec. 4.3 we look at updates to regulations on subscriptions for the countries included in this study. In Sec. 4.4.2, we give an overview of each countries market and user surveys related to subscriptions and cancellations. Sec. 4.5 outlines the methodology employed in this study. Sec. 4.6 reveals the results of the study for each country in detail, separated into subscribing and cancelling sections. This section is followed by our discussion in Sec. 4.7 and conclusions in Sec. 4.8. Extra information such as subscription study steps, tables and extra screenshots can be found in Appendix E.

4.2 Background

Chapter 3 introduced the topic of dark patterns with regards to cookie banners in this chapter we look more closely dark patterns specifically related to purchasing and cancelling subscriptions, known as *Roach Motel*. As we noted; *Roach Motel*, also referred to as *Hard to Cancel* and *Subscription Traps*, refers to the situation where you find it easy to sign up for something but very difficult to leave it [66]. The 'click-to-subscribe, call-to-cancel' is a common tactic used by online businesses [209].

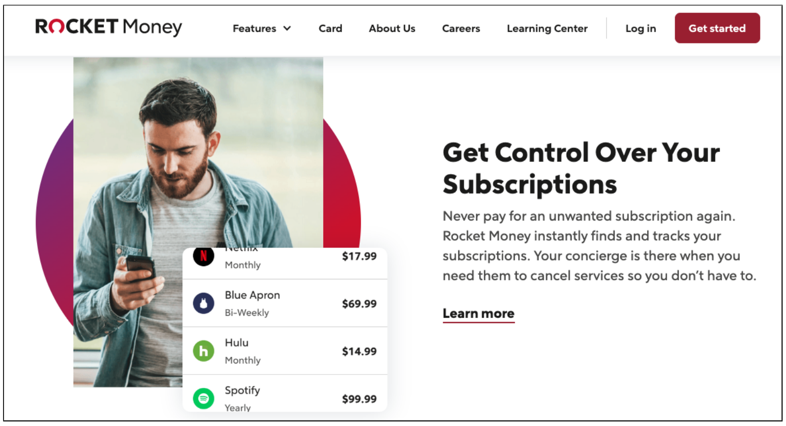


Figure 4.2: Third party method of avoiding subscription traps [256].

The concept of a subscription-based model is not a recent development. Their origins can be dated back to 1856, when individuals had the option to lease a sewing machine for a monthly fee of $3, following a $5 initial deposit [209]. Nowadays, there is little you can not purchase a subscription for [7]. A more recent (2022) addition to the subscription market, is subscriptions for certain extra features in cars. For $18 a month you can enjoy heated front seats for your BMW [154].

There are three different classes of subscription plans [85].

- **Access** - Online subscriptions to access such services like streaming platforms such as Netflix, education, gaming and newspapers.
- **Curation** - Personalised surprise boxes in fashion, beauty, food, drink among others.
- **Replenishment** - groceries, vitamins, day to day items.

The expansion of the subscription-based economy exhibits no indications of slowing down. By 2021, it had already witnessed a remarkable surge of over 435% within the preceding nine years [209]. As a result of the pandemic this growth rate has accelerated by 11.6% [142]. This expansion is commonly connected to two main factors. Firstly, the growth of e-commerce has enlarged the scope for payment structures based on subscriptions. Secondly, there's a belief that subscriptions assist consumers by alleviating the inconvenience of making one-time purchases [123]. However, as a result of cost of living, many users are cancelling their services, more than two million UK customers gave up their streaming services last year [35, 283].

Perhaps the most well-known example of easy-to-enroll but hard-to-cancel subscription practices is used by Amazon Prime, which has more than 200 million subscribers worldwide [106]. The recent US Federal Trade Commission (FTC) complaint against Amazon alleges that Amazon knew that their customers involuntarily enrolled into Prime subscriptions and that customers were frustrated about the arduous and perplexing Prime cancellation procedure [235]. The complaint asserts that it requires a minimum of six clicks to cancel the Amazon Prime subscription and the cancellation flow contains several dark patterns such as *Forced Action*, *Interface Interference*, *Misdirection* and *Obstruction* [147, 235]. In July 2022, Amazon agreed to change its cancellation process for EU and EEA users, following a complaint made by the European Consumer Organisation (BEUC), the Norwegian Consumer Council and the Transatlantic Consumer Dialogue [99]. Thanks to these changes, EU and EEA users have been able to cancel their subscriptions in two clicks with a clear and prominent cancel button–an option that was not available in the US until April 2023 [235]. Amazon's changes in their cancellation process for the EU and EEA highlight how regulations regarding subscriptions can vary between countries and jurisdictions. These differences in practices and regulations partly motivates our multi-vantage point investigation into subscription and cancellation flows.

4.2.1 Subscription Traps & Vulnerable Users

For most subscribers, hard-to-cancel subscriptions can result in financial harm and, at the least, frustration. Such cancellation challenges can have a more pronounced effect on individuals with mental health conditions. A 2017 survey by Money and Mental Health Policy Institute[4], revealed that individuals facing mental health challenges are more likely to forget to cancel and three times more likely to avoid cancelling when having to do so by phone [128]. The same survey also found that 21% of the participants expressed their inclination to postpone cancelling a service, despite no longer desiring it. The participants cited concerns that the company would apply pressure tactics to retain their subscription [128]. When a company deliberately creates a cancellation procedure that is unnecessarily challenging for the average consumer, it further exacerbates the difficulties faced by individuals with disabilities when attempting to cancel [139]. Moreover, the commonly used tactic of requiring customers to contact a customer service representative to cancel their subscription presents an insurmountable challenge for users with hearing impairment [139].

Jennifer King, a Privacy and Data Policy Fellow at the Stanford Institute for Human-Centered Artificial Intelligence, in speaking on dark patterns claims that "Some of these are patterns that would seem shady to a digital native or a person with at least a high school education, but might successfully trick a person who is older and less digitally proficient, or less educated, or a non-native English speaker" [211].

[4] A charity dedicated to understanding the relationship between money and health.

An example of how subscription traps can effect disabled people is revealed in Caroline Bailey's case, who is deaf and registered for a Fabletics[5] subscription online. Fabletics mandated that customers must call and talk with a representative to terminate their subscription. Caroline faced several months of frustration as she could not cancel her monthly clothing orders due to her inability to call and converse with a representative. While Fabletics eventually provided an online cancellation option for Caroline, it is quite evident how call-based cancellation procedures create significant difficulties for individuals with disabilities [209].

As the elder population increases, their presence online will also increase. With ageing, hearing and memory can degrade and as a result barriers to cancelling subscriptions will be problematic. When a company deliberately complicates its cancellation process for the typical consumer, it exacerbates the challenge of cancellation for individuals with disabilities [209].

4.3 Updates to Regulations on Subscriptions

The countries involved in this study have seen some changes in regulations regarding subscriptions and dark patterns. These changes are discussed below.

4.3.1 United States

In October 2021, the Federal Trade Commission (FTC) issued an enforcement policy statement on the Restore Online Shoppers' Confidence Act (ROSCA) of 2010 [9], which signalled a ramp up of enforcement on dark patterns in subscriptions [101]. In 2023, the FTC announced an amendment to the Federal Trade Commission act, which introduces three main requirements businesses must adhere to [24, 100]. The requirements consist of 1) clearly disclose all details about the subscription, including price, renewal dates and how to cancel; 2) obtain customers expressed consent before charging them for products or services; 3) provide an easy and simple method to cancel subscriptions [24].

California: In 2017, an online cancellation provision was added into the California Business and Professions Code. In accordance with this provision, if a consumer

[5]Fabletics is a retail website for workout wear `https://www.fabletics.com/index.cfm?action=home.main&`.

chooses to subscribe to a service online, the business is obligated to offer an online cancellation option as well [209]. On October 4, 2021, California amended the Automatic Renewal Law (ARL) of 2010 [258], to provide more explicit cancellation guidelines compared to the previous rule. This amendment which went into effect in 2022, applies to all businesses that offer automatic renewal or continuous service to Californians. Of the 50 US states, half have also adopted an automatic renewal law, and eight states with no existing laws are considering adopting them [203].

Texas: To the best of our knowledge, Texas still lacks specific regulation on subscription services [110, 203]. None of the bills introduced in 2009, 2011 and recently in 2021 (HB 2259) were enacted into law [110]. The lack of regulation is indeed one of the reasons why we include Texas in the study, so we can compare the potential effects of local (as opposed to federal) regulation, or lack thereof.

4.3.2 Europe

In addition to national laws described below, EU-wide legislation, such as the Unfair Commercial Practices Directive (UCPD), also applies to subscriptions or cancellations in the e-commerce domain [17]. The UCPD prohibits unfair commercial practices such as untruthful information or aggressive marketing techniques, and it lists "dark design patterns" as one of the explicitly prohibited practices [28]. Moreover, the official guidance document on the interpretation and application of the UCPD mentions several potential infringements related to subscriptions [18]. These include "not making it clear to consumers that they may enter into subscriptions by signing up to a free trial" and "[o]mitting or providing information in an unclear manner on the recurring costs of a subscription" [18]. Note that the EU directives need to be incorporated (*transposed*) into the national laws by the EU Member States. In the UK, the Consumer Protection from Unfair Trading Regulations 2008 (CPUT) was introduced to enact the EU UCPD. After the UK's exit from the EU, CPUT continues to be effective, with EU references removed [47].

Germany: In Germany, the new Fair Consumer Contracts Act (FCCA)[6] came into effect in July 2022. The act states that businesses offering subscriptions to German consumers must make it possible for them to cancel subscriptions online. In addition, the act requires businesses to have a 'termination' or a 'cancel now' button to easily cancel subscriptions [3, 140, 231]. This button is referred to as the 'two click termination button' [181], we refer to it as a 'two step termination button' elsewhere in this chapter. This button can lead to a page where customers are requested to fill in their details, the contract they wish to cancel and reasons for cancelling [20,231]. This page should also incorporate a clear confirmation button, which upon clicking, guarantees the termination of the contract. The consumer should receive a confirmation email immediately afterwards [3].

The Netherlands: The Dutch Authority for Consumers and Markets (ACM) offer guidelines on the protection of the online consumer [22] (updated March 2023) for businesses involved in e-commerce. Highlighting that "online persuasion cannot turn into deception" when promoting your product. With respect to subscriptions, the ACM states that businesses must provide clear information on how consumers can terminate a contract and if a contract is initiated through a website, it should also be possible to terminate it through the same online platform [26]. The ACM also states that termination via the website should not involve excessive obstacles such as extensive questionnaires. The guidelines suggest that marketing, design, and legal departments coordinate to comply with regulations and to adhere to the principles of *fairness by design* and *privacy by design*. This can help businesses to comply with rules and adhere to the principles of fairness and privacy by design. The guidelines also point out that some groups of customers are more vulnerable than others such as the elderly [22].

[6]Prior to the reform, the inclusion of auto-renewal clauses in contracts allowed for the extension of the contract for an additional one-year term. Additionally, the required notice period before the end of the initial contract period could be three months [70].

United Kingdom: Responding to a *super-complaint*[7], the UK's Competition and Markets Authority (CMA) launched an investigation into *subscription traps* and loyalty penalties in 2019 [38]. Their study focusing on anti-virus software and online video games resulted in Norton and McAfee committing to changes in their practices [95, 96]. These commitments included making auto-renewing contracts easier to understand and exit, and ensuring refund rights [95, 96]. Following this study the CMA published guidelines (Oct 2021) on auto-renewal opt-outs and notifications [11]. These guidelines however are not legally binding [238].

In April 2022, reforms were announced by the UK government to address online dark patterns [218]. The CMA will be given more power to deal with companies that break these rules. They will also be able to compensate consumers who lose out from these dark patterns without getting the courts involved [218, 219]. In April 2023, the Digital Markets, Competition and Consumers Bill was submitted and is currently at the committee stage [134]. The bill addresses auto-renewal and cancelling information and highlights that consumers should be able to cancel online at any time.

4.3.2.1 Summary

The above updated regulations from all jurisdictions share certain themes, with different levels of detail. In summary, consumers should be informed about the terms of a service when signing up, and businesses must not erect unreasonable barriers to cancellation. Consumers should be notified throughout the process, for auto-renewal and recurring charges. They should also be provided with a subscription receipt and cancellation confirmation. All jurisdictions highlight the importance of consumers being made aware of auto-renewal and to be given the opportunity to cancel online. In short, these regulations aim to address the *Roach Motel* problem and lays out the normative perspective that our study benefits from [207].

[7] Broadly speaking, a *super-complaint* is a complaint submitted by a designated UK consumer body about practices or businesses that significantly harm consumer interests [37]

4.4 Related work

Dark patterns are defined by Mathur et al. as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make" [206].

To date, there are a growing number of papers in the area of deceptive design research such as [51, 60, 119, 194, 200, 206]. To classify different dark patterns in detail, Mathur et al. in a subsequent study, review recent studies on dark patterns and identify that the literature does not have a consistent definition or singular concern on how dark patterns impact the user [207]. Observing dark patterns through different disciplines, they propose a set of normative guidelines that can be used to evaluate dark patterns.

Coined by Brignull, the *Roach Motel* dark pattern refers to a situation where signing up for a service is straightforward, but the process of discontinuing or terminating the service is challenging or complex [66]. The *Hard to Cancel* category from Mathur et al. also refers to designs that are difficult to cancel [206]. Gray et al. categorized *Roach Motel* under their *Obstruction* category of dark patterns, which is defined as "[m]aking a process more difficult than it needs to be, with the intent of dissuading certain action(s)" [147]. Chivukula et al. analyzed 1002 posts from the subreddit '/r/assholedesign', where they found *Obstruction* to be the second most frequent dark pattern discussed [88]. Despite Chivukula et al.'s observation, the *Roach Motel* dark pattern appears to be less recognised compared to other dark patterns from a user's perspective [196]. Finally, *Preselection* is another dark pattern, where options that are favourable to the business are pre-selected, such as options to receive promotional email or agreeing to recurring charges [207].

Di Geronimo et al. examined 240 mobile apps and conducted an online experiment with 589 users on how they perceive dark patterns [119]. Their analysis revealed that 95% of the examined apps include one or more forms of dark patterns, with popular applications typically featuring at least seven distinct forms of deceptive interfaces, on average. Einav et al. analysed credit card data used in

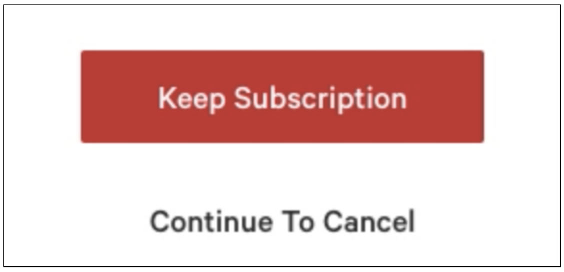


Figure 4.3: The Athletic cancel button, where 'keep subscription' is notably highlighted.

payment for ten subscriptions, and revealed that subscription businesses benefit from inattentive customers [123]. Using data from 23 million accounts, they found that users are more likely to cancel their subscriptions during the months when their cards are replaced (e.g., due to theft or loss). In a similar study Miller et al. studied consumer *inertia*, using a news site contract that automatically renews or cancels [212]. They find that consumers anticipate their inattention and avoid subscribing to contracts which auto-renew.

Recently, Glaser compared the cancellation process of four major streaming platforms and found dark patterns, such as highlighted re-subscribe buttons (see Fig. 4.3 for an example of this) in all platforms except Netflix [143]. Disney+ took the least time to cancel at 51 seconds with C More taking 60 seconds. Glaser also performed a user study and found that users aged 50-59 had the most difficulty in unsubscribing compared to those in their 20's [143].

Table 4.1 provides a overview of literature available and comparatively highlights how this study differs from others.

Table 4.1: Comparative literature table, highlighting what our study covers and the gap in related work

Title	Year	Vulnerable Users	Roach Motel	Dark Patterns	Subscribing	Regulations	Simulated Users
Tales from the dark side: Privacy dark strategies and privacy dark patterns [65]	2016			✓			
The dark (patterns) side of UX design [147]	2018	✓	✓				
Dark patterns at scale: Findings from a crawl of 11K shopping websites [206]	2019			✓		✓	
Dark patterns–An end user perspective [199]	2019			✓			
"Nothing Comes Before Profit" Asshole Design In the Wild [88]	2019			✓			
Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems. [91]	2019			✓			
UI dark patterns and where to find them: a study on mobile applications and user perception [120]	2020			✓			

Table 4.1: Comparative literature – continued from previous page

Title	Year	Vulnerable Users	Roach Motel	Dark Patterns	Subscribing	Regulations	Simulated Users
Towards the identification of dark patterns: An analysis based on end-user reactions [196]	2020			✓	✓		
Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces [222]	2020			✓			
Dark Patterns: Malicious Interface Design From a Users' Perspective [51]	2021		✓				
"I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!"- Dark Patterns from the End-User Perspective [60]	2021			✓			
Shining a light on dark patterns [194]	2021			✓		✓	
What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods [207]	2021			✓		✓	

Table 4.1: Comparative literature – continued from previous page

Title	Year	Vulnerable Users	Roach Motel	Dark Patterns	Subscribing	Regulations	Simulated Users
A comparative study of dark patterns across web and mobile modalities [151]	2021			✓		✓	
Dark patterns: Towards a socio-technical approach [42]	2021		✓	✓			
Dark patterns and the legal requirements of consent banners: An interaction criticism perspective [146]	2021			✓		✓	
What is the optimal unsubscribing journey for paid video streaming services? [143]	2022			✓	✓		
Towards understanding the dark patterns that steal our attention [214]	2022			✓			
Selling Subscriptions [124]	2023			✓	✓		
Sophisticated consumers with inertia: Long-term implications from a large-scale field experiment [212]	2023				✓		

Table 4.1: Comparative literature – continued from previous page

Title	Year	Vulnerable Users	Roach Motel	Dark Patterns	Subscribing	Regulations	Simulated Users
Staying at the Roach Motel: Cross-Country Analysis of Manipulative Subscription and Cancellation Flows [268]	2024	✓	✓	✓	✓	✓	✓

4.4.1 Digital Newspaper Subscriptions

Research regarding newspaper subscriptions is largely from the business point of view, focusing on consumer retention and the underlying factors that motivate individuals to subscribe to online news services [92, 131]. Notably the research describes a model that is struggling to retain subscribers [92]. Many online articles and blogs can be found to provide advice to news media on how to keep their churn rate low (the annual percentage rate at which customers stop subscribing to a service) such as tracking what content their consumers are reading and identifying which consumers are at risk of not renewing their subscription [274]. The following papers discuss business strategies to attract and retain consumers [71, 81, 114, 127, 169, 226, 244, 296]. COVID 19 boosted news paper subscriptions with many users opting for paid subscriptions due to a heightened need for reliable and detailed news [174]. Borchgrevink-Brækhus et al. analyse non-paying digital news sites users and conclude that young people's experiences with digital news subscriptions are shaped by financial constraints, content relevance, user experience, and trust in the news source [64]. Chen et al. investigate how individuals perceive the value of news both on a personal level and within a societal context [86]. They also examines attitudes towards paying for news subscriptions and the factors that influence these perceptions. The Irish digital news report says that 33% of Irish users get their news from online sources, with a significant increase in the number of people aged 18-24 paying for digital news content [220]. According to the Digital News Report conducted by Reuters Institute for the Study of Journalism University of Oxford, the proportion that pay for online news across 20 countries is 17% – a figure that has not changed for the last three years [255]. This same study highlights that trial prices usually draw people into subscribing but the full price turns them away [255]. Given that digital news appears to struggle to retain subscribers, this could in part explain why newspaper subscriptions are notably difficult to cancel [166].

4.4.2 State of subscriptions

Here we mention market and user surveys related to subscriptions and cancellations. We note that most surveys cited here are not peer-reviewed.

4.4.2.1 United States

Subscriptions to newspapers have increased by 30% in the US during the pandemic and they appear to still be on the rise [82]. In 2021, the American Press Institute conducted a study on 526 publications' retention strategies, and found several strategies appear to aim at reducing cancellations [274]. For instance 60% of the respondents said their "customer service reps are trained in tactics for 'saving' renewals when customers ask to cancel", 28% said they segment subscribers based on their cancellation risk [274]. On the other hand, 41% said they make their subscriptions easy to cancel to improve customer experience [274].

4.4.2.2 Germany

In 2022, the Federation of German Consumer Organisations (vzbv) examined around 840 websites involving subscriptions across all sectors to study how the Fair Consumer Contracts Act (FCCA) was being implemented [3]. The study revealed that of the 840 websites, 349 did not feature a cancellation button, 65 featured concealed cancellation buttons, with 38 featuring invalid labels. The vzbv[8] released a website where consumers can report any website that does not have a compliant *cancel button* [3]. In the months following the enactment of the FCCA, consumer watchdogs were reportedly sending cease and desist letters to several online businesses [179].

[8]vzbv: https://www.verbraucherzentrale.de/vertraege-reklamation/kuendigungsbutton-nicht-gefunden-so-muss-die-onlinekuendigung-aussehen-78472

According to a survey [248] conducted by the subscription management platform Recurly, the majority of German consumers spend up to €100/month on subscriptions, with 67% of Germans using one or more subscription services. On average, German consumers have three subscriptions, and 70% cancel their subscriptions as soon as any benefits expire [248]. A study undertaken by the German newspaper Der Spiegel found special offers work better in attracting and retaining customers as paid trial subscribers overall tend to value the content more and are more likely to keep their subscriptions than those who had a free trial [161].

4.4.2.3 The Netherlands

The National Institute for Budget Information report (2021) on subscription consumers in the Netherlands found that Dutch people underestimate how many subscriptions they have. The average household has 14 subscriptions, with 28% saying they often forget to cancel their subscriptions [157]. Of the respondents taking the survey, 22% said they find it a "hassle" to cancel online, with 30% saying they prefer to cancel online and 13% saying they put off cancelling as long as possible, as they dread the task [157].

In 2021 the Dutch Authority for Consumers and Markets (ACM) conducted a study into subscriptions and found websites make it unnecessarily difficult to cancel a subscription. In their study, they checked newspapers, magazines and lotteries. It was revealed that none of the nine businesses in the study provided an adequate range of online subscription cancellation options. Furthermore, some of the businesses did not offer the ability to cancel subscriptions online [135].

4.4.2.4 The United Kingdom

Consumers in the UK currently are estimated to spend £1.8 billion per year on subscriptions, the average household spends over £500 per year on subscription services [171]. Where the average household is spending up to £60 per year on unwanted subscriptions [171, 219], in other words subscriptions that are easily forgotten and not actively used. These usually occur as a result from free trials, automatic renewals, and/or extended roll-over periods [171]. A 2021 survey conducted on 2,000 UK adults showed that 16% of the respondents hold newspaper and magazine subscriptions, with 68% feeling their subscriptions were good value for money [251].

4.4.2.5 Summary:

The surveys mentioned above show that across all countries included in our study, subscriptions constitute a major market where users spend billions of dollars every year, with many underestimating how many subscriptions they have. In addition the surveys show the difficulties users experience when trying to cancel their subscriptions.

4.5 Methodology

An overview of the methodology can be seen in Fig. 4.4. As we discussed in Sec. 4.1, our objective is to characterise the subscribing and cancelling pathways for news media sites in the USA, the UK, the Netherlands, and Germany. This objective can be achieved through various methods. One potential approach involves direct inquiries to businesses regarding their practices, while another entails leveraging crowdsourcing to gather information from participants about their encounters with the studied businesses. In our study, we chose the method of employing simulated personas for subscription and cancellation processes, which enabled us to directly collect the study data. This approach mitigated the potential for inaccurate or biased information stemming from businesses or participants.

The budget for this project was capped at €500. Planning had to accommodate some uncertainty; for instance, if cancelling a website subscription proved challenging, there was a risk of exceeding the budget. As a result we targeted 80 sites at an expected cost of €5 per site per month, knowing also that some sites would likely have free trials. The total for this study amounted to €412.92. The total cost to subscribe to all new-sites including the US to Europe would have been €990.65.

We scheduled an average time span of 1.25 months to accommodate some subscriptions potentially extending into an unplanned second month. We kept paid subscriptions for one month and cancelled all subscriptions before the end of the payment term, or before trials ran out, to avoid being charged for a second term. The subscription and cancellation processes started in 5 January 2023 and ended in 7 February 2023. We spent roughly two person-months to record and code the subscriptions and cancellations.

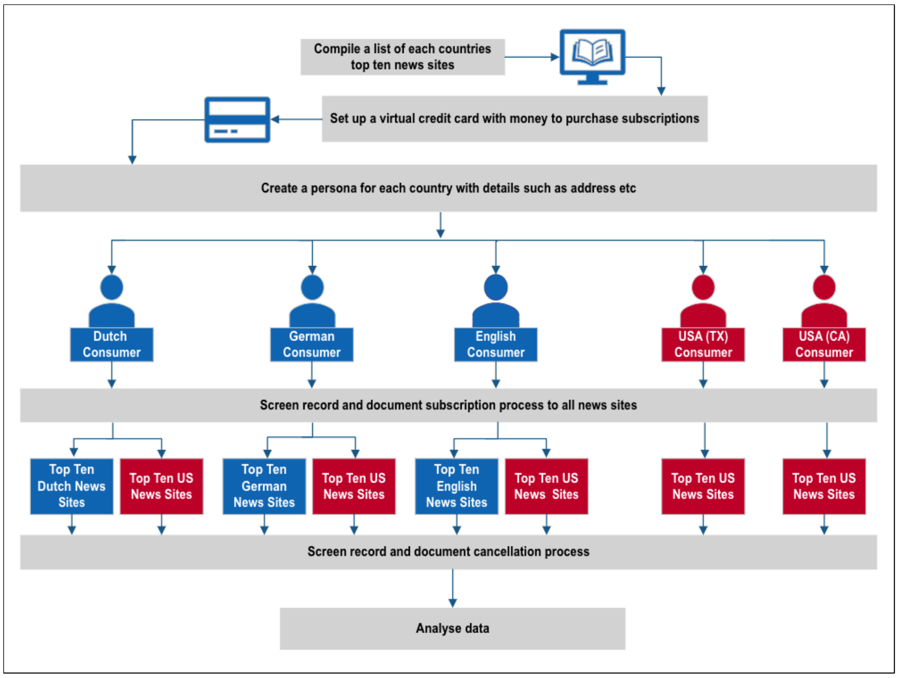


Figure 4.4: Subscription methodology process.

4.5.1 Selection of news sites

For each country, we compiled a list of ten news sites. The news sites were gathered from the Global Digital Subscription Snapshot (Q4 2022) report compiled by the International Federation of Periodical Publishers (FIPP) [233]. Data about all forms of media are included in this report, including a list of newspapers ranked according to the number of subscribers they have [232]. From this list, we took the top ten US and German newspapers. We omitted two US media outlets, which were not news related[9] and replaced these with next ranking news media websites. We chose to include the newsletter subscription service Substack, because it offers subscriptions to independent journalists, subject-matter experts, and media platforms [107]. There were only seven British newspapers and no Dutch newspapers in the Global Digital Subscription Snapshot report. To account for this, we picked the remainder from Wikipedia's lists of Dutch and British newspapers by circulation [302, 303]. Since we focus on online subscriptions, instead of circulation volume (modern news papers do not publish circulation numbers anymore),

[9]The Weather Channel and Americas test kitchen

we ordered these by their Tranco rank[10], which are marked with an asterisk in Table 4.2.

This table provides an overview of the news sites we successfully subscribed to from each country. Newspapers that are picked from Wikipedia and ranked by Tranco are marked with an asterisk.

4.5.2 Personas and subscriptions

For each country, we created a persona to subscribe to our compiled lists of news sites. Our Dutch, German and English persona subscribed to both their national and US news sites. American personas subscribed to American news sites only. Our rationale behind this decision was based on the assumption that Europe in general, has stricter regulations, making European subscriptions to US sites more likely to yield intriguing results than the reverse scenario.

As mentioned in Sec. 4.3.1, California has implemented guidelines on cancelling subscriptions online, but Texas has no guidelines in place as yet [130]. For this reason, when subscribing to American media, we used a separate persona for California and Texas. This resulted in a total of five personas, which we created using a fake name generator website [21]. Using a VPN connection, each persona signed up for subscriptions appearing to connect from their own country[11]. The subscriptions were paid for with a virtual credit card with a low limit, which we monitor for charges.

4.5.3 Data collection protocol and evaluation parameters

Following the protocol below in Sec. 4.5.3.1, we documented the subscription process by recording the screen during the subscription and cancellation processes. In addition we documented each subscription and cancellation according to the parameters listed in Table 4.3.

[10]Tranco website `https://tranco-list.eu/`. This website was also employed in Chapter 3 on cookie banners to identify and collect Irish websites.
[11]We used Mullvad VPN [23].

Location	Organization	Num. of Subscribers (or Tranco rank*)	Subscription Price	Trial Period	Trial Price
United States	The New York Times	8.3M	$4.25/w	1 y	$1.00/w
	Wall Street Journal	3M	$9.75/w	1 y	$2.00/w
	Washington Post	2.7M	$12.00/m	1 y	$4.00/m
	The Athletic	1.1M	$7.99/m	1 y	$1.99/y
	Substack	1M	$5.00/m	-	-
	Medium	725k	$5.00/m	-	-
	The Daily Wire	600k	$14.00/m	-	-
	Barrons	535k	$5.00/w	1 y	$1.00/w
	LA Times†	500k	$4.00/w	6 m	$ 1.00/w
	Bloomberg Media	375k	$34.99/m	3 m	$1.99/m
United Kingdom	Financial Times	1M	£55.00/m	1 m	£1.00/m
	The Telegraph	578k	£12.99/m	3 m	Free
	The Times/Sunday†	421k	£26.00/m	3 m	£1.00
	The Guardian	420k	£3.00/m	-	-
	Tortoise	110k	£12.00/m	-	-
	Mail +	100k	£10.99/m	3 m	£0.90/m
	Spectator	33k	£33.99/q	1 m	Free
	The Economist	(628*)	£18.90/m	1 m	Free
	iNews	(5k*)	£1.24/w	-	-
	The Week†	(15k*)	£38.99 /13 issues	6 issues	Free
Netherlands	Het Algemeen Dagblad	(4k*)	€2.19/w	2 y	€1.50/w
	Telegraaf	(5k*)	€3.00/w	1 y	€1.75/w
	De Volkskrant	(7k*)	€3.12/w	2 y	€2.50/w
	NRC	(9k*)	€4.38/w	-	-
	Trouw	(13k*)	€3.12/w	2 y	€2.50/w
	Het Financieele Dagblad†	(26k*)	€52.00/m	1 m	€10.00/m
	Eindhovens Dagblad	(39k*)	€2.19/w	2 y	€2.00/w
	Noordhollands Dagblad	(44k*)	€3.00/w	1 y	€1.75/w
	Tubantia	(49k*)	€2.19/w	2 y	€2.00/w
	PZC	(65k*)	€2.19/w	2 y	€2.00/w
Germany	Bildplus	603k	€7.99/m	1 y	€1.99/m
	WeltPlus	200k	€9.99/m	1 m	€1.00/m
	Süddeutsche Zeitung+	136k	€9.99/m	1 m	Free
	Frankfurter Allgemeine	91k	€4.95/w	1 y	€2.95/y
	Rheinpfalz Plus†	47k	€15.40/m	1 m	€1.50/m
	Heise+	45k	€12.95/m	1 m	Free
	Rheinische Post+	26k	€7.99/m	3 m	€4.00/m
	Allgemeine Zeitung+†	21k	€2.99/m	-	-
	Kieler Nachrichten+	20k	€9.99/m	1 m	Free
	The Pioneer	17k	€25.00/m	-	-

Table 4.2: The compiled list of news sites, subscribers/rankings, subscription cost and trial subscription period/prices offered. †All news sites blocked from subscribing. *News sites sourced from Wikipedia and ranked by site visits in Tranco.

In compiling the parameters we aimed to record as much detail as possible about each subscription and cancellation, pertaining to our objectives in Sec. 4.1.1 Moreover, we included parameters based on regulatory requirements in the studied countries such as whether a two-step termination button exists or whether users are informed about auto-renewals. Additional parameters that we recorded but have not tabulated in the results section are listed in Sec. E.3 in Appendix E.

While we tried to be as thorough as possible in compiling the evaluation parameters, we do not claim that they constitute an exhaustive list. Certain parameters such as 'Num. of Clicks' for subscription and cancellation (S5 and C7) may not precisely capture the difficulties that users experience when engaging with these flows. We discuss further limitations in Sec. 4.7.2.

In the cases where it was necessary to cancel by phone, we took notes on the conversation. For the subscription and cancelling steps, we count how many 'click next' buttons we encounter in the subscription and cancelling flow. The number of 'clicks' made during subscription or cancellation flows roughly correspond to the number of steps in the process. Clicks made during account sign-up, those used to select survey answers from drop-down menus, and clicks made for personalising service preferences were all exempt from the click count.

Code	**Table**	**Parameter**	**Description**	**Relevance**
S1	3	Renewal information	Is information on renewal terms available on the website?	Important for properly informing users. Required by regulation such as: FTC Act (US, CA) [24], UCPD (EU) [18], CMA Guidance (UK) [11].
S2	3	Email Confirmation (Subscription)	Did we receive an email confirming subscription?	To provide details on subscription. Required by regulation such as: FTC Act (US, CA) [24], FCCA (DE) [79].
S3	3	Information on Cancelling (Before Subscription)	Is information available on the interface before subscription?	Info before subscribing could aid in decision to purchase subscription. Required by regulation such as: FTC Act (US, CA) [24], ACM Guidelines (NL) [26].
S4	3	Information on Cancelling (During Subscription)	Is information available on the interface during the subscription process?	Required by regulation such as: FTC Act (US, CA) [24], ACM Guidelines (NL) [26].
S5	3	Num. of Clicks (Subscription)	How many times do you need to 'click' to move to next page or task when subscribing?	Number of clicks quantify the length of the subscription flow.
S6	3	Required Sign-up Data	When subscribing what data is requested? Email, phone number etc.	Often data requested is unecessary *Forced Action* (dark pattern) adding to time needed to subscribe.
C1	4	Cancellation Method	Was the subscription cancelled online, by email, phone, chatbot or a form?	For usability purposes what options are available? Online cancellation required by legislation such as: FTC Act (US, CA) [24], FCCA (DE) [79] ACM Guidelines (NL) [26].
C2	4	Exit Survey	When cancelling, is there an exit survey asking for cancellation reason?	Exit surveys can add extra steps to cancelling, ACM Guidelines (NL) [22].
C3	4	Mandatory Exit Survey	Is the exit survey mandatory to answer?	Forcing people to take a survey can constitute a barrier, ACM (NL) guidelines [22] . Dark pattern: *Forced Action*.
C4	4	Special Offers	Are there special offers or discounts while cancelling?	Offers and discounts can add extra steps to cancelling.
C5	4	Email Confirmation (Cancellation)	Did we receive an email confirming cancellation?	Provides proof of cancellation. Required by regulation such as: FTC Act (US, CA) [24], FCCA (DE) [79].
C6	4	Two-step Termination	Is there a termination button such as the German FCCA law stipulates, which allows cancelling in two steps?	For comparison to strictest regulation (FCC Act [79, 140, 230]).
C7	4	Num. of Clicks (Cancellation)	How many times do you need to 'click' to move to next page or task when cancelling?	Number of clicks quantify the length of the cancellation flow.

Table 4.3: Descriptions of evaluation parameters considered in this study. Subscription parameters are denoted by codes starting with S, and cancellation parameters by C. The 'Table' column shows in which table the corresponding results can be found. Additional parameters that are recorded but not used in the results are given in Table E.3 in Appendix E.

4.5.3.1 Subscription Study Protocol

In order to make sure that the subscription process ran smoothly, we compiled a standard procedure. This prevents mistakes such as forgetting to change your VPN location when subscribing from Germany, and also saves time on inputting details.

1. For each individual persona, set up a Chrome account.
2. Before subscribing to a website, have your personas details ready for copying and pasting. The card details should also be on same page, along with passwords needed for accounts.
3. Another spreadsheet containing all media links and details should also be open.
4. When subscribing from each individual personas country, turn on VPN for their location and open their Chrome account.
5. From this personas Chrome account, click on subscription link in spreadsheet for each newspaper and start screen recording.
6. Scroll down through the website to document everything on all pages you click through.
7. Go through the process of subscribing to the account by copying and pasting persona details and stop recording when done.
8. Note details under each column in spreadsheet.
9. Repeat for cancelling subscriptions.
10. When phoning to cancel, have subscription details ready for verification.
11. Save recordings in separate folders for subscribing and cancelling.

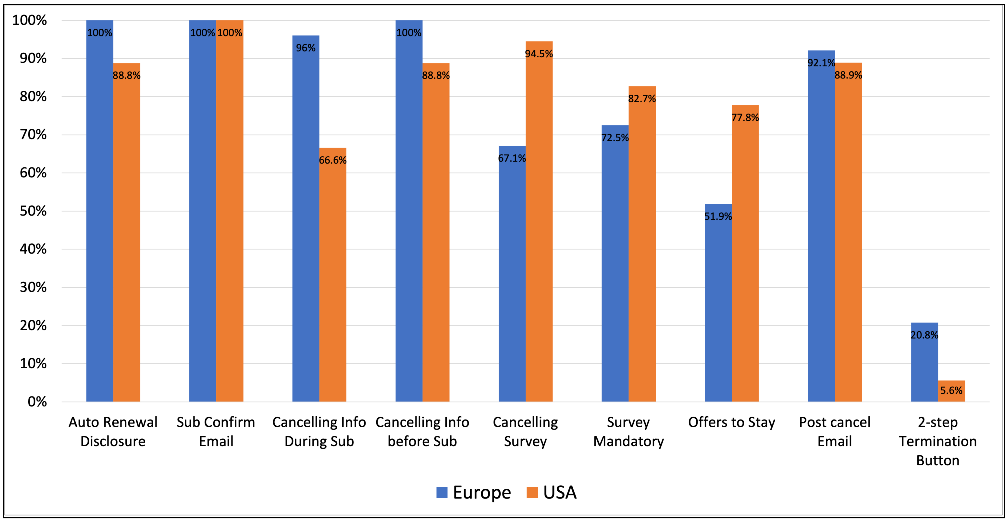


Figure 4.5: Overall summary of subscribing and cancelling results comparing Europe and USA. For the USA, the average of Texas and California is taken.

4.6 Results

4.6.1 Overview

We successfully signed up for 67 subscriptions of the total 80 subscriptions. Thirteen could not be made due to issues such as requirements to provide real addresses, and payment issues (reasons addressed for each country in the following sections). The LA Times was the only website in which all five personas failed to sign up to, potentially due to our use of a VPN connection. Fig. 4.5 displays overall differences in subscribing and cancelling between USA and Europe. Other aspects of the cancellation flow for each country are summarised in Fig. 4.8. Table 4.4 and 4.5 give an overview of subscription and cancellation flows studied.

Subscribing to European media from Europe required on average 3.5 clicks and 4.9 clicks to cancel. To subscribe to American sites from Europe on average required 3.2 clicks and 6.2 to cancel. Our American personas needed on average 3.6 clicks to subscribe to their American news sites and 5.8 clicks to cancel. The average number of clicks required to subscribe or cancel in each location is given in Fig. 4.6.

Country	Organization	Automatic renewal disclosure	Sub. confirm email	Info on cancelling during subscription	Info on cancelling before subscription	Clicks to subscribe
Germany	Bildplus	✓	✓	✓	✓	3
	WeltPlus	✓	✓	✓	✓	3
	Süddeutsche Zeitung+	✓	✓	✓	✓	5
	Frankfurter Allgemeine	✓	✓	✓	✓	5
	Heise+	✓	✓	✗	✓	4
	Rheinische Post+	✓	✓	✓	✓	4
	Kieler Nachrichten+	✓	✓	✓	✓	5
	The Pioneer	✓	✓	✓	✓	4
Average		100%	100%	87.5%	100%	4.1
Netherlands	Het Algemeen Dagblad (AD)	✓	✓	✓	✓	3
	Telegraaf	✓	✓	✓	✓	3
	De Volkskrant	✓	✓	✓	✓	3
	NRC	✓	✓	✓	✓	3
	Trouw	✓	✓	✓	✓	3
	Eindhovens Dagblad (ED)	✓	✓	✓	✓	3
	Noordhollands Dagblad	✓	✓	✓	✓	3
	Tubantia	✓	✓	✓	✓	3
	PZC	✓	✓	✓	✓	3
Average		100%	100%	100%	100%	3.0
United Kingdom	Financial Times	✓	✓	✓	✓	3
	The Telegraph	✓	✓	✓	✓	3
	The Guardian	✓	✓	✓	✓	2
	Tortoise	✓	✓	✓	✓	4
	Mail +	✓	✓	✓	✓	4
	Spectator	✓	✓	✓	✓	4
	The Economist	✓	✓	✓	✓	3
	iNews	✓	✓	✓	✓	3
Average		100%	100%	100%	100%	3.3
United States	The New York Times	✓	✓	✓	✓	4
	Wall Street Journal	✓	✓	✓	✓	5
	Washington Post	✓	✓	✓	✓	4
	The Athletic	✓	✓	✓	✓	2
	Substack	✗	✓	✗	✓	3
	Medium	✓	✓	✗	✓	3
	The Daily Wire	✓	✓	✗	✗	3
	Barrons	✓	✓	✓	✓	5
	Bloomberg Media	✓	✓	✓	✓	3
Average		88.8%	100%	66.6%	88.8%	3.6

Table 4.4: Overview of subscription flow features. United States represent both Texas and California, which had identical results for the scope of this table. Addressed in this table are questions S1 to S5 from Table 4.3. Not included in table are news sites which were blocked to our personas.

Country	News sites	Cancellation method	Cancellation survey	Cancellation survey mandatory?	Offers to stay	Post-cancel email	2-step termination button	Num. of steps/clicks to cancel
Germany	Bildplus	Online	✓	✓		✓		5
	WeltPlus	Online	✓	✓	✓	✓		6
	Süddeutsche Zeitung+	Online				✓	✓	5
	Frankfurter Allgemeine	Online			✓	✓		7
	Heise+	Online	✓		✓	✓		5
	Rheinische Post+	Online	✓	✓	✓	✓		5
	Kieler Nachrichten+	Online				✓	✓	4
	The Pioneer	Online (Form)				✓	✓	4
Average			50%	*75%	50%	100%	37.5%	5.1
Netherlands	Het Algemeen Dagblad	Online	✓		✓	✓		4
	Telegraaf	Online	✓			✓		6
	De Volkskrant	Online	✓	✓	✓	✓		5
	NRC	Phone				✓		
	Trouw	Online	✓	✓	✓	✓		4
	Eindhovens Dagblad	Online	✓	✓	✓	✓		4
	Noordhollands Dagblad	Online	✓					6
	Tubantia	Online	✓	✓	✓	✓		4
	PZC	Online	✓	✓	✓	✓		6
Average			88.9%	*62.5%	55.6%	88.9%	0%	4.9
United Kingdom	Financial Times	Online	✓		✓	✓		6
	The Telegraph	Online	✓	✓	✓	✓		8
	The Guardian	Online	✓	✓	✓			5
	Tortoise	Online				✓	✓	4
	Mail+	Phone	✓	✓		✓		
	Spectator	Online (Form)				✓		4
	The Economist	Online	✓	✓	✓	✓		7
	iNews	Online				✓	✓	4
Average			62.5%	*80%	50%	87.5%	25%	5.4
USA Texas	The New York Times	Online	✓		✓	✓		7
	Wall Street Journal†	Phone	✓	✓		✓		
	Washington Post	Online	✓	✓	✓	✓		6
	The Athletic	Online	✓	✓	✓	✓		6
	Substack	Online	✓			✓		5
	Medium	Online	✓	✓	✓	✓		5
	The Daily Wire	Online	✓	✓	✓	✓		4
	Barrons	Online	✓	✓	✓	✓		5
	Bloomberg Media	Online (ChatBot)	✓	✓	✓			10
Average			100%	*77.8%	77.8%	88.9%	0%	6.0
USA California	The New York Times	Online	✓		✓	✓		7
	Wall Street Journal	Online	✓	✓		✓		5
	Washington Post	Online	✓	✓	✓	✓		6
	The Athletic	Online	✓	✓	✓	✓		6
	Substack	Online				✓	✓	3
	Medium	Online	✓	✓	✓	✓		5
	The Daily Wire	Online	✓	✓	✓	✓		4
	Barrons	Online	✓	✓	✓	✓		5
	Bloomberg Media	Online (ChatBot)	✓	✓	✓			10
Average			88.9%	*87.5%	77.8%	88.9%	11.1%	5.7

Table 4.5: Overview of the cancellation flow in each country. Percentage taken from news-sites which presented surveys*. Addressed in this table are questions C1 to C7 from Table 4.3. Not included in table are news sites which were blocked to our personas.

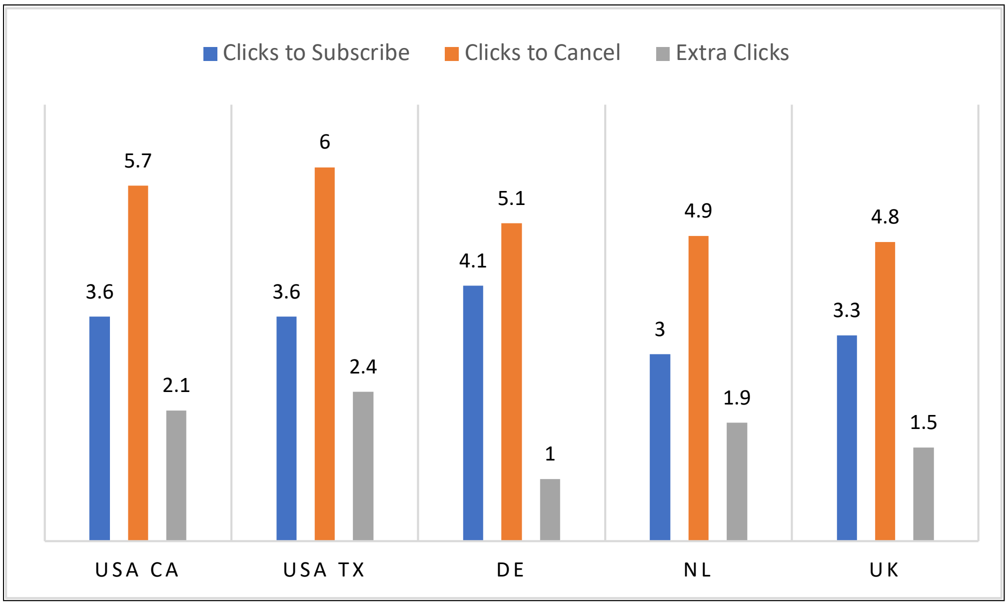
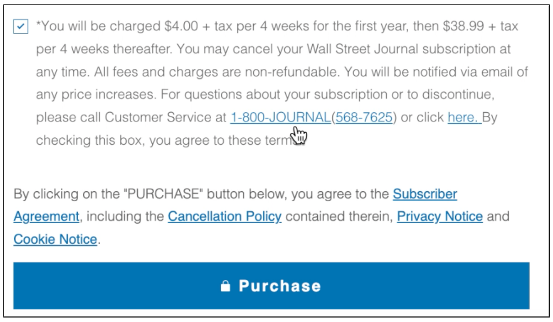


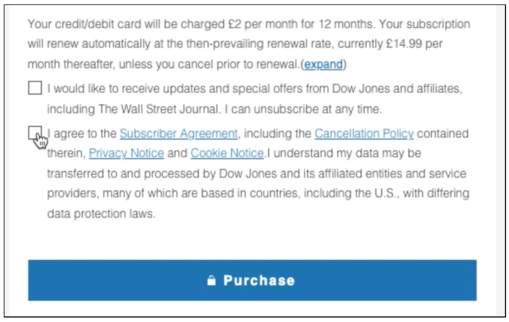
Figure 4.6: Average number of clicks it takes to subscribe and cancel for each location. Extra clicks indicate the difference between the number of clicks for cancelling and subscribing. Note: CA and TX are subscribing to the same list of American news sites and each European persona is subscribing to their national news sites.

Auto-renewal disclosure: Substack (US) was the only website that did not refer to auto-renewal in their subscription flow[12]. All other sites informed users about the auto-renewal of their subscriptions. Auto-renewal information is predominantly presented in fine print on the payment page (see Fig. 4.10b). This message informs users that by purchasing a subscription, users acknowledge and agree to the terms of automatic renewal. On 14 of the 34 websites, this auto-renewal message included a tick box, whereupon ticking indicates that you understand the subscription's auto-renewal terms and conditions. Examples of three different terms and conditions acknowledgement messages can be seen from The Wall Street Journal in Fig. 4.7. Three news sites included an auto-renew button that can be toggled to disable subscription from auto-renewing at the end of the month. This design allows users to pause their subscriptions and saves them from the burden of cancelling.

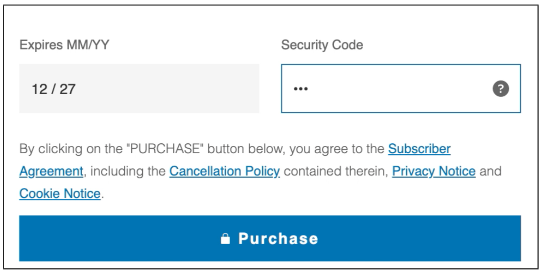
[12] According to its help page, Substack sends reminders one week before automatic renewal of both monthly and yearly subscriptions [29]



(a) WSJ, California USA



(b) WSJ, United Kingdom



(c) WSJ, Texas USA

Figure 4.7: Three different auto renewal information boxes for Wall Street Journal, California (a) includes a tick box acknowledging auto renewal terms, UK (b) acknowledges subscriber agreement and is less clear and Texas (c) acknowledges subscriber agreement by purchasing the subscription.

Only 3 out of the 34 individual media sites (USA, UK, NL & DE) included an auto-renew button which can be toggled to disable subscription from auto-renewing at the end of the month.

Information on cancellation: All European media provide information on cancelling subscriptions in the website, either on the homepage or inner pages. In the US, the situation is similar with eight out of nine websites providing some form of information about cancelling.

Offers to stay & exit surveys: Overall 51.9% of the European media we subscribed to, presented special offers to incentivise staying and an average of 67.1% requested reasons for leaving the subscription through the means of a survey. For roughly 72.5% of the European websites, it was mandatory to answer these surveys.

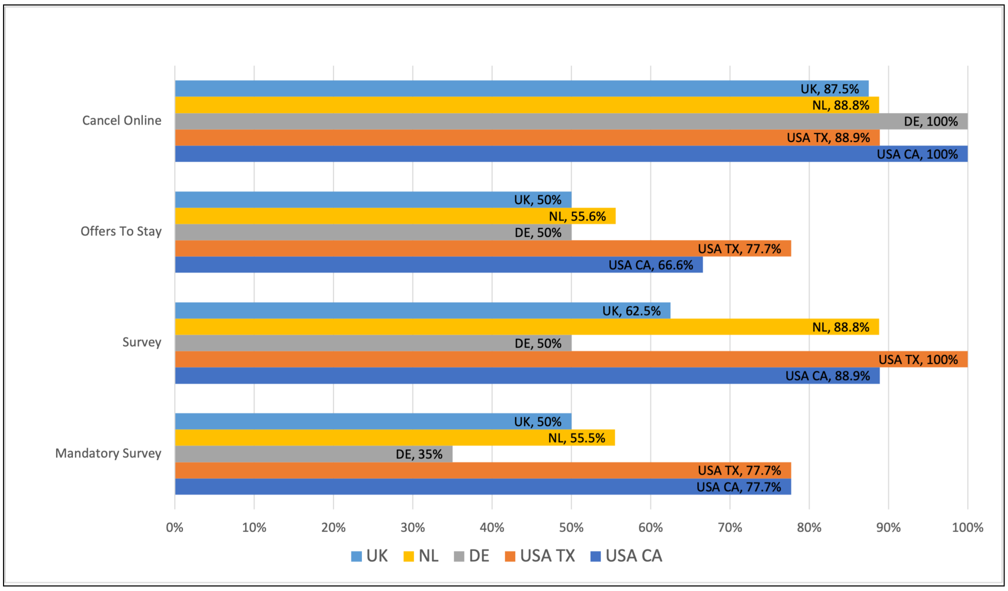


Figure 4.8: Average percentages per country measuring whether we could cancel online, if advertising followed cancelling, if we were asked why we want to leave and if this survey was mandatory.

For the US roughly 77.8% of the websites offered discounts to encourage staying, and almost all of the US websites (for Substack California no survey was requested) requested reasons for cancelling the subscription in the form of a survey, with 82.7% making it mandatory to answer.

Post-cancellation email: After cancelling all subscriptions, 88.9% of the American and 92.1% of the European news subscriptions provided a post-cancellation email. Exceptions to this were the Dutch media site Noordhollands Dagblad and the UK's Guardian. Once subscriptions were cancelled for all accounts, our personas continued to receive emails requesting they re-subscribe and providing news updates.

Below we will discuss results in more detail for each country and we give an overview of dark patterns encountered during our subscription and cancellation processes.

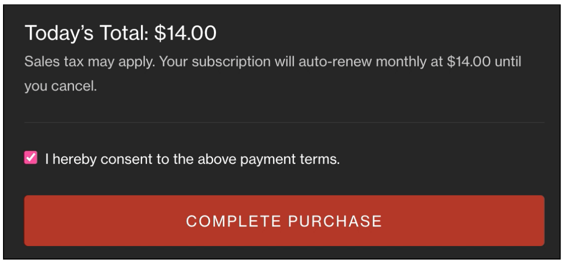


Figure 4.9: Daily Wire's auto-renewal acknowledgement tick box.

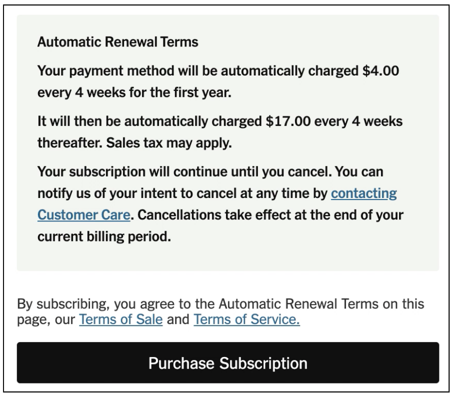
4.6.2 United States of America

4.6.2.1 Subscribing

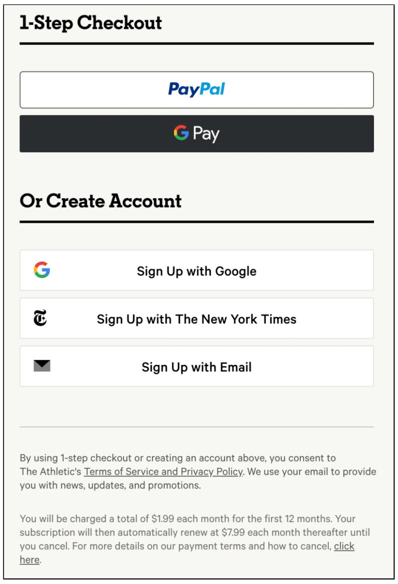
We successfully subscribed to nine of the ten American news sites using our Texan and Californian personas. As mentioned in the overview, LA Times blocked our attempts to subscribe from all countries. Our European personas were successful in subscribing to eight of the ten US media sites. As well as being blocked from LA Times, our European personas were also blocked from subscribing to Barron's due to location.

Six of the nine US news sites provided information on cancelling during the subscription flow. Eight of the nine media sites informed our users about the automatic renewal of their subscriptions, during the subscription process, Substack provided auto-renew information only on their help centre page.

All websites provided a post-subscription email in which they notified consumers of their renewal policy. Only four of the nine US websites subscribed to by our Californian persona, featured an auto-renew acknowledgement box to tick (for example see Fig 4.9). For our Texan consumer, Barron's and Wall Street Journal did not feature this tick box, which was available to our Californian consumer. The remaining websites informed their consumers of their renewal policy with a notification at the payment level with very small print. The New York Times notice, despite not featuring an acknowledgement tick box was at least clearer and easier to read, (see Fig. 4.10a). McCants asserts that companies take advantage of consumers' neglect in reading the fine print, as indicated by a Deloitte survey conducted in 2017 [209].



(a) New York Times



(b) The Athletic

Figure 4.10: (a) New York Times auto-renew notice at payment stage for all the countries in the study. Writing is in bold and notably bigger than the majority of news media sites studied. (b) The Athletic checkout page with their renewal information in small print at the end of the page.

The survey revealed that 91% of individuals consent to terms of service without actually reading them [73].

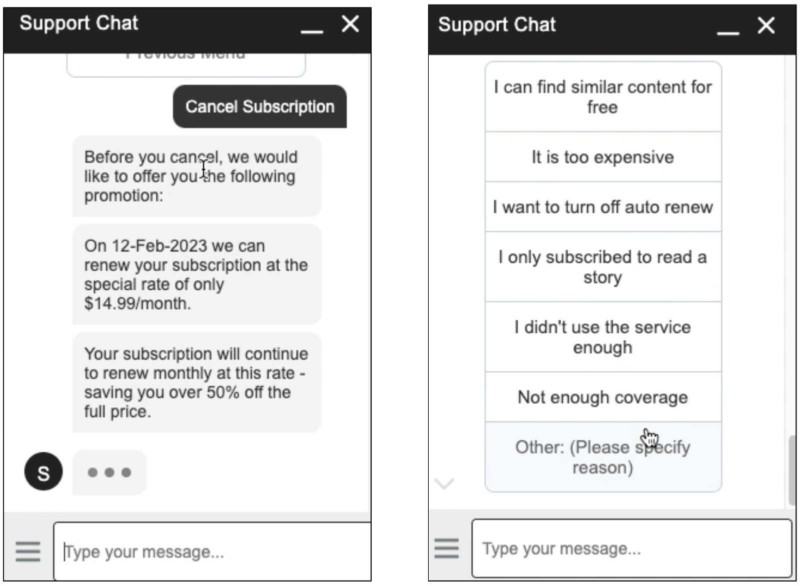
Washington Post, Medium and The Daily Wire were the only websites that explicitly state the next billing date in their post-subscription email. After subscribing to the Daily Wire's monthly subscription, we received several promotional emails inviting us to upgrade to their annual plan. Comparing the number of clicks required to subscribe, we find similar results for US and EU personas subscribing to US newspapers. On average, US personas executed 3.6 clicks, while European personas executed 3.2 clicks when subscribing to American websites.

4.6.2.2 Cancelling

It was possible to cancel all Californian subscriptions online. A phone call was required to cancel Wall Street Journal for our Texan and British consumers. The calls were no more than three minutes long, we were asked for an email address and a choice of giving a home address or the last few digits on the credit card. In all but one case (NRC), the customer representative requested our reasons for terminating the subscription. We were not offered discounts to stay during the calls. Shortly following the call, a cancellation confirmation email was received. Barron's and Wall Street Journal are both published by Dow Jones & Company. When purchasing a Barron's and Wall Street Journal subscription, they appear together on both website's settings. Despite this, Wall Street Journal requires you to call to cancel from Texas, when it is possible to cancel online for California, yet it is possible to cancel Barron's online for both California and Texas. The Bloomberg subscription required cancellation via chatbot flows for all personas, which required a total of ten clicks to cancel. The chatbot offered promotional discounts and asked for our reason for leaving (see Fig. 4.11).

On average it required 5.8 clicks to cancel, this average is taken from both Texas and California. With the exception of Substack for California, all American media sites inquired as to the reasons for your departure. Of these, 77.7% made answering mandatory. Seven of the nine Texan USA media accounts offered discounts to keep the subscription, whereas for California six out of the nine accounts offered discounts to stay. When cancelling Barron's from Texas, discount offers are presented, but not when cancelling from California. For the UK and Germany, Substack offered discounts.

Nineteen days after cancelling The Daily Wire, our consumers received a promotional email with an offer to re-subscribe. The initial email was followed by another email two days later, with the line "no pressure just wanted to bump this promotion". Yet again nine days later, another email is received notifying all personas that the offer is expiring. The Daily Wire was the only website which sent third-party promotions via email. Some of these emails requested donations. All media apart from Bloomberg sent a confirmation of cancellation email. The Washington Post's cancellation flow stood out from others, with the emphasis more on cancelling rather than convincing the customer to keep subscription. The 'Continue to cancel' button was presented more prominently in all dialogues in the cancellation flow (see Fig. 4.12).



(a) Bloomberg response after choosing to cancel from a list of options.

(b) After cancelling, Bloomberg requesting you answer a survey.

Figure 4.11: Bloomberg chatbot cancelling procedure.

Figure 4.12: Washington Post's cancel button highlighted with 'nevermind, don't cancel' less visible, contrary to the majority of media cancellation interfaces.

4.6.3 Germany

4.6.3.1 Subscribing

Our German persona was successful in subscribing to eight German media websites. Rheinpfalz Plus and Allgemeine Zeitung+ required real German addresses for a subscription, which we could not provide. Five of the news websites featured a *cookie paywall*, (see Fig. 4.13), where the user is presented with a paid subscription option that will limit tracking and advertisements. Morel et al. explored cookie paywalls and noted they are mostly used in news sites and do not prevent all tracking [215].

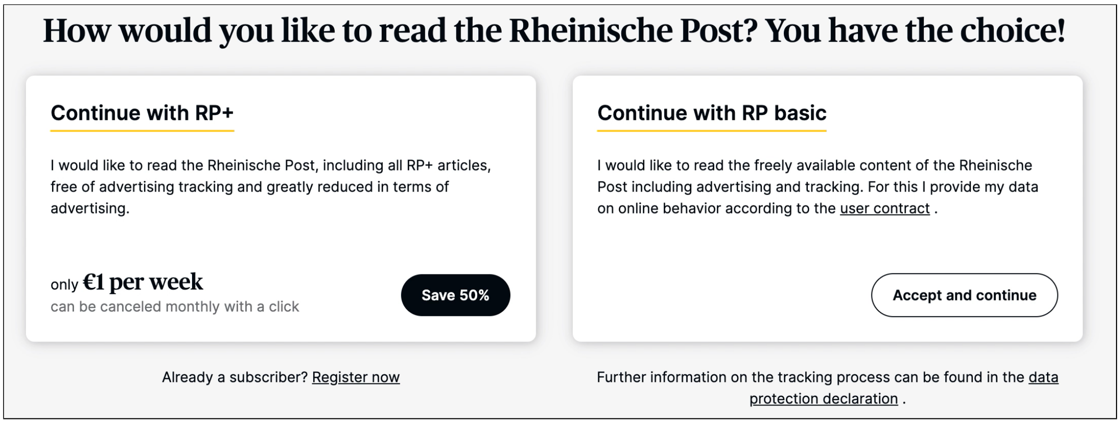


Figure 4.13: The *cookie paywall* [215] on Rheinische Post subscription page.

In Europe at present, there is a lack of consensus among Data Protection Agencies (DPA) as to whether cookie paywalls comply with GDPR requirements [215].

All websites provided notice of automatic renewal and information on cancelling was provided during the subscription flow. The exception to this was Heise, who provided no information on cancelling in their subscription flow. There were no auto-renewal acknowledgment/terms and conditions tick boxes at the payment level for any of the German websites.

All websites provided emails after subscribing, Kieler Nachrichten+ was the only account to state a renewal date in their post-subscription email. Bildplus and the Pioneer attach receipts with account information in their emails. The average number of clicks to subscribe was 4.1.

4.6.3.2 Cancelling

It was possible to cancel all subscriptions online on a monthly basis and all websites provided information for cancelling on their interface. One of the eight websites (The Pioneer) required filling in a form to cancel the subscription. This form requested full name, email and invoice number, the latter not being mandatory.

The Fair Consumer Contracts Act (FCCA), states it should take no more than one extra step after pressing the 'cancel now' button to successfully cancel your subscription [3].

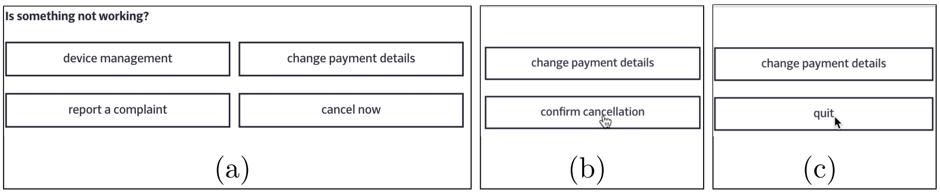
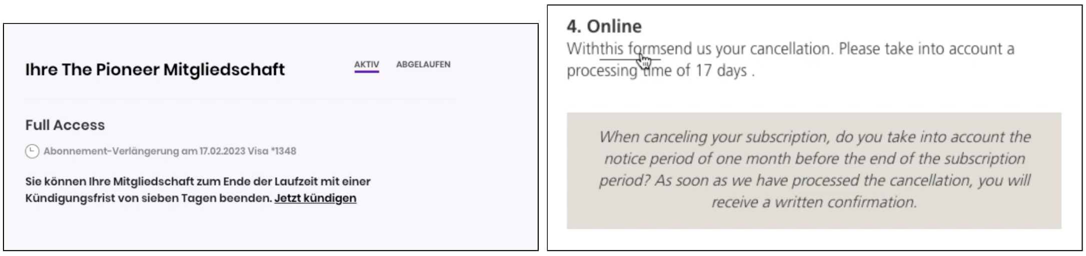


Figure 4.14: Süddeutsche Zeitung+ two click termination button



(a) The Pioneer

(b) De Telegraaf

Figure 4.15: Discrete links for cancelling Pioneers subscription (a), and De Telegraaf's discrete link for it's cancellation form (b).

In our study of German websites, we noted how many 'clicks' were required to cancel after pressing the 'cancel now' button. Only three of the eight websites satisfied this requirement. KN+ was the only German website which featured an auto-renew button which could be switched off. Fig. 4.14 shows an example of cancelling a subscription in two clicks, part (a) shows a clear 'cancel now' button, after clicking this, the button changes to a 'confirm cancellation' button (b). The subscription is cancelled when the 'confirm cancellation' button is clicked.

The Fair Consumer Contracts Act also stipulates that the 'termination button' must be prominently displayed and appropriately labelled. Certain links encountered on German news sites were not clear or obvious, compared to an clearly visible button. For instance, while the Pioneer's cancel link in Fig. 4.15a is underlined, it is unclear whether it constitutes a 'prominently displayed' button.

Out of the eight German websites, four inquire as to the reason for cancellation through the means of a survey, with three of these requiring mandatory responses. Four out of the eight websites offer discounts to stay. All provided emails confirming the cancellation, some of these contained further offers.

On average for German news sites it required 5.1 clicks to cancel.

4.6.4 The Netherlands

4.6.4.1 Subscribing

From our list of Dutch websites our Dutch persona was successful in subscribing to nine of the ten Dutch media sites on our list. Het Financieele Dagblad (FD) rejected Revoluts IBAN as payment. All websites provided information on automatic renewal and cancelling, both in the subscription flow and the website interface. All websites provided a tick box to acknowledge auto-renewal or terms and conditions. All Dutch websites required direct debit payments and sent post-subscription emails, none of which mentioned billing dates. It took on average three clicks to purchase a subscription.

4.6.4.2 Cancelling

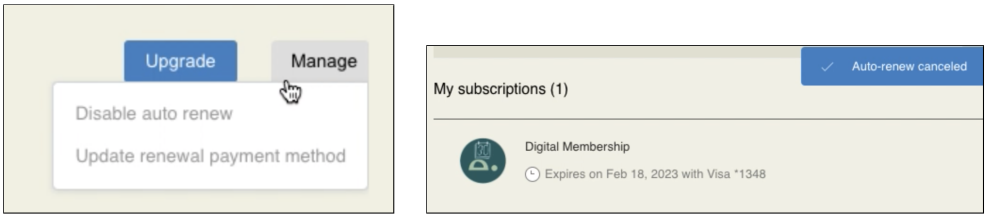
It was possible to cancel all subscriptions online with the exception of the NRC news site. Cancelling NRC required a phone call, during which we were on hold for ten minutes. When cancelling our Dutch media sites, all sites apart from NRC, requested a reason for leaving. De Telegraaf and Noordhollands Dagblad required us to fill in an online form that included an optional survey on reasons for leaving.

On average 55.6% of Dutch news sites display special offers to stay, but notably, these offers were often positioned on the same page as the 'cancel now' button. This contrasts with practices in other countries where such offers typically appear after starting the cancellation process. We received cancellation confirmation emails for all subscriptions bar one (Noordhollands Dagblad). On average it took 4.9 clicks to cancel.

4.6.5 United Kingdom

4.6.5.1 Subscribing

Our British persona successfully subscribed to eight out of the ten British websites from our list. The Times and The Week news sites also rejected Revolut as payment.



(a) (b)

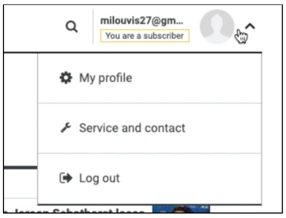
Figure 4.16: Tortoise auto renew button, (a) Disabling auto renew in manage subscription section, and (b) Information displayed after disabling auto renew.

All websites provided information on cancelling and automatic renewal, and all websites sent a post-subscribing email. Three websites provided a tick box to acknowledge auto-renew/terms and conditions. Emails varied in the amount of details given regarding subscription. The Daily Mail, The Guardian and Tortoise provided no details about renewal dates. On average it required 3.3 clicks to subscribe.

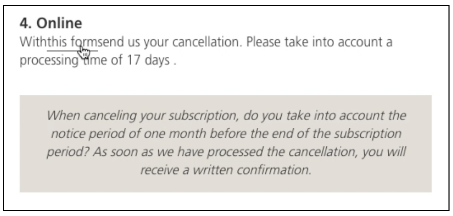
4.6.5.2 Cancelling

With the exception of The Daily Mail, it was possible to cancel all accounts online. For three of the websites, it was possible to cancel with two clicks. The Spectator required us to fill in an online form to cancel (see Fig. E.3 (b) in Appendix E). Tortoise and iNews both had a auto-renew button that could be toggled to disable auto-renewal without cancelling the subscription (see image 4.16).

Out of the eight British websites our British persona subscribed to, five requested a reason for cancelling in the form of a survey, and four of these websites made it obligatory to provide an answer. Four out of the eight websites offered discounts before confirming cancellation. All news sites apart from The Guardian, provided confirmation emails on cancelling accounts and on average required 5.4 clicks to cancel.



(a) Step One

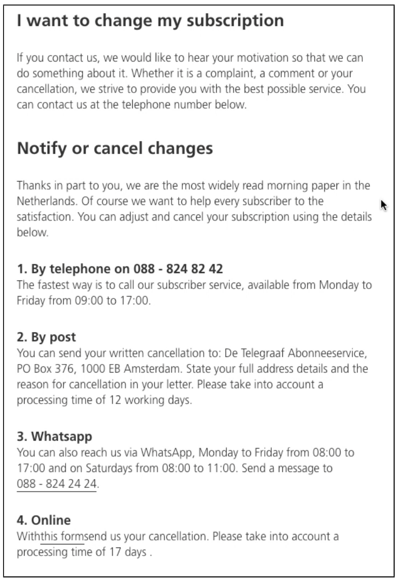


(b) Step Two

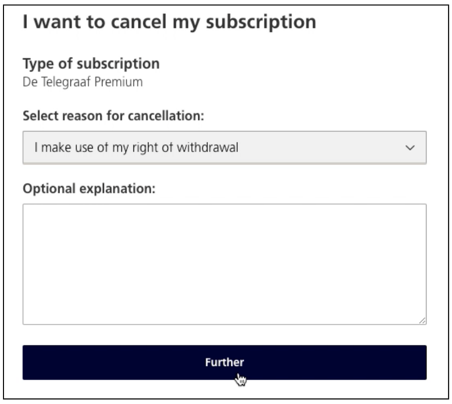
Figure 4.17: First two steps in cancelling De Telegraaf.

4.6.6 Cancelling De Telegraaf

An example of one cancellation process comes from De Telegraaf in the Netherlands. To cancel, our persona first goes to their profile in the top right corner of the website interface to a drop down menu (Fig. 4.17a). In the menu they choose 'service and contract' and are brought to another page. In this page they need to click on 'my subscription' and are brought to another page with their account details. This page displays a 'cancel now' button (see Fig. 4.17b), upon clicking this you are brought to a page which shows the different options to cancel (see Fig. 4.18a). The final option is to cancel online, where a barely visible link directs you to a form which you need to fill in. This form includes a drop-down choice of responses as to why you are leaving, one of which is "I make use of my right of withdrawal", after picking an option you click on 'further' (see figure 4.18b). The next page displays a confirmation notice where you can confirm cancellation by clicking the 'To confirm' button (Fig. 4.19a). The final page displays a notice confirming your cancellation and a message stating our persona would receive a confirmation email which we never received (Fig. 4.19b). On emailing the newspaper for information on this issue, a confirmation email was received a week later.

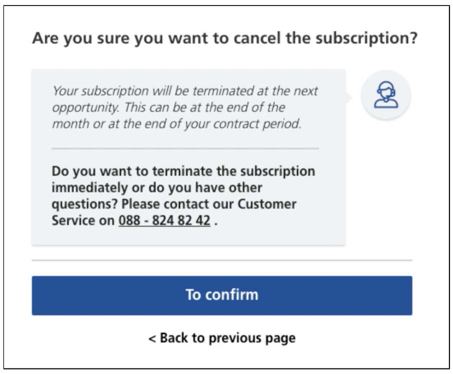


(a) Step Two

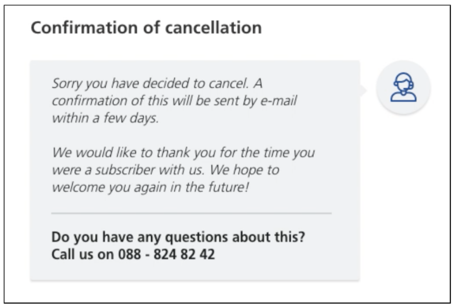


(b) Step Three

Figure 4.18: Choices of cancelling, cancelling online option at the bottom which leads you to the form in step three.



(a) Step Four



(b) Step Five

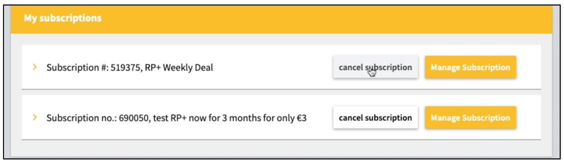
Figure 4.19: Final two steps in De Telegraaf cancellation process.

Category	Type	Description
Obstruction	Hard to Cancel (Roach Motel)	Making it easy for the user to sign up for a service, but hard to cancel it.
Forced Action	Forced Enrollment	Coercing users to create accounts or share their information to complete their tasks.
Misdirection	Confirmshaming	Using language and emotion (shame) to steer users away from making a certain choice.
	Visual Interference	Using style and visual presentation to steer users to or away from certain choices.
	Pressured Selling	Pre-selecting more expensive variations of a product, or pressuring the user to accept the more expensive variations of a product and related products.

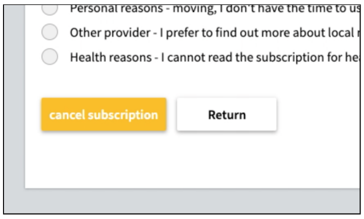
Table 4.6: Dark patterns found in this study with their descriptions and subcategories, taken from Mathur et al. [206].

4.6.7 Dark Patterns

In this section we present some examples of dark patterns encountered during our subscriptions and cancellation. We do not claim to present an exhaustive list of dark patterns, which is out of scope for our study. Instead, we aim to share representative examples based on the taxonomy classified by Mathur et al. [206]. We selected this taxonomy [206] for consistency, as the project lead from Radboud University, Gunes Acar, was also a co-author of the work. The patterns noted in subscribing were *Obstruction*, *Forced Action* and *Misdirection*. Some of these dark patterns are further categorised into types, which is seen in *Misdirection*. The three *Misdirection* types encountered in this study were *Visual Interference*, *Pressured Selling* and *Confirm Shaming*. *Hard to cancel* or *Roach Motel* are categorized under the *Obstruction* category. A summary of the dark patterns found in our study can be seen in Table 4.6. The most notable barrier to cancelling was the necessity of clicking through numerous steps of (often mandatory) surveys and promotional offers before finally cancelling the service.



(a) 'Cancel subscription' button here is white.



(b) 'Cancel subscription' is now yellow.

Figure 4.20: RP+ cancellation flow displaying colour changing.

Mathur et al. characterises *Visual Interference* as cases where an interface uses style and visual presentation to influence users' choices [206]. We noted many cases of alternating colours between the 'cancel' button and the 'keep subscription' button, which is categorized as *Bait and Switch* [66].

An example of this can be seen can be seen in Fig. 4.20 from the German newspaper Rheinische Post. The 'Cancel Subscription' button is initially white with the 'Manage Subscription' button in yellow. After pressing 'Cancel Subscription' however, the next page now displays the 'Cancel Subscription' button as yellow and the 'Return' button as white. This is a form of misdirection [206] and can potentially lead a consumer to inadvertently give up cancellation by pressing the wrong button.

Another example of *Visual Interference* noted was misleading buttons in a promotional offer from the Financial Times when cancelling. Our British persona is presented with both her current subscription and a yearly subscription, her options are to keep her current offer or to upgrade to a yearly offer. The 'Cancel Subscription' button is in black at the end of the page. The 'Confirm Change' button could be mistaken for 'Confirm Cancel' (see Fig. 4.21).

Although the majority of websites provided information on auto-renew, oftentimes the information was in very small print and could be overlooked. Cancel buttons were often hard to locate, hidden amongst plain text (Fig. 4.15 and Fig. 4.23) or placed at the bottom of the dialogues where they can missed (Fig. 4.21).

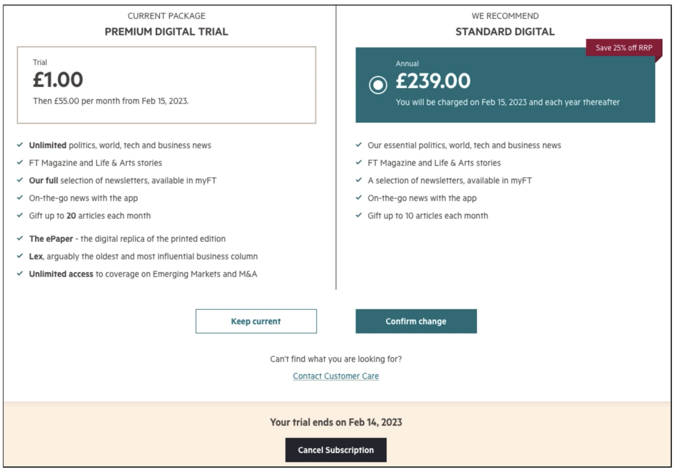
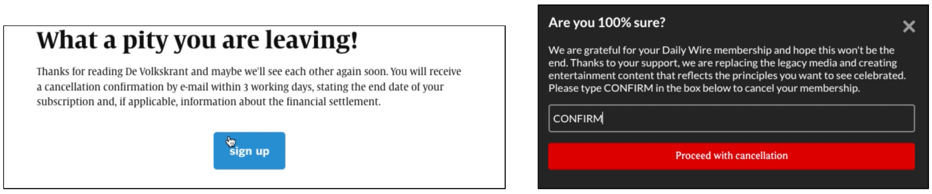


Figure 4.21: The 'confirm change' button may lead users to believe they are confirming the cancellation, but in fact it confirms purchasing an annual offer. The actual cancel button is in black at the bottom of the page, and it can be missed if the user does not scroll down.



(a) De Volkskrant

(b) Daily Wire

Figure 4.22: (a) Message received after cancelling De Volskrant and (b) the Daily Wire required users to type 'CONFIRM' to proceed with cancellation.

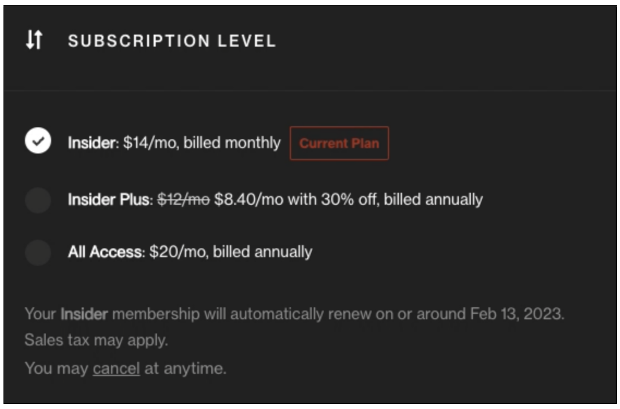
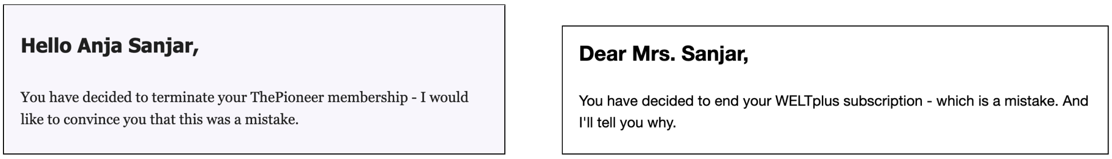


Figure 4.23: Spot the Cancel button, Daily Wires barely visible cancel button in its manage subscription level.



(a) The Pioneer

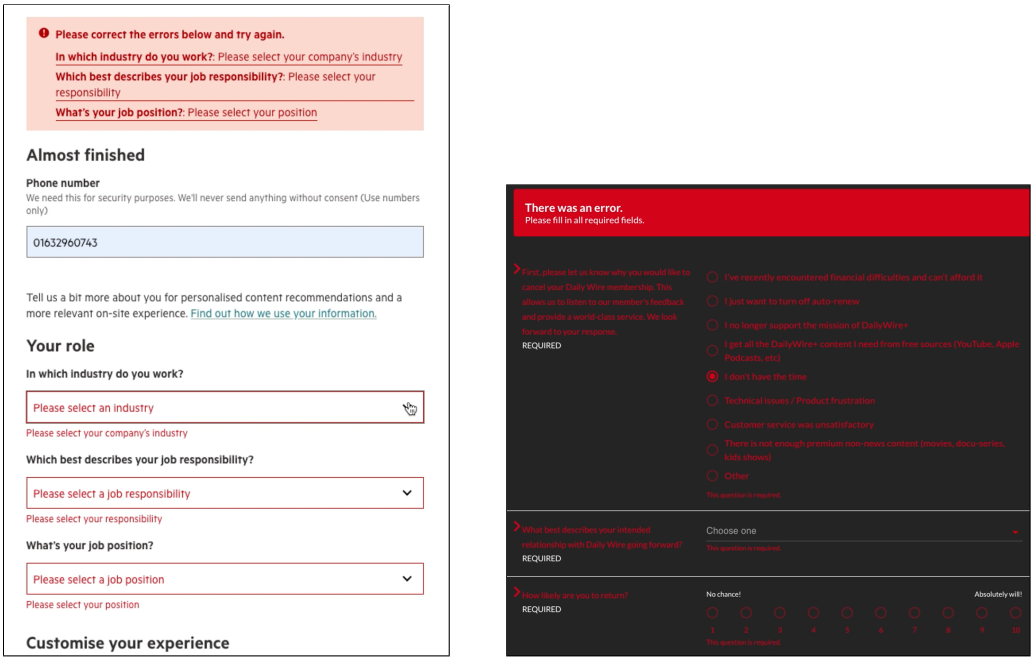
(b) WeltPlus

Figure 4.24: Messages received after cancelling subscriptions from WeltPlus and The Pioneer's news sites.

The *Pressured selling* dark pattern was observed for subscription options, with the most expensive option usually always pre-selected. *Confirmshaming* dark patterns was observed when cancelling subscriptions and in post-cancellation emails. Cancellation emails opened with a line such as "What a pity you are leaving!" (see Fig. 4.22a). The Pioneer's post-cancellation email expresses their belief that "Journalism is a participatory event" and they would like us to "be a part of the party again..". In some cases, the tone varied calling our decision to cancel our subscription a 'mistake' (see Fig. 4.24)[13].

Forced Action refers to interfaces that coerce users to take a certain action to complete a task. The Daily Wire required our consumer to type in 'CONFIRM' to cancel their subscription (see Fig. 4.22b)—which constitutes a *Forced Action*. While requiring users to create an account is understandable and does not constitute forced action, certain newspapers required more than necessary information during subscription. Overall, the type of data collected during subscription varied across our countries. Table E.1 in Appendix E shows what data each website requested. Some websites require only an email and others require country of residence and phone number. The USA and the United Kingdom news sites seem to demand a greater amount of data compared to their Dutch and German counterparts. Several websites asked for extensive personal details, including full address, date of birth, occupation, and phone number. Newspapers such as The Financial Times, The Economist, and Barron's requested significant personal information, such as occupation, under the pretext of 'improving' or 'tailoring' the user experience.

[13]The translation was confirmed as being accurate by one of the co-authors who is a native German speaker.



(a) Financial Times (b) Daily Wire

Figure 4.25: (a) Mandatory information required to sign up for the Financial Times subscription. (b) The Daily Wire makes it mandatory to answer survey questions during cancellation.

In certain instances, providing this information is mandatory (refer to Fig. 4.25a), leading to a cumbersome and long registration process. Many websites also featured pre-ticked boxes for promotional emails or newsletters.

4.7 Discussion

An overview of the results reveals that more European news sites provide information relating to auto-renewal and cancelling compared to the US. The US news sites also display more exit surveys and special offers to stay (Fig. 4.5). European news sites require fewer clicks to cancel in comparison to their American counterparts (Fig. 4.6). Differences were noted between some countries, for example the Netherlands subscriptions all required payment via direct debit and displayed their special offers on their manage-subscription page as opposed to after pressing cancel. Certain German news sites used cookie paywalls, which was not encountered in any of the other countries' news sites.

While our results show differences across jurisdictions, we cannot precisely attribute these changes to the differences in regulations. Other factors including market dynamics may have played a role, among others.

Throughout the process of investigating the regulatory framework in our selected countries, a commonly noted notion was that 'websites should make it as easy to cancel, as it was to subscribe'. Although cancelling online was available for 63 of the 67 subscriptions made in the study, it was not an effortless process. When cancelling, websites often took us through many different steps before reaching the end goal of exiting the contract. These obstacles included locating the cancellation button or link, answering mandatory survey questions (see Fig. 4.25b), and typing in a specific phrase.

While subscribing was usually less circuitous, not all were straightforward and certain subscriptions required considerable amount of personal information disclosure (see Table E.1).

As previously noted, certain subscriptions could only be cancelled by making a phone call to the customer representative. Calling to cancel, in most cases, was straightforward. Often the phone number was easier to locate than a cancel button. Three of the four phone calls made took only about three minutes. The remaining call (NRC, NL), however, took more than ten minutes. As mentioned in Sec. 4.1, requiring users to make phone calls is often associated with cognitive burdens insofar as anticipating and engaging in phone conversations can evoke anxiety in certain individuals. While offering the choice to cancel via phone call can be beneficial, it may not be a suitable option for all users. It should not be regarded as a one-size-fits-all solution or as a sufficient substitute for an easy online cancellation process.

To conclude this section, we would like to discuss possible paths to improve the state of user experience related to subscriptions and cancellations. From a regulatory perspective, we echo the three-fold route that Busch suggests [70]: (1) clear choices at the beginning of the subscription process (2) reminders about auto-renewals and prolonged inactive subscriptions and (3) a simple and unambiguous cancellation protocol.

Given the variety and complexity of cancellation flows observed in our study, a combination of high-level principles and specific regulations may simplify the process. The newly introduced German regulation mentioned in Sec. 4.3.2, is an example of unambiguous cancellation process as it requires a 'termination button'. This regulation provides details as to what this button should look like and where it should be placed. These precise requirements may make it harder to circumvent regulations, but in the long term they may potentially suffer from being too *technology-specific*, and may need to be updated.

4.7.1 Cancelling Subscriptions & The Seven Principles of Universal Design

As noted in Sec. 4.4 and Table 4.1, there is little research in the area of vulnerable users and dark patterns. In terms of aligning with the seven principles we note that cancelling subscriptions fail to align with five principles. Principle one; equitable use, as we noted in Sec. 4.2.1, if you are deaf or hard of hearing, it is not possible or very difficult to call to cancel, if this is necessary. Principle three; simple and intuitive use, subscriptions for the most part did not make it simple and intuitive to cancel contracts. It can require extensive searching to locate cancel features. Principle four; perceptible information, it is very often not clear how to cancel, with websites hosting different and sometimes confusing ways to cancel. Principle five; tolerance for error, if you make a mistake in the often confusing cancelling process, you end up paying for another month of a subscription, in some cases this can be a year long contract. Principle six; low physical effort, "minimise repetitive actions" we noted the steps to cancel are highly repetitive and unnecessarily long winded.

4.7.2 Limitations

The news sites which we investigated in this study are highly popular, and therefore may be subject to higher scrutiny and less likely to use manipulative design. While a random and varied list of newspapers could uncover other practices, studying popular websites has the advantage of studying the experience faced by millions of users.

Another limitation noted was the fact that all news sites used in our study were not all sourced from the same source FIPP [233]. It was difficult to get official subscription numbers from each countries news websites. Companies such as Statista[14] usually provide these stats and are behind a payroll, whats more these results (what could be seen) did not seem to match each other and therefore we thought the fairest way to gather a list was to source all the missing countries news sites from the same source; Wikipedia and then use Tranco to rank site visits. As our goal was to compile a list of news sites with a view to analyse the subscription and cancellation protocol and not gather official subscriber stats we felt this was reasonable.

To subscribe to Irish news sites would have been in keeping with the theme of this thesis admittedly, as we analyse Irish cookie banners in Chapter 3. As we note in Sec. 4.1.1 the Netherlands proved to be a more suitable choice for this study.

The study's budget limited the amount of new sites we were able to subscribe to, we acknowledge that it would be fairer to have our American personas subscribe to European news sites and likewise, with our individual European personas to subscribe to all countries in our European list of countries. We made an educated assumption that European countries are not likely to change their subscription process for other countries.

Screen captures were recorded and coded by myself (main language English) to identify dark patterns. In order to prevent potential biases and mistakes, the results were reviewed and discussed in several meetings with my collaborators; three senior researchers in the field of law, computer science and human computer interaction (HCI).

For non-English websites we used Google Chrome's internal translator and Gmail's translation option for emails. When these translators failed, we manually copied and pasted text to Google Translate, or used a smartphone app to translate non-English text. While the accuracy of these translations are generally high, there may be minor mis-translations.

[14] Statista:https://www.statista.com/

Our study is based on a snapshot of the subscription and cancellation processes at the start of 2023. These practices may change in time due to upcoming regulations, user feedback or for other reasons. Moreover, businesses that use A/B testing (split testing) might offer alternative cancellation options that may not be captured in our recordings.

The metrics that we use to characterise user experiences, such as the number of clicks, do not fully capture all difficulties posed by the cancellation interfaces. For example, in certain cases, finding a cancellation link hidden within a maze of menus may be a larger challenge than the actual cancellation process. For instance, several times the cancellation link was found at the bottom of the page, which could have been missed if the user did not scroll. Studying user experience metrics that consider the mental effort caused by these designs could help us understand the challenges of subscription and cancellation interfaces better.

4.7.3 Future Work

Future studies may use our methods to study news websites from different countries, for example Ireland and the global south. Another direction for further research would be to study different types of subscriptions, such as streaming services, online games, and physical deliveries (e.g., cosmetic products, cleaning supplies, groceries, clothes).

A longitudinal study, considering changes over time, might also shed light on the effects of regulatory changes or industry trends. Buying multiple subscriptions for the same site could identify A/B testing and help investigate the consistency of the subscription and cancellation process over multiple attempts. A user study could investigate what users find particularly challenging in subscription and cancellation flows, and what dark patterns are particularly effective in preventing cancellations against users' will.

The emails sent by the subscription services also offer an opportunity for further research, exposing the tactics employed to win back unsubscribed users.

4.8 Conclusion

While subscriptions can benefit online businesses by providing a sustained revenue, they may also pose a challenge when it comes to the complexities and obstacles users encounter while attempting to cancel them. To the best of our knowledge, our study is the first attempt to comprehensively characterise the difficulties encountered by users when trying to cancel online subscriptions across a range of news websites, from multiple vantage points.

Our results show that the majority (63/67) of subscriptions could be cancelled online, with a few exceptions where we were required to make a phone call. Nevertheless, our findings indicate that online cancellation processes were not without their share of barriers and complexities, including dark patterns such as *Misdirection*, *Obstruction* and *Forced action*. Given it takes roughly twice as many 'clicks' to cancel, as it does to subscribe, cancelling is more complicated and takes longer. Our findings also show cancelling subscriptions do not align with the seven principles of universal design.

Comparing results across European and US news websites, we find that compared to their European counterparts, US news sites require more clicks to cancel, they ask more information when subscribing, and they are more likely to force users to fill in a mandatory exit survey.

While we believe that upcoming regulatory interventions rightfully focus on preventing problematic practices related to subscriptions, their success depends on effective enforcement. In the meantime, we believe businesses should focus on gaining and retaining users' trust instead of short-term gains.

CHAPTER 5

Conclusions

This chapter concludes the thesis with an overall summary and conclusion with additional thoughts on all projects within. We speak here of the thesis implications and to conclude we end with some final thoughts.

5.1 Thesis Summary

Here we briefly reiterate our research questions and how they were addressed. We also discuss some open questions around each topic.

5.1.1 Chapter Two: Partial PIN Security

The first topic covered in this thesis, explored the area of guessing PINs. We examined potential approaches for making educated guesses of a PIN within a login system that requires selecting a subset of m digits out of a total of n. In doing so, we answered the following questions.

RQ1:1 Can you guess a full PIN quicker by guessing its partial PIN?

Of the four guessing strategies we devised, two were highly effective using a list of possible PINs, while the other two, not using this list, were less efficient. We assessed full PINs with 4 to 6 digits with partial PINs of size 2 to 6 and found that the number of guesses increased with both n and m. Our results suggest moderate success within tens to hundreds of attempts. In short, partial PIN systems are more vulnerable than full PINs, which take longer to guess.

RQ1:2 Is this system of authentication a viable system in terms of usability and security?

Considering that we have observed it is easier to guess a full PIN incrementally via its partial PIN than guessing a full PIN outright, questions the value of the additional cognitive effort required from users. This is especially important when considering the effect on vulnerable users. Partial PINs were introduced for reasons that are no longer applicable, such as preventing a phone operator from knowing your full PIN when phone banking. In light of additional authentication methods such as 2FA, partial PINs do not add any extra security benefits and as such we can say in terms of usability and security this is no longer a viable system of authentication.

RQ1:3 Do partial PINs align with the seven principles of design?

When judging partial PINs through the lens of the seven principles of universal design, we see that they do not align and do not meet with the requirements stated in principle one; equitable use and principle five; tolerance for error. For example, users with memory issues potentially may find it difficult to recall specific digits from a full PIN.

5.1.1.1 Open Questions

An interesting observation in this study, was the fact that the partial PIN system is not widely used across the world. What we would have liked to verify with more certainty, is all countries which do or at one stage did implement the partial PIN scheme. The partial PIN scheme in some locations is known by other names such as the Dutch ING bank, who refer to their partial PIN as a DIBA key meaning direct banking [40]. This may be a reason why it was not easy to locate more examples of partial PIN use.

We would also have liked to find out if the partial PIN scheme has had any impact on banking security. However, banking information was quite difficult to attain, in particular, details regarding accounts being hacked. As a result, obtaining this information was not possible.

Other avenues we would have liked to explore with regards to this area is comparing users recall of full PINs compared to partial PIN inputs. This would involve timing users as they inputted a full PIN versus a few digits from that full PIN. Logging any mistakes made etc. This would be a good way to determine usability.

5.1.1.2 Final Thoughts

Password authentication continues to be prevalent across the Internet, despite more than three decades (2010) of research highlighting its vulnerabilities [62]. Anecdotally it appears that there is a reluctance to let go of the old. This appears to be evident in the case of partial PINs. AIB is the only bank in Ireland (thus far) who have changed their partial PIN system to a full PIN system. Previously when using the AIB banking app you were required to input three digits from a five-digit personal access code. Today you are required to input your full five-digit code (PAC).

5.1.2 Chapter Three: Cookies Banners in Ireland

In this chapter we studied Irish cookie banners in detail using the web crawler OpenWPM and answered the following research questions.

RQ2:1 Do Irish cookie banners adhere to GDPR?

As discussed in Chapter 3, our study's findings align with those from other countries [168,182,205], indicating widespread disregard for GDPR due to the difficulty of policing the Internet. Internet regulation varies by country, causing compliance issues and deterring website designers from adhering to best practices. We discovered many banners did not comply with GDPR, such as assuming compliance by directing users to change their own settings or sending users to a link to explain cookies. This can arise from the fact that GDPR is very difficult to understand, however the language can also be easy to manipulate. We also found evidence of 'invisible banners' where we noted code for banners present in the HTML but the banner itself is not visible, technically the website therefore is not compliant with

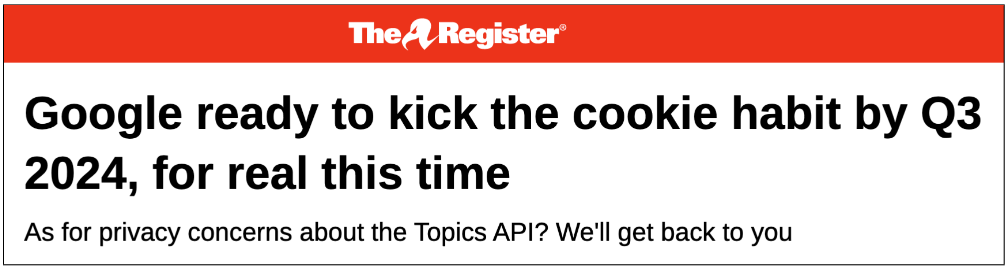
GDPR in this case. Many users are unaware of how cookies affect their privacy and are unlikely to report infringements. Consequently, with minimal repercussions, websites continue to extract as much data as possible for revenue.

RQ2:2 What manipulative practices (dark patterns) and barriers are present (if any) in managing cookies.

We found several dark patterns in Irish banners such as hard to see decline buttons or options for privacy hidden in numerous layers. Cookie banner design were for the most part thin slivers at the bottom of the page, which can be easily missed. We also noted misleading language such as an x on a banner, which often users assume mean decline cookies but is in fact accepting cookies and closing the banner. However, we did note a slight improvement compared to Greece and the UK, for example we discovered less third party cookies and less pre-ticked banner options. This could be in part due to the judgement in the Planet49 case [113], which made pre-ticked options not compliant with GDPR. This case occurred after the Greece and UK study. As we note in Sec. 3.2.3, individual countries in the EU can vary in their regulations according to GDPR, this could have had an impact. Ireland is also the base for the data protection commission for the EU and so this could also be a factor in banners being more compliant. Ireland in fact appears to use less manipulative practices online compared to other European countries. In an EU study on dark patterns online, 16 Irish retail online stores were reviewed and no infringements were found [102]. Our results seem to also reflect this in terms of dark patterns.

RQ2:3 Do Irish cookie banners align with the seven principles of design?

We believe Irish cookie banners fail to align with principle one; equitable use, principle three; simple and intuitive use, principle four; perceptible information, principle five; tolerance for error and principle seven; size and space for approach and use. An example of the last principle for users with Parkinson's disease may find accepting cookies difficult having to click on numerous small buttons in order to navigate layers to find more private options.


The Register

Google ready to kick the cookie habit by Q3 2024, for real this time

As for privacy concerns about the Topics API? We'll get back to you

Figure 5.1: Cynical headline referring to Google's cookie free future [291].

5.1.2.1 Open Questions

Spreading our net more widely by including more countries for comparison using and more sophisticated tools for identifying cookie banners both in style and GDPR compliance would be interesting. A more accurate sentiment analysis tool would be have given more accurate results on language also[1].

With increasing regulations and suspicions of cookies, it seems that they may be slowly falling out of favour. Lakshmi Narayanan Jayakumar [223] highlights that, while the giants of the browser world, such as Google's Chrome and Apple's Safari, are phasing out third-party cookies, new technologies are emerging, such as Privacy Sandbox [90]. These latest technologies aim to serve targeted ads without cookies, although some believe that this will have little effect on tracking by Google and Facebook and have less privacy benefits than expected [141]. The danger in this technology is that it will be already embedded in your browser and therefore you no longer have the choice to opt out. Smaller companies, who do not have access to this technology, may have to resort to more invasive techniques like fingerprinting to compete [223].

Google had intended to block third-party cookies in Chrome in June 2021, but this was pushed back to 2023 and was yet again pushed to summer 2024 [291]. This induced scepticism in the media as to whether this will happen at all (see Fig. 5.1). Google have since (July 2024) decided to give up on their ambition to eliminate cookies. Instead, it will introduce a new prompt allowing users to choose how they wish to be tracked across Google's search products [132].

[1] As we were following the Kampanos's template, we used the same tools.

Firefox is currently (April 2023) developing a feature for its browser that will enable automatic interaction with cookie banners. Users will have the option to activate this feature, which will automatically click ‘reject all’ when a banner appears. It is important to note that this functionality may not be effective for all banners if they lack a ‘reject all’ option [67]. The idea of targeting customers without tracking however, is not new, with a history going back to at least 2010 [138, 150, 292].

The European Commission’s consumer protection office announced a pledge to address ‘cookie fatigue’ in March 2023, by first discussing how the problem can be solved [54]. One idea revolves around users not being repeatedly prompted for consent through a cookie banner whenever they visit a website. Instead, they would express their preference just once as a part of the browser settings, accompanied by comprehensive explanations regarding the reasons for data request, potential benefits, and the business model governing the data processing [53].

5.1.2.2 Final Thoughts

In summary this study brought to mind the quote from Stephen Hawking “The greatest enemy of knowledge is not ignorance, it is the illusion of knowledge”. Giving people the illusion they have some control over their data leads them into a false sense of security. It also provides some insurance for companies if and when their data is used against their users. In short, GDPR is protecting businesses more than users.

5.1.3 Chapter Four: Hard to Cancel Subscriptions

The final project in this thesis analysed the subscribing and cancellation flows to the top ten news sites from the Netherlands, UK, USA and Germany. The goal being to observe how current regulations impact how easy it is to cancel a subscription. This resulted in 67 successful subscriptions. It was possible to cancel online for 94% of the subscriptions.

RQ3:1 What barriers and dark patterns exist which can potentially impact cancelling subscriptions across the UK, Netherlands, Germany and American states Texas and California?

Cancelling our subscriptions involved many steps, almost twice as many as subscribing, which included surveys and numerous advertisements for special offers. Dark patterns were found in most news sites. These came in the form of misleading language and visual deterrents such as buttons changing colours leading users to press the wrong button. Other patterns found were 'confirm shaming' and 'pressured selling' where more expensive subscriptions are highlighted and often is is hard to find the cheaper option. A similarity noted between this study and the previous study on cookie banners was that in order to cancel a subscription, it required clicking through various steps. This is similar to declining cookies in consent banners, where it is necessary to click through different levels. Each country had their own traits in subscribing and cancelling, for example, Germany had subscriptions where you had the option to pay extra for privacy.

RQ3:2 Have regulations new or old, had any impact in cancelling subscriptions online across the countries mentioned above?

Our results show a growing need for clearer regulations that address dark patterns in more detail. There is progress in this area, in that it is much more likely you can cancel online now than previously. For example Germany's strict regulation on cancelling subscriptions did appear to be having an effect on the ease of cancelling online. Regulations in the USA are worded slightly different, requesting websites to allow the user to be able to cancel online. However, simply declaring that it should be possible to cancel online could potentially allow websites to take advantage of the general language. For example, adding many layers of advertising and manipulative and confusing language before the cancel button appears. This was noted throughout the study, despite being able to cancel online for most of our subscriptions the process was not easy. Regulations in Europe are more strict and this is evident in cancelling subscriptions in our European countries.

RQ3:3 Does subscription practices in these tested services, align with the seven principles of design?

We found that cancelling subscriptions does not align with principle one; equitable use, principle three; simple and intuitive use, principle four; perceptible information, principle five; tolerance for error and principle six; low physical effort. An example of principle three; simple and intuitive use was often seen to be ignored when cancelling. We noted it was rarely obvious where to go to find the cancel button and different for all websites. Often users need to search online to find out how to cancel a specific service.

5.1.3.1 Final Thoughts

The subscription business model is quickly expanding with different types of businesses adopting this model, such as car manufacturers (see Fig. 5.2). With BMW for example, you can now subscribe to have heated car seats [297]. This is why I feel it is important to essentially nip these dark patterns in the bud. It is one thing to find it difficult to cancel a monthly subscription that costs under €10 a month and another to find it difficult to leave a subscription of €65 a month. Individually subscriptions may not cost huge amounts of money. But many subscriptions can amount to huge outgoings, especially as it is quite easy to subscribe and then forget to cancel or meet barriers to cancelling. A New York Times opinion piece refers to this as *Background Spending*, "Think of it as automated capitalism. Spending without the hassle of spending. Acquisition without action or thought." [198]. This is especially significant in a cost of living crisis.

5.1.3.2 Open Questions

Much like our cookie crawl, conducting a much bigger crawl of sites would be interesting. Exploring different types of subscriptions, different countries and how they compare. Analysing email responses for subscribing and cancelling would also be another interesting aspect of subscribing. Additionally, UX design, location of cancelling information and how easy it is to find this information etc.

5.2 Thesis Implications

This thesis highlights a broad lack of attention to universal design in designing security measures, privacy online and shopping online. It also highlights inconsistencies in regulations online. For example, our first project highlighted usability issues with regards to partial PINs and what this can mean for vulnerable users. As numerous physical banks close across Ireland, many feel pressured to shift to

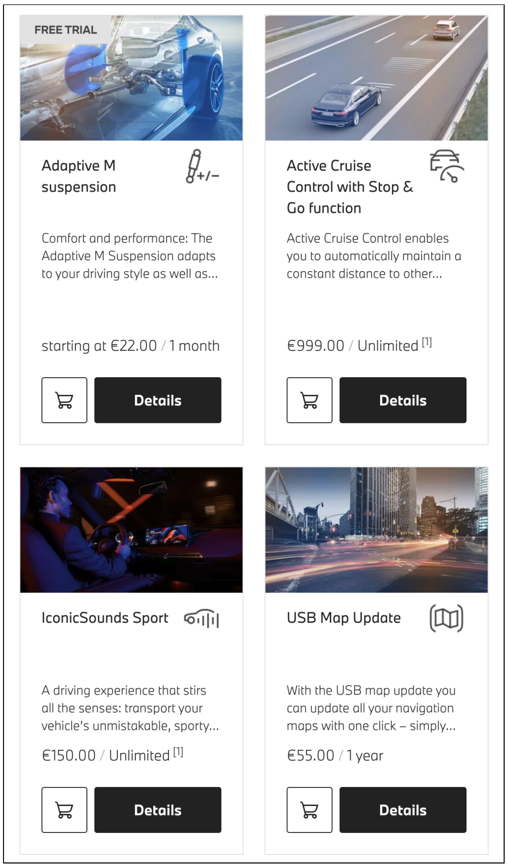


Figure 5.2: Screenshot of BMW's Irish digital store, with subscriptions for sporty car sounds and cruise control [297].

online banking [299]. Making banking online as user friendly as possible is important as services rapidly transition from analogue to digital platforms.

Another theme throughout this thesis is deception and illusion. For partial PINs there is an illusion of security. For cookie banners; an illusion of privacy and for subscriptions, a whole host of deceptions that can lead you to avoid cancelling subscriptions. In the world as it is today with the cost of living crisis and uncertainty, unaccounted for subscriptions accumulating in the background can cause undue stress [164]. Barriers to cancelling subscriptions not only affects vulnerable users, but is a general cause of annoyance for many people. This was noted when the article we wrote for RTÉ Brainstorm on the topic, was one of the most read articles for several days[2]. Likewise with the unknown amount of data that we unknowingly reveal online, can lead to other issues such as being targeted for scams. Although cookies alone do not present security risks, cyber criminals can exploit them to impersonate users, collect financial data, access accounts, or steal passwords stored in the browser [118]. This can lead to the spread of malware and trick users into visiting harmful websites. Younger users, view sharing personal information online as a standard part of the modern economy and tend to place less emphasis on giving consent when their online activities are being tracked [228]. Thus younger users potentially may be more at risk from cyber-crime.

Our cookie chapter and subscription chapter both discuss regulations and our research shows that clear and strict regulations can be effective. As we can see with Germany and their very clear regulation on cancelling online. GDPR on the other hand has vague guidelines which can easily be misinterpreted either accidentally or on purpose to harvest huge amounts of data from users online. As we note in Sec. 1.4.4, we submitted our findings to the Data Protection Agency in Ireland, in the hopes that our work can highlight the many discrepancies in Irish cookie banners in relation to GDPR. This work reveals how regulations can be worded to be more effective leaving no room for interpretation. This work also highlights the need for consistent regulations. As we note some countries in the EU have slightly different variations on GDPR. For example, GDPR surrounding age consent for consent managed by parental figures is not consistent in all countries [257]. This can have implications for how much data children reveal online.

This body of work highlights the value of interdisciplinary research on the topic of user experience and usable security. Recognising and understanding the individual behind the computer is immensely important. This necessitates people who understand human interaction with technology and its psychological effects.

Research on vulnerable users in relation to the topics we discuss seems to receive less focus. We bring attention to this gap by reviewing related work in all areas. This thesis contributes to this gap, in providing a unique insight into nuanced

[2] RTÉ Brainstorm article: https://www.rte.ie/brainstorm/2024/0509/1448035-dark-patterns-cancel-online-subscriptions/

areas in operating as a user online. It highlights tangible proof of how widely the principles of universal design are widely ignored. As such vulnerable cohorts need to be included in the design and research of user experience (UX). In designing universally accessible security measures, privacy banners or developing regulations around design and combating dark patterns, this thesis provides some valuable insights.

5.3 Thesis Final Thoughts

These projects ignited a personal interest in philosophy and psychology, particularly in how they can be subtly applied to manipulate people online. I became especially intrigued by how individuals with disabilities might be uniquely impacted. An additional area of personal interest is how to effectively oversee the Internet and whether it is advisable to do so. How do you ensure GDPR compliance? How do you implement regulations for dark patterns online and ensure websites follow these? In research, one method of large scale analysis of the Internet is via web crawlers, this is how we examined Irish cookie banners in Chapter 3. This method in future however, may not be possible, with Google developing a *Web Environment Integrity* application programming interface (API). This proposal, in a nutshell, effectively means a third party will need to authenticate if you are a real person or a bot [278]. It will also prevent people using ad-blockers and having control on what data is being shared. This proposal has been widely criticised, with many believing this to be an "all-out attack on the free Internet" [304].

For GDPR violations, there are definitive privacy risks with too much personal data being freely available online. Whereas dark patterns are almost a judgement call, many papers have different interpretations on dark patterns, describing them as "tricks" or "misleading", others describe them as "coercing, steering, or deceiving" [207]. Some businesses would argue this is how you sell products online and they are simply trying to earn a living, which is mentioned in Sec. 1.3.2. However, there is a risk also I believe, in over policing the Internet, which can bleed quite quickly into censorship. If too much control is given to bodies in power to make decisions on what is 'allowed' or not online.

If anything else, it does make for an interesting philosophical debate.

Moving forward, I am curious as to how an Internet free of dark patterns would look like, if indeed this is possible. Or what a completely universal Internet would look like, where no one is at a disadvantage, regardless of age or disability. The common thread in this thesis is universal design and as such I would like to end the thesis with a thought and a quote on the topic. O Neil ends his study on universal and inclusive design, by highlighting that when the civil rights of marginalised individuals are respected, new opportunities for inclusion arise [240].

> *"When UX (user experience design) doesn't consider ALL users, shouldn't it be known as "SOME User Experience" or... SUX?"*
>
> - Billy Gregory, Senior Accessibility Engineer [281].

APPENDIX A

Further Partial PIN Analysis

In this appendix is a detailed analysis on the probability of guessing partial PINs with a subset size ${}^nC_n$ and ${}^nC_1$ for the Max and Random strategy. We focus on these particular subset sizes as they both appeared to perform similarly when being guessed. We discuss their equivalence and mathematically analyse both methods for these subset sizes.

A.1 Equivalence of Strategies for ${}^nC_n$ and ${}^nC_1$ Problems

In the process of guessing different sized PIN and subsets, we observed in the cases where we were guessing a full PIN ${}^nC_n$ and a full PIN with a partial PIN of 1 ${}^nC_1$, there were similarities in the how fast these PINs were guesses and visually this was seen in the graphs. This prompted us to look into these cases in more detail. In these cases analysis is easier.

Note, that in the ${}^nC_n$ (full PINs, with no partial PIN) case all PINs start as equally likely. After each guess, we either guess correctly (and stop as $n = m$, when full PIN is guessed) or we guess incorrectly and eliminate one possible PIN from the list. This in short means for a full PIN we either guess it first time and there is no further guessing needed or we guess incorrectly and this incorrect guess is eliminated from the PIN list, before guessing our next guess.

Thus, the Max and Educated Guess strategies are presented with a list of equally likely options, and so choose effectively randomly from the list. In other words for the first guess they are on equal footing and means that in the ${}^{n}C_{n}$ case, Max and Educated Guess perform equally well.

Similarly, in the ${}^{n}C_{1}$ case, we effectively have independent PIN lists for each position, as a guess about one position tells us nothing about the other positions. Each guess for each position is either correct or removes a digit, and either way we are left with a list of equally likely possibilities for this position. So, when Max or Educated Guess come to make choices, they will again behave in the same way. In fact, the Round Robin strategy will also perform in the same way, as even though it does not use the PIN list, in the ${}^{n}C_{1}$ case, it will not repeat any guesses for a position, effectively choosing at random from the remaining digits because the PIN was assigned randomly.

A.1.1 Performance of Max and Random Strategies for ${}^{n}C_{n}$ and ${}^{n}C_{1}$ Problems

As we noted, in the case where $m = n$, analysis of the guessing problem is greatly simplified. In this case, each guess either results in the identification of the PIN or the elimination of a single PIN from the PIN list. This makes it possible to calculate the distribution of the number of guesses explicitly for both the Max and Random strategies, using standard probabilistic techniques in Eq. A.1 and Eq. A.6. Via our observation in Sec. A.1, we note the analysis also covers the Educated Guess strategy.

Similarly, in the case where $m = 1$, we are essentially faced with guessing a sequence of independent digits, where guessing one digit does not influence what we know about the others. Note that after k guesses, the number of times we will have guessed each digit will follow a multinomial distribution. By using this observation, and the results for the ${}^{1}C_{1}$ problem, we obtain explicit expressions for the distribution of guesses when using Max and Random strategies for the ${}^{n}C_{1}$ problems, see Eq. A.3 and Eq. A.8. Via our observation in Sec. A.1, we see that the analysis will also cover the Educated Guess and Round Robin strategies.

We note that these expressions can become unwieldy when applied for larger numbers of guesses.

Using these distributions, we can also calculate the expected number of guesses required. This requires an infinite sum, but we show how to bound the infinite sum using a finite number of terms (see Eq. A.11). As we will see, Fig. A.1 and Fig. A.2 graphically show how the empirical simulations results generated by the code mentioned in Sec. 2.3 closely match the theoretical analysis results conducted in Sec. A.2 and Sec A.3 for ${}^{n}C_n$ and ${}^{n}C_1$ problems using the Random and Max strategies. The code carries out 500 random trials to guess a PIN selected at random. In each case, $n = 1 \ldots 6$, we show the Cumulative Distribution Function (CDF) for the number of guesses required to recover the PIN. While we will show the details of these results in the next section, we can see that the two methods of estimating the distribution of number of guesses concur. We also see that, as expected, the Max strategy also tends to use fewer guesses than the Random strategy. This gives us confidence that, at least in these simplified cases, our analysis and code are operating as expected.

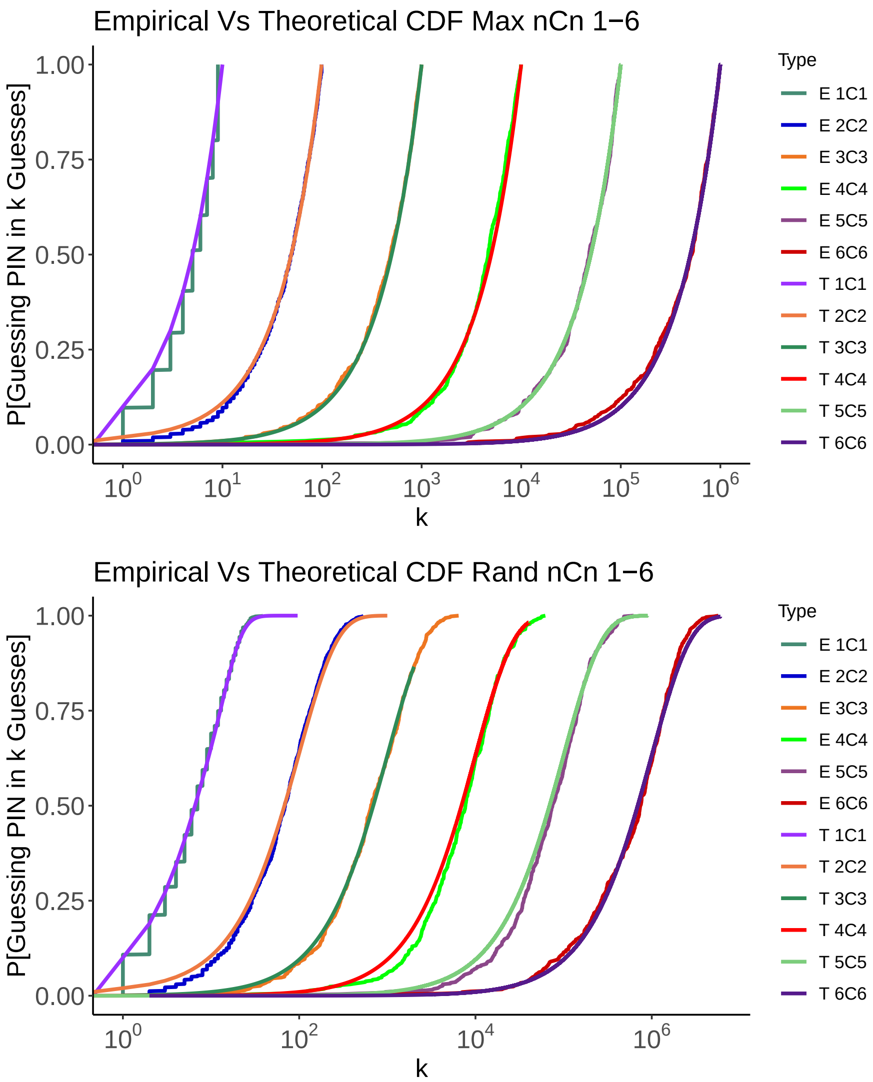


Figure A.1: Simulated and analytic performance of the Max (above) and Random (below) strategies for ${}^{n}C_{n}$. Each graph shows the CDF for the number of guesses (k) required to recover the PIN.

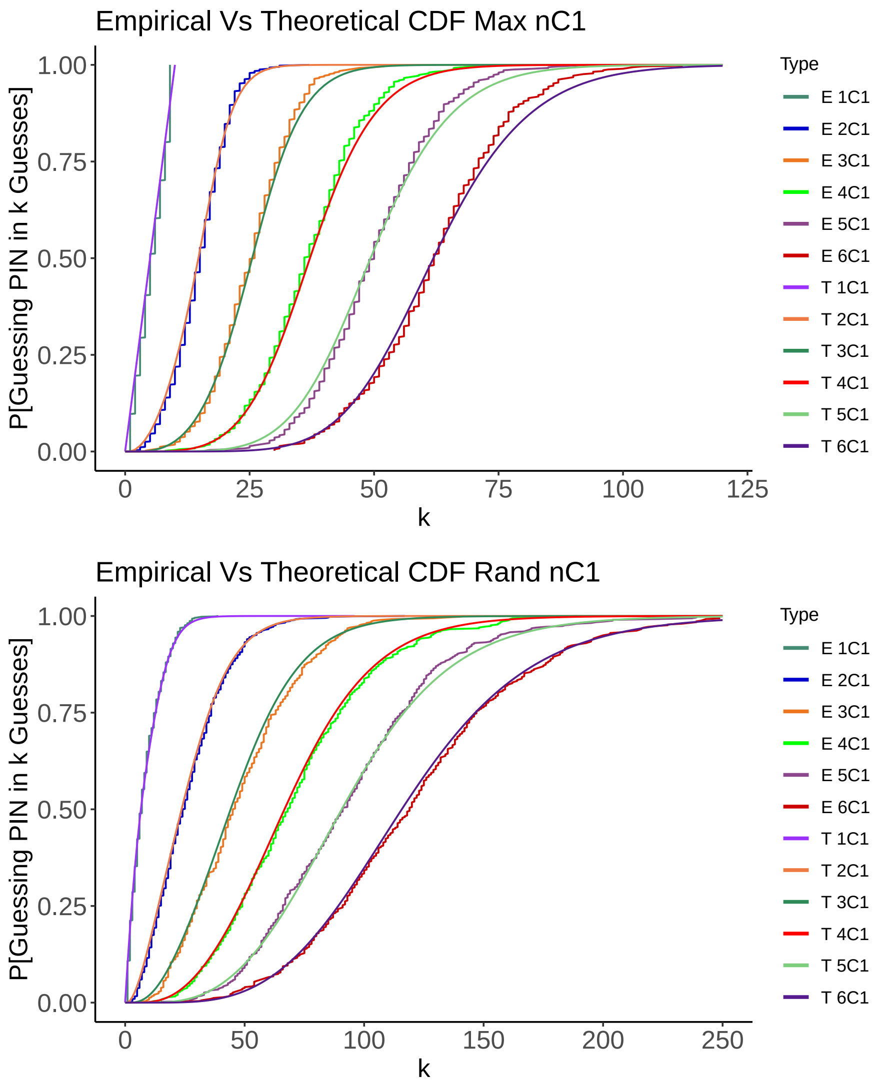


Figure A.2: Simulated and analytic performance of the Max (top) and Random (bottom) strategies for ${}^nC_1$. Each graph shows the CDF for the number of guesses (k) required to recover the PIN.

A.2 Mathematical derivation of Max Strategy

Here we show how to derive the distribution of number of guesses using the Max strategy for ${}^nC_n$ and ${}^nC_1$ problems.

A.2.1 Max Strategy for ${}^nC_n$ Problems

The expression for this problem is relatively easy to derive, but will be useful for studying the ${}^nC_1$ problem. Suppose we are following the Max strategy, and we are guessing a ${}^nC_n$ problem. Each guess involves all n digits, and so tells us if one PIN is on the list. As all PINs are equally probable, we essentially eliminate one possibility among 10^n each time. Thus, the probability that we are correct within the first k guesses is simply

$$\mathbb{P}[\text{correct in first } k \text{ guesses}] = \min\left(\frac{k}{10^n}, 1\right). \tag{A.1}$$

Or, if G is the number of guesses required,

$$\mathbb{P}[G > k] = 1 - \min\left(\frac{k}{10^n}, 1\right) = \max\left(1 - \frac{k}{10^n}, 0\right).$$

and so, by the Tail Sum Formula, the expected number of guesses is

$$\mathbb{E}[G] = \sum_{k=0}^{\infty} \mathbb{P}[G > k] = \sum_{k=0}^{\infty} \max\left(1 - \frac{k}{10^n}, 0\right) = \sum_{k=0}^{10^n} 1 - \frac{k}{10^n} = \frac{10^n + 1}{2}. \tag{A.2}$$

We note that for an ${}^nC_n$ problem, recovering the full PIN is essentially the same as achieving a successful guess.

A.2.2 Max Strategy for ${}^nC_1$ Problems

Now, suppose that we are using the Max strategy on a ${}^nC_1$ problem, so each guess tells us about just one digit, and we can maintain independent lists for each digit. First consider the case where we have made k guesses in total, with k_i guesses made for each digit i.

$$\mathbb{P}[G > k | k_i \text{ guesses of digit } i] = 1 - \mathbb{P}[\text{all digits correct} | k_i \text{ guesses of digit } i],$$

but, as the guesses for digit i are independent

$$\mathbb{P}[G > k | k_i \text{ guesses of digit } i] = 1 - \prod_{i=1}^{n} \mathbb{P}[\text{digit } i \text{ correct} | k_i \text{guesses of digit } i].$$

Now, we can treat each digit as a ${}^1C_1$ problem and, using Eq. A.1 with $n = 1$, we get

$$\mathbb{P}[G > k | k_i \text{ guesses of digit } i] = 1 - \prod_{i=1}^{n} \min\left(\frac{k_i}{10}, 1\right).$$

Now, given that we have made k guesses in total, if the digits guessed were randomly chosen, we can also find the probability that we have made k_i guesses for digit i. Naturally $k_1 + k_2 + \ldots + k_n = k$. Using the multinomial distribution, the probability of this is

$$\binom{k}{k_1\, k_2\, \ldots\, k_n} \frac{1}{n^{k_1}} \cdots \frac{1}{n^{k_n}} = \binom{k}{k_1\, k_2\, \ldots\, k_n} \frac{1}{n^k}.$$

Then, by the law of total probability, we can find $\mathbb{P}[G > k]$ as

$$\sum_{k_1 + \ldots + k_n = k} \mathbb{P}[G > k | k_i \text{ guesses for digit } i] \binom{k}{k_1\, k_2\, \ldots\, k_n} \frac{1}{n^k}.$$

So, by the Law of Total Probability, we find,

$$\mathbb{P}[G > k] = \sum_{k_1 + \ldots + k_n = k} \left(1 - \prod_{i=1}^{n} \min\left(\frac{k_i}{10}, 1\right)\right) \binom{k}{k_1\, k_2\, \ldots\, k_n} \frac{1}{n^k}.$$

or, slightly simplifying using the multinomial theorem,

$$\mathbb{P}[G > k] = 1 - \frac{1}{n^k} \sum_{k_1 + \ldots + k_n = k} \binom{k}{k_1\, k_2\, \ldots\, k_n} \prod_{i=1}^{n} \min\left(\frac{k_i}{10}, 1\right). \tag{A.3}$$

We may then find $\mathbb{E}[G]$ by summing this over k.

$$\mathbb{E}[G] = \sum_{k=0}^{\infty} \mathbb{P}[G > k] = \sum_{k=0}^{\infty} \left(1 - \frac{1}{n^k} \sum_{k_1 + \ldots + k_n = k} \binom{k}{k_1\, k_2\, \ldots\, k_n} \prod_{i=1}^{n} \min\left(\frac{k_i}{10}, 1\right)\right). \tag{A.4}$$

We briefly note that the inner sum is a effectively a sum over compositions of n, as if any $k_i = 0$, then the whole term is zero. Also note that the terms are symmetric in the k_i, and so this sum over compositions could be written as a sum over partitions, by accounting for how many compositions correspond to each partition.

We note that a similar calculation can be used to find the distribution of times to first successful guess. First, observe that the chance of the first success happening in k guesses is the complement of there being no successes in k guesses. Then note that that is independent for each digit being guessed, and so a product and the conditioning on k_i guess for digit i can be used.

A.3 Mathematical derivation for Random Strategy

Here we derive the distribution of number of guesses using the Random strategy for ${}^nC_n$ and ${}^nC_1$ problems, using a similar method to that used for the Max strategy. While we are focused on the number of guesses to recover the full PIN, we note that for the random strategy for an ${}^nC_m$ problem, the distribution of the number of guesses before the first success is particularly simple, as each guess is effectively guessing an m digit number using no state, so the distribution will be geometric.

A.3.1 Random Strategy for ${}^nC_n$Problems

Suppose we are looking at an ${}^nC_n$ problem, and as we use the Random strategy each guess is uniformly random, ignoring our previous choices. We will stop guessing if we either choose the correct pin or we choose every incorrect PIN. After guess k, the chance that we have never chosen the correct PIN is

$$\left(1 - \frac{1}{10^n}\right)^k.$$

If $k < 10^n - 1$, then the chance of having selected all incorrect PINs is zero.

Thus, if $k < 10^n - 1$, and again G is the random variable for the number of guesses required to guess correctly, we have

$$\mathbb{P}[G > k] = \left(1 - \frac{1}{10^n}\right)^k \tag{A.5}$$

If $k \geq 10^n - 1$, then there is a possibility that we have guessed all the incorrect numbers, and we need to make a correction:

$$\mathbb{P}[G > k] = \left(1 - \frac{1}{10^n}\right)^k \left(1 - \frac{\left\{ {k \atop 10^n - 1} \right\} (10^n - 1)!}{(10^n - 1)^k}\right), \tag{A.6}$$

where the numerator of the second term uses Stirling numbers of the second kind to count partitions of k into non-empty sets corresponding to each of the $10^n - 1$ incorrect digits, and the denominator is the number of ways of assigning k choices to *any* subset of the $10^n - 1$ incorrect possibilities. Note, in both cases we have

$$\mathbb{P}[G > k] \leq \left(1 - \frac{1}{10^n}\right)^k.$$

Now, we can calculate the expected number of guesses and also upper bound it.

$$\mathbb{E}[G] = \sum_{k=1}^{\infty} \mathbb{P}[G \geq k] = \sum_{k=0}^{\infty} \mathbb{P}[G > k] \leq \sum_{k=0}^{\infty} \left(1 - \frac{1}{10^n}\right)^k = 10^n. \tag{A.7}$$

A.3.2 Random Strategy for ${}^nC_1$ Problems

Now, suppose we are looking at ${}^nC_1$ with the Random strategy. On guess k we will stop guessing if we have correctly guessed each digit, or we have eliminated all digits except the correct one. Again, let's condition on having made k_i guesses for digit i and naturally $k_1 + k_2 + \ldots + k_n = k$. As we saw for the Max strategy case, given there have been k_i guessed for digit i, the probability what we are still guessing is the probability that not all digits are known,

$$1 - \mathbb{P}[\text{all digits known}] = 1 - \prod_{i=1}^{n} \mathbb{P}[\text{digit } i \text{ known}] = 1 - \prod_{i=1}^{n} 1 - \mathbb{P}[G_i > k_i],$$

where G_i is the number of guesses taken to guess digit i. By treating each digit as a ${}^1C_1$ problem, we can use Eq. A.6 with $n = 1$ we can get $\mathbb{P}[G_i > k_i]$. We can then sum this using the law of total probability, to get

$$\mathbb{P}[G > k] = \sum_{k_1+\ldots+k_n=k} \left(1 - \prod_{i=1}^{n} 1 - \mathbb{P}[G_i > k_i]\right) \binom{k}{k_1\, k_2\, \ldots\, k_n} \frac{1}{n^k}.$$

Or, tidying using the multinomial theorem,

$$\mathbb{P}[G > k] = 1 - \frac{1}{n^k} \sum_{k_1+\ldots+k_n=k} \binom{k}{k_1\, k_2\, \ldots\, k_n} \prod_{i=1}^{n} 1 - \mathbb{P}[G_i > k_i]. \tag{A.8}$$

Again, we can use the Tail Sum Formula to get

$$\mathbb{E}[G] = \sum_{k=0}^{\infty} \left(1 - \frac{1}{n^k} \sum_{k_1+\ldots+k_n=k} \binom{k}{k_1\, k_2\, \ldots\, k_n} \prod_{i=1}^{n} 1 - \mathbb{P}[G_i > k_i]\right). \tag{A.9}$$

Using the same observations as above, the inner sum could be written as a sum over partitions rather than compositions.

A.4 Bounding the Expectation

In the cases of the Max and Random ${}^nC_n$ and ${}^nC_1$ problems we have found $\mathbb{P}[G > k]$, and then used the Tail Sum Formula to find $\mathbb{E}[G]$ via an infinite sum. For our guessing strategies, there is a useful way to evaluate only a finite number of terms while still bounding $\mathbb{E}[G]$ above and below.

First, consider a modified guessing process, where we choose a constant h and make up to h guesses using the original strategy. If we are successful on any guess, we stop guessing. However, if we reach guess h we stop regardless of if we are successful on guess h. Let H_h be the random variable representing the number of steps this process takes to stop. Clearly, $H_h \leq G$ for any set of guesses, so $\mathbb{E}[H_h] \leq \mathbb{E}[G]$. We also note that if $k < h$ then $\mathbb{P}[H_h > k] = \mathbb{P}[G > k]$ and $\mathbb{P}[H_h > k] = 0$ for $k \geq h$.

This means that we can find

$$\mathbb{E}[H_h] = \sum_{k=0}^{h-1} \mathbb{P}[G > k], \tag{A.10}$$

and use this as a lower bound for $\mathbb{E}[G]$ for the original strategy. We also note that the probability that this process failed to make the correct guess is just $\mathbb{P}[G > h]$.

Next, consider a second modified guessing process which takes up to h guesses using the strategy, but then forgets everything that it has learned if it has not found the correct PIN (say, by restoring all possibilities to the PIN list). This forgetting happens after every block of h guesses. Let F_h be the number of steps required before modified this process finds the correct PIN. Compared to any reasonable strategy, this modified process should be less efficient than the unmodified strategy, so $\mathbb{E}[G] \leq \mathbb{E}[F_h]$. Under the assumption that success in each block of h guesses is independent, we can use the law of total expectation to write

$$\begin{aligned}
&\mathbb{E}[F_h] \\
&= \sum_{k=1}^{\infty} \mathbb{E}[\#\text{guesses}|\text{success in } k^{\text{th}} \text{ block }] \times \mathbb{P}[\text{successful in } k^{\text{th}} \text{ block}], \\
&= \sum_{k=1}^{\infty} ((k-1)h + \mathbb{E}[\#\text{guesses}|\text{successful in} \leq h \text{ guesses}]) \times \mathbb{P}[G > h]^{k-1}(1 - \mathbb{P}[G > h]), \\
&= h\frac{\mathbb{P}[G > h]}{1 - \mathbb{P}[G > h]} + \mathbb{E}[\#\text{guesses}|\text{successful in} \leq h \text{ guesses}].
\end{aligned}$$

However, observe that

$$\mathbb{E}[\#\text{guesses}|\text{successful in} \leq h \text{ guesses}] = \frac{\sum_{i=0}^{h} \mathbb{P}[G = i]i}{1 - \mathbb{P}[G > h]},$$

and the sum in the numerator is bounded above by $\mathbb{E}[H_h]$. So using $\mathbb{E}[H_h] \leq \mathbb{E}[G] \leq \mathbb{E}[F_h]$ and Eq. A.10 we get convenient bounds:

$$\sum_{k=0}^{h-1} \mathbb{P}[G > k] \leq \mathbb{E}[G] \leq \frac{1}{1 - \mathbb{P}[G > h]} \left(h\mathbb{P}[G > h] + \sum_{k=0}^{h-1} \mathbb{P}[G > k] \right). \tag{A.11}$$

As the bounds are all in terms of quantities that we will calculate when evaluating the Tail Sum for $\mathbb{E}[G]$, they provide useful guidance when truncating the infinite sum when evaluating the sum in practice. This can be particularly useful for the sums in Eq. A.4 and Eq. A.9, which involve summing over increasingly large compositions/partitions. An example of these bounds is shown in Fig. A.3 for calculating the mean of the Max ${}^5C_1$ problem. We see that the bound is quite tight after approximately 70 terms.

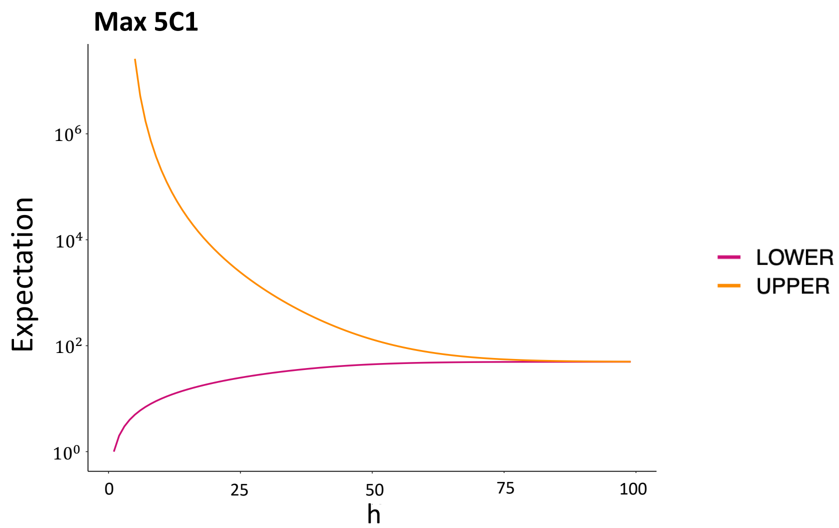


Figure A.3: Bounding the expectation number of guesses for Max ${}^5C_1$, where h is the estimated number of guesses.

APPENDIX B

Additional Partial PIN Results

B.1 Results for Different Problem Sizes

B.1.1 $n = 1$ Digits

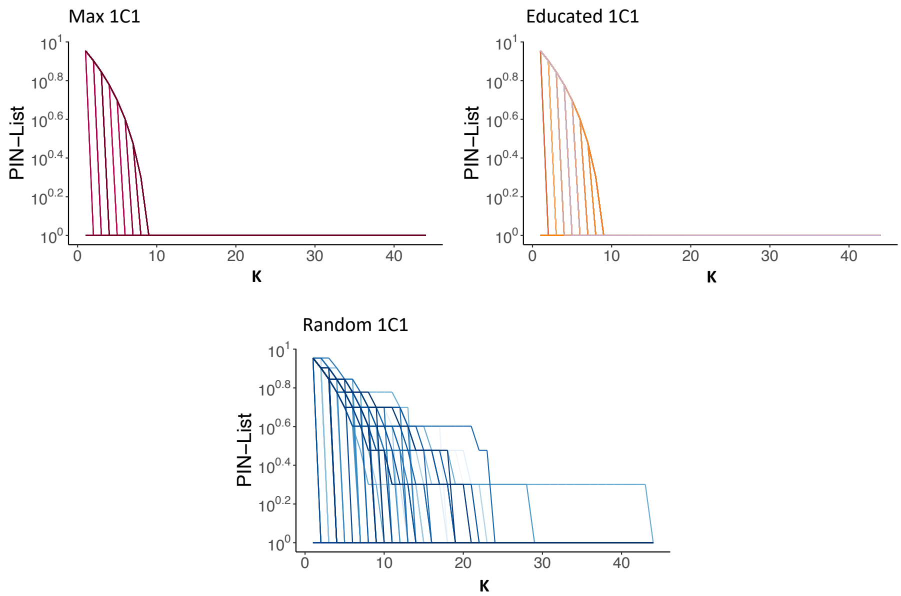


Figure B.1: Number of remaining entries (log scale) in PIN list after each guess k for guessing $m = 1$ digits from $n = 1$. 100 runs of each strategy.

B.1.2 $n = 2$ Digits

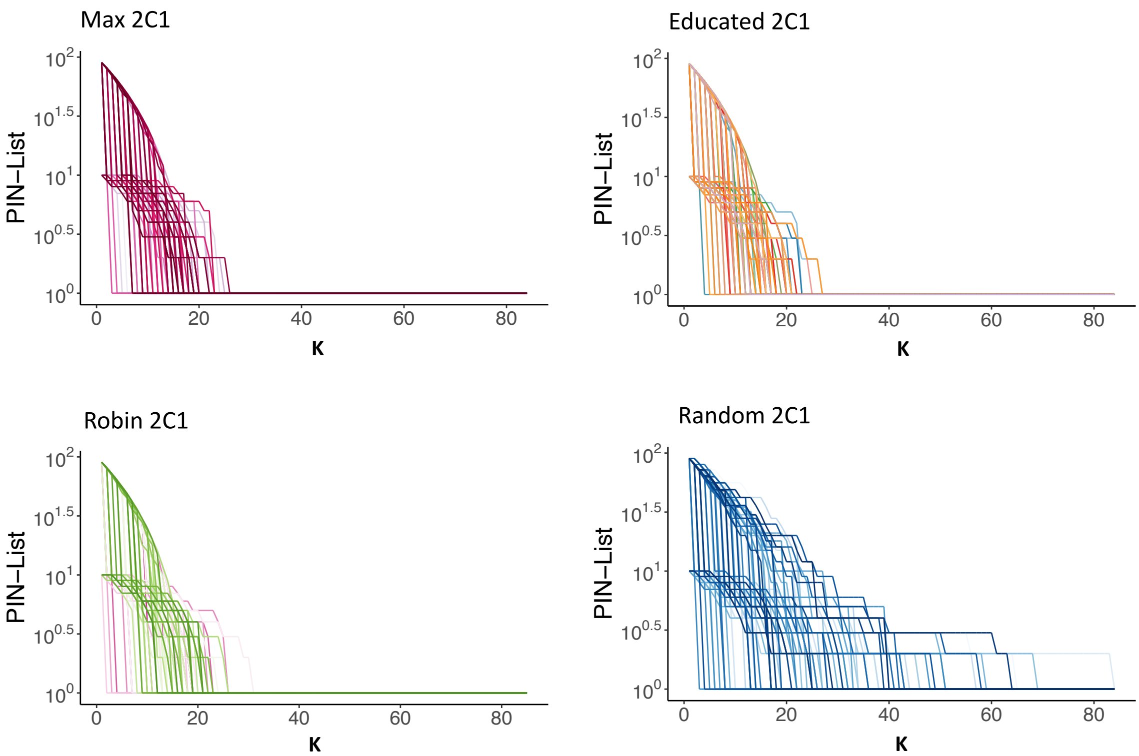


Figure B.2: Number of remaining entries (log scale) in PIN list after each guess k for guessing $m = 1$ digits from $n = 2$. 100 runs of each strategy.

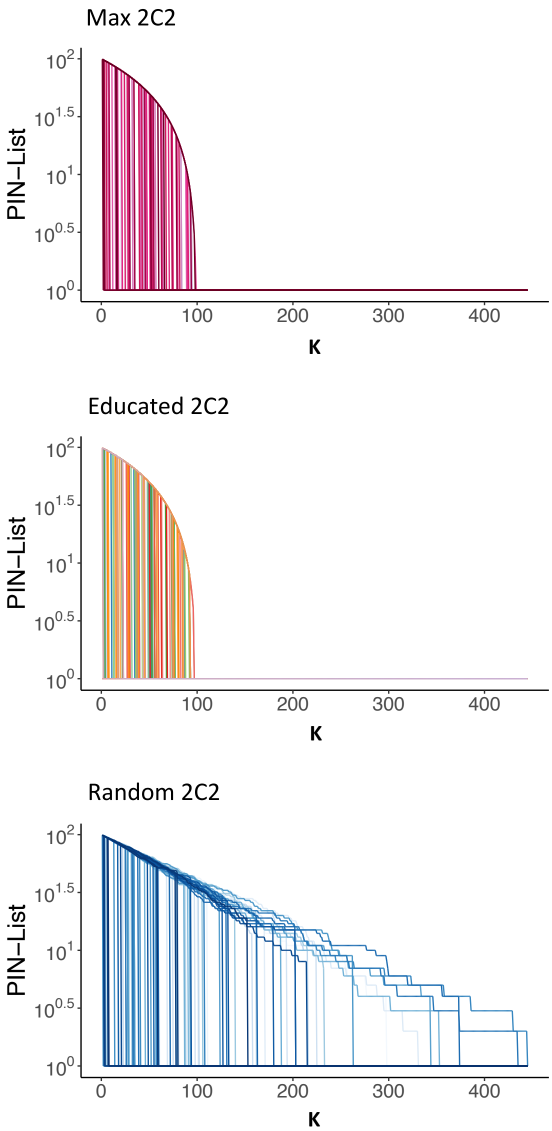


Figure B.3: Number of remaining entries (log scale) in PIN list after each guess k for guessing $m = 2$ digits from $n = 2$. 100 runs of each strategy.

B.1.3 $n = 3$ Digits

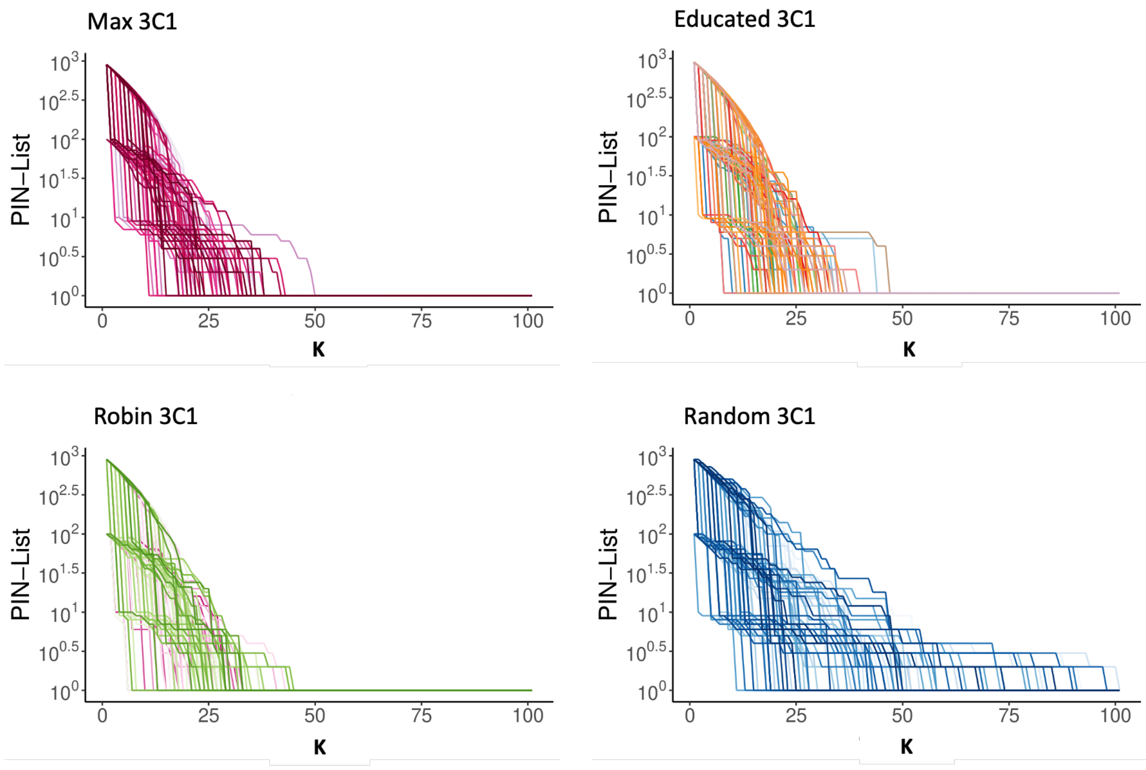


Figure B.4: Number of remaining entries (log scale) in PIN list after each guess k for guessing $m = 1$ digits from $n = 3$. 100 runs of each strategy.

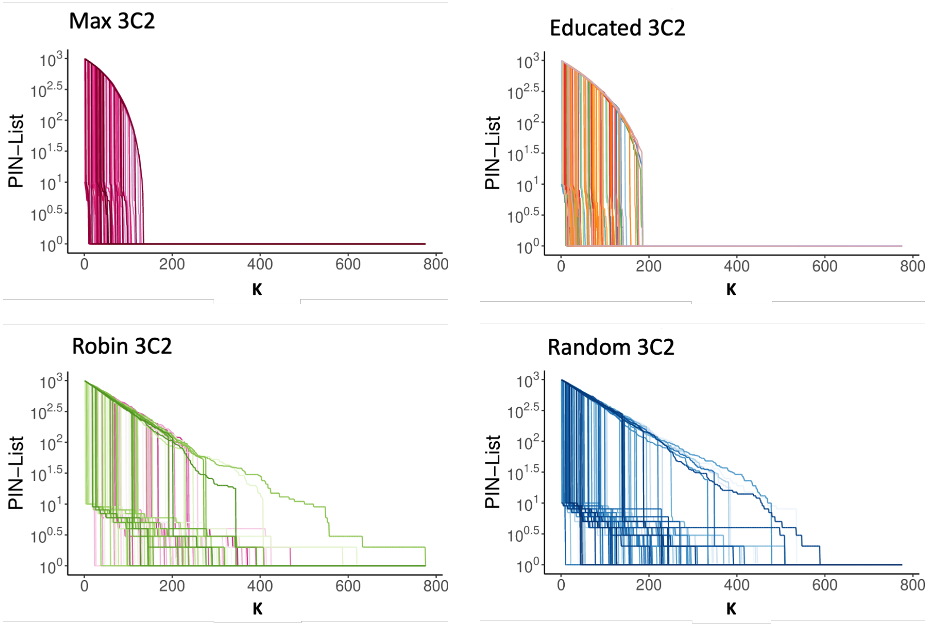


Figure B.5: Number of remaining entries (log scale) in PIN list after each guess k for guessing $m = 2$ digits from $n = 3$. 100 runs of each strategy.

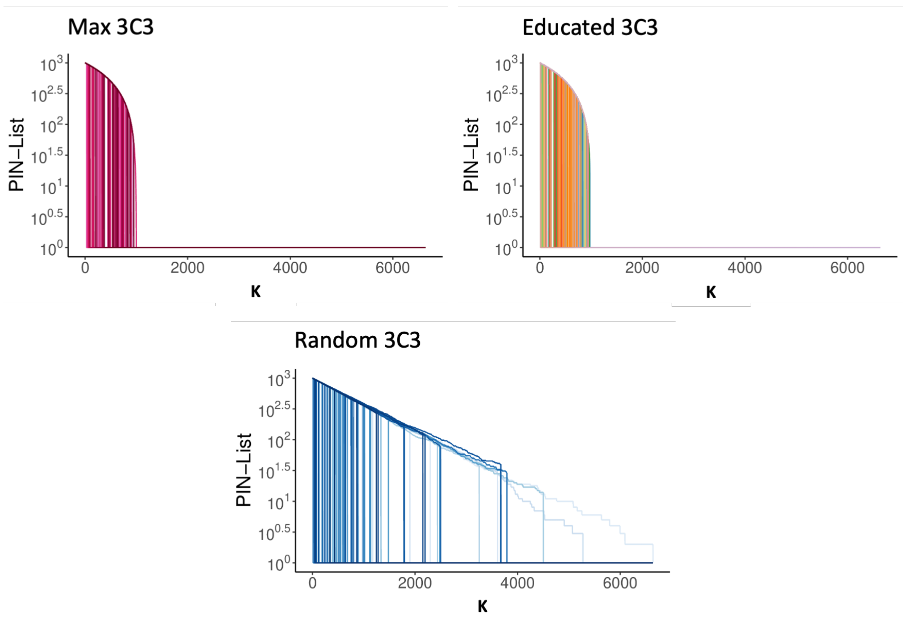


Figure B.6: Number of remaining entries (log scale) in PIN list after each guess $k$for guessing $m = 3$ digits from $n = 3$. 100 runs of each strategy

B.1.4 $n = 4$ Digits

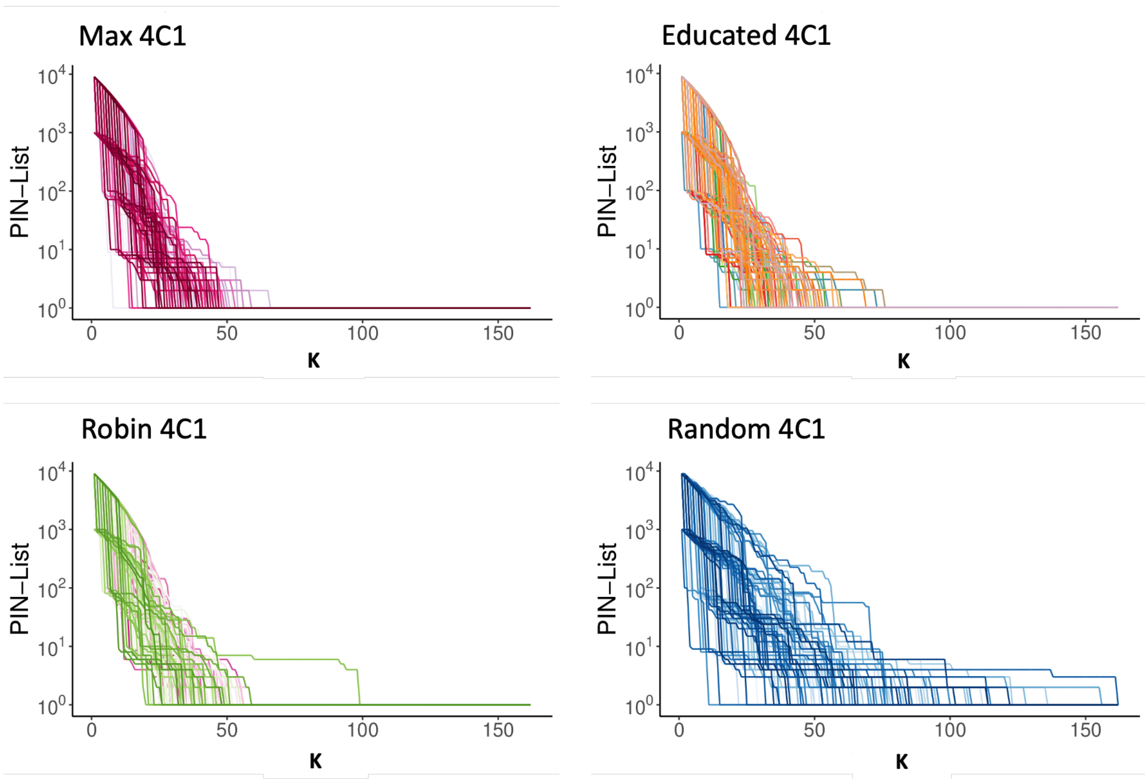


Figure B.7: Number of remaining entries (log scale) in PIN list after each guess k for guessing $m = 1$ digits from $n = 4$. 100 runs of each strategy.

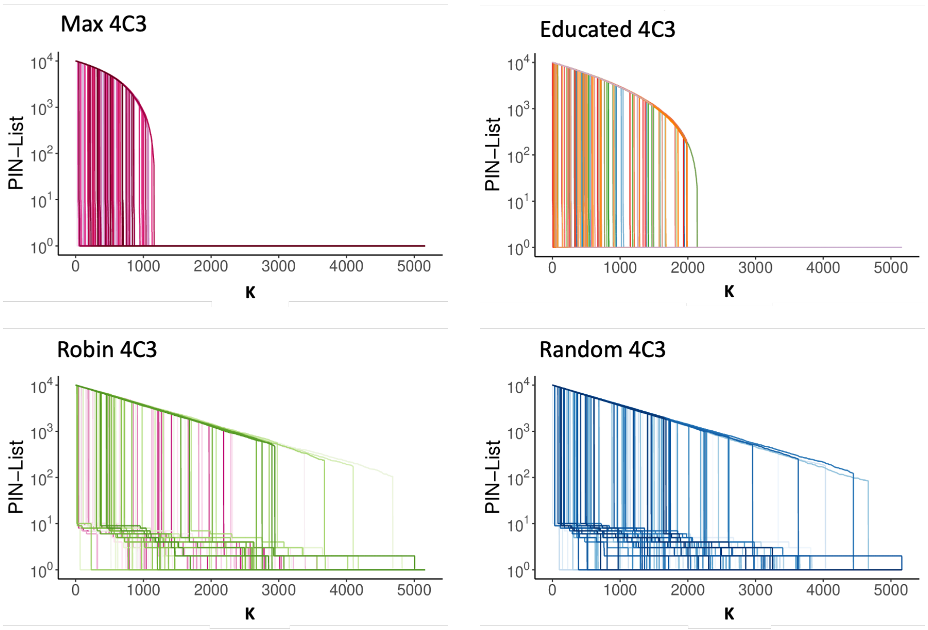


Figure B.8: Number of remaining entries (log scale) in PIN list after each guess k for guessing $m = 3$ digits from $n = 4$. 100 runs of strategy.

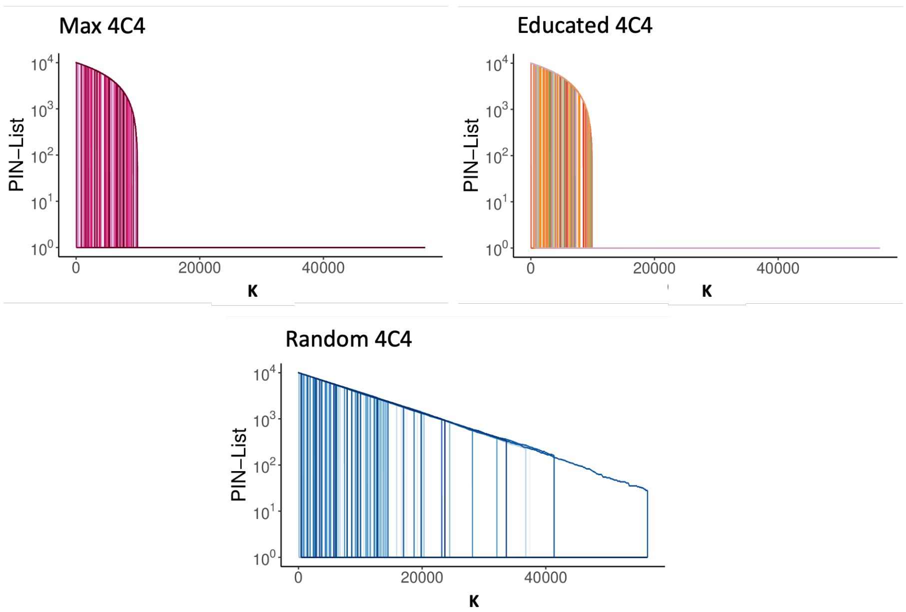


Figure B.9: Number of remaining entries (log scale) in PIN list after each guess k for guessing $m = 4$ digits from $n = 4$. 100 runs of each strategy.

B.1.5 $n = 6$ Digits

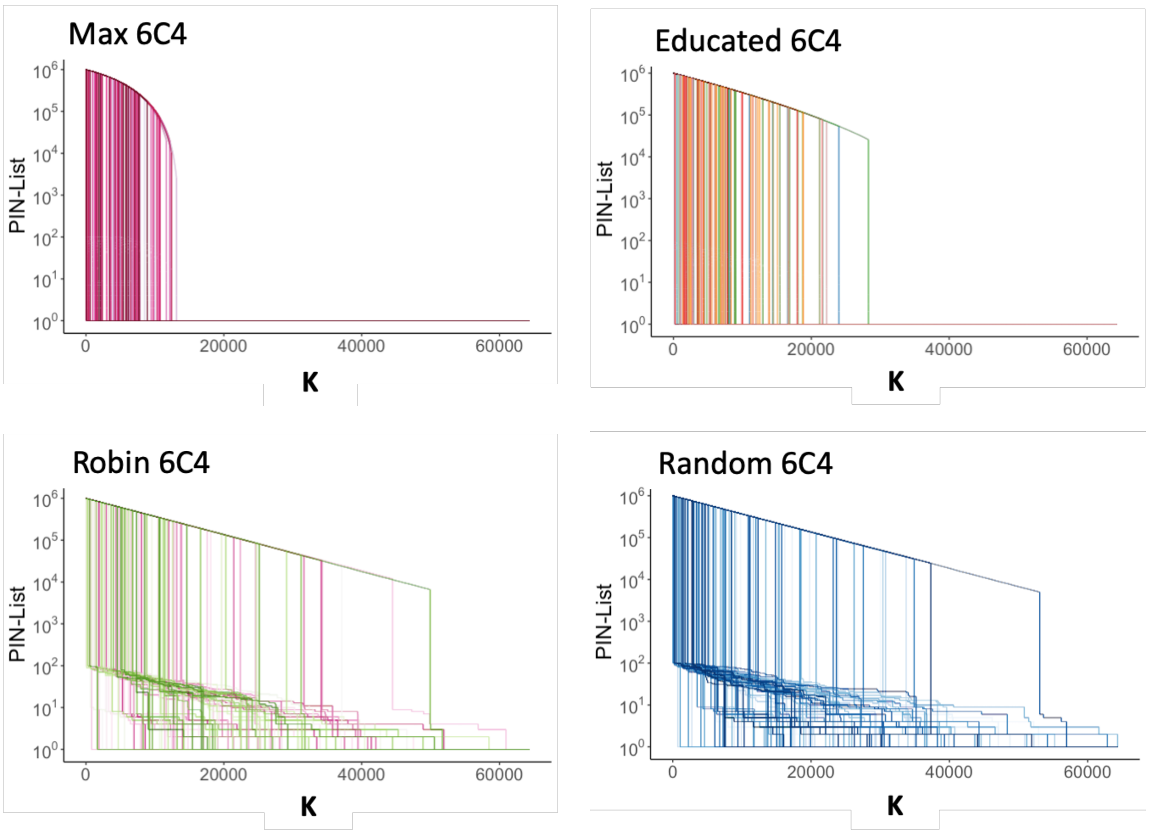


Figure B.10: Number of remaining entries (log scale) in PIN list after each guess k for guessing $m = 4$ digits from $n = 6$. 100 runs of each strategy.

B.2 Empirical CDF Results for all Strategies

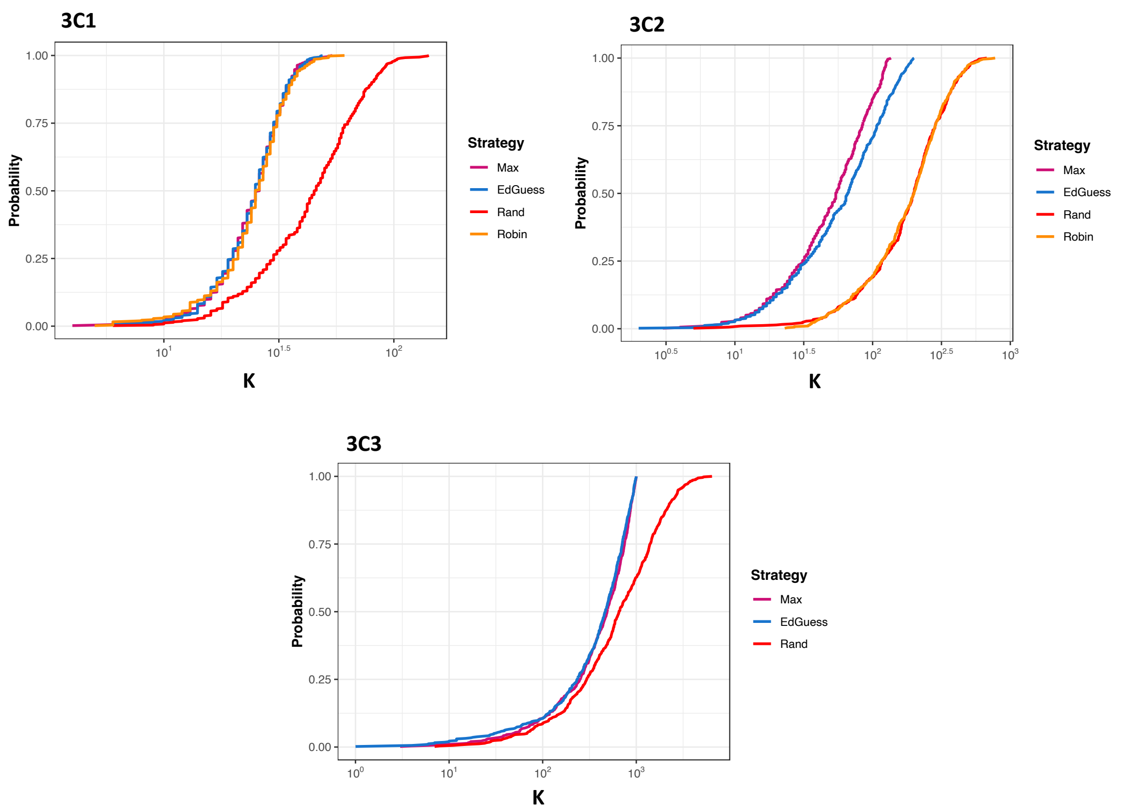


Figure B.11: Empirical CDF for all strategies ${}^3C_m$, where k = guess.

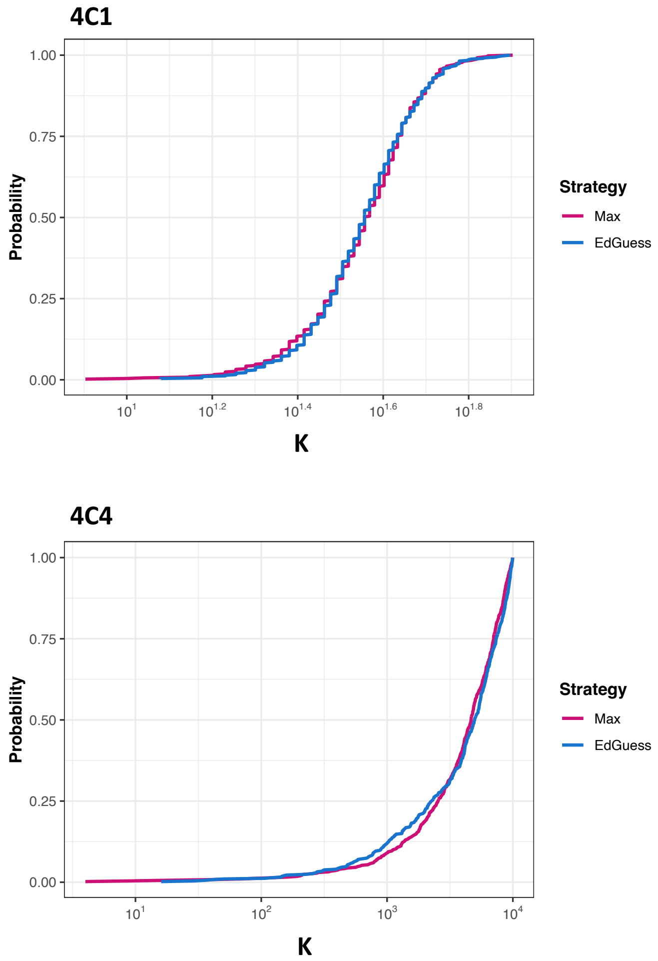


Figure B.12: Empirical CDF for Educated Guess & Max method ${}^4C_1$ & ${}^4C_4$, where k = guess.

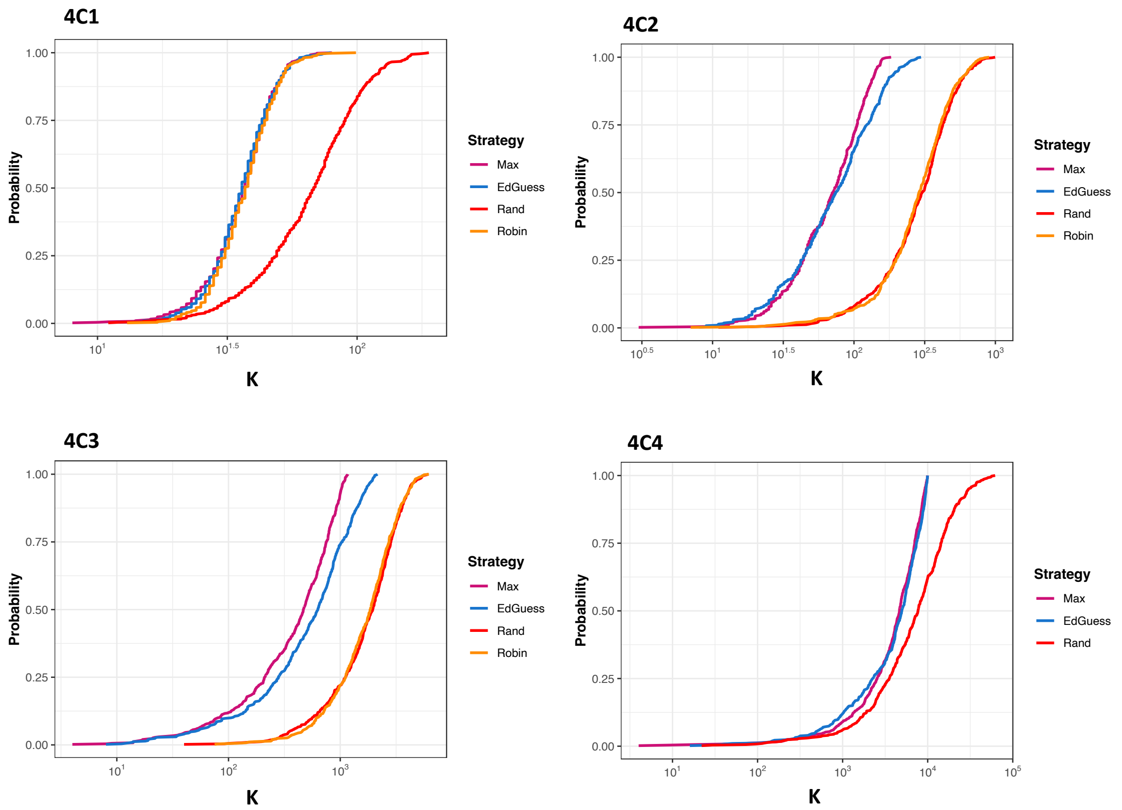


Figure B.13: Empirical CDF for all strategies ${}^4C_m$, where k = guess.

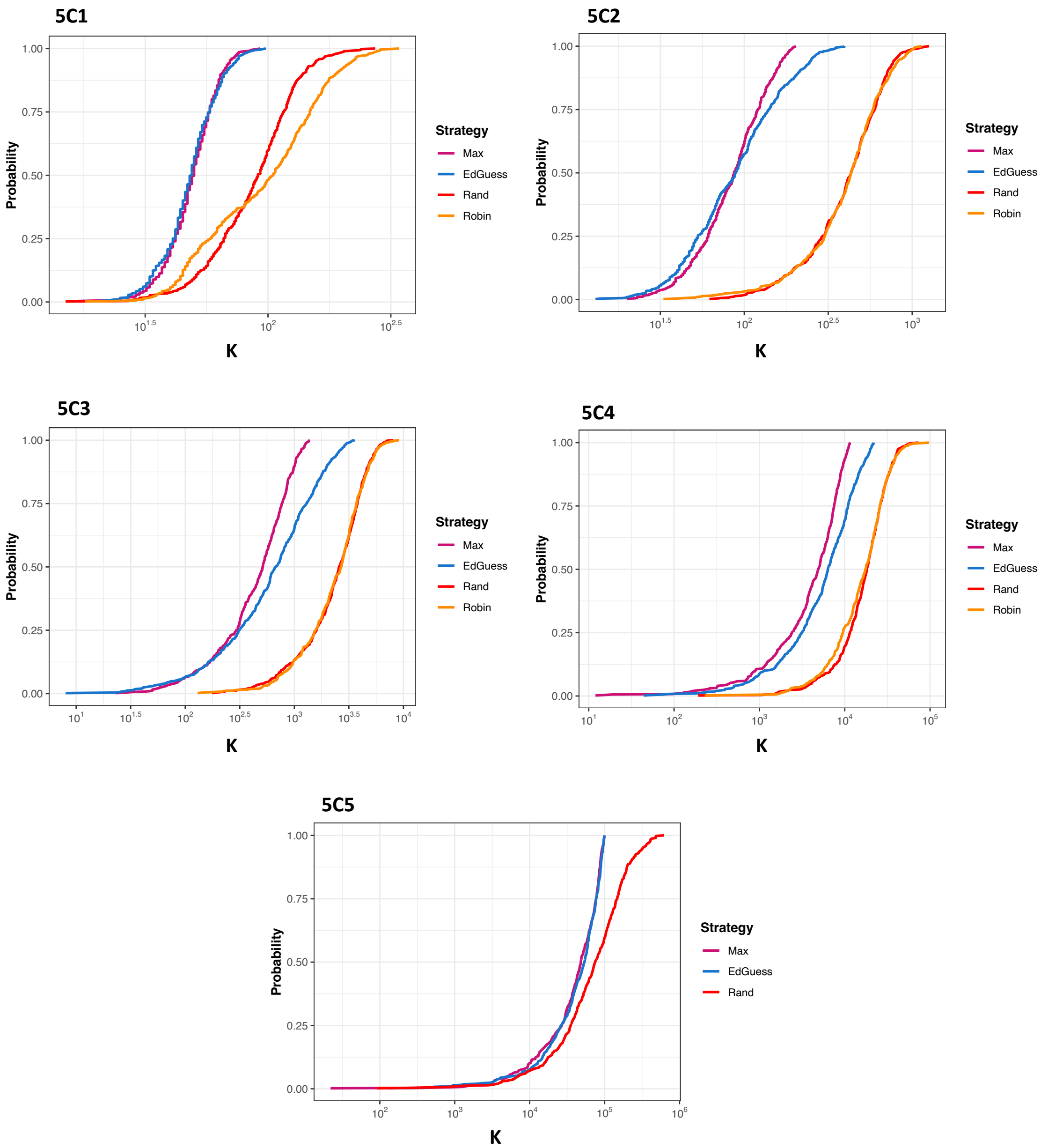


Figure B.14: Empirical CDF for all strategies ^5C_m , where k = guess.

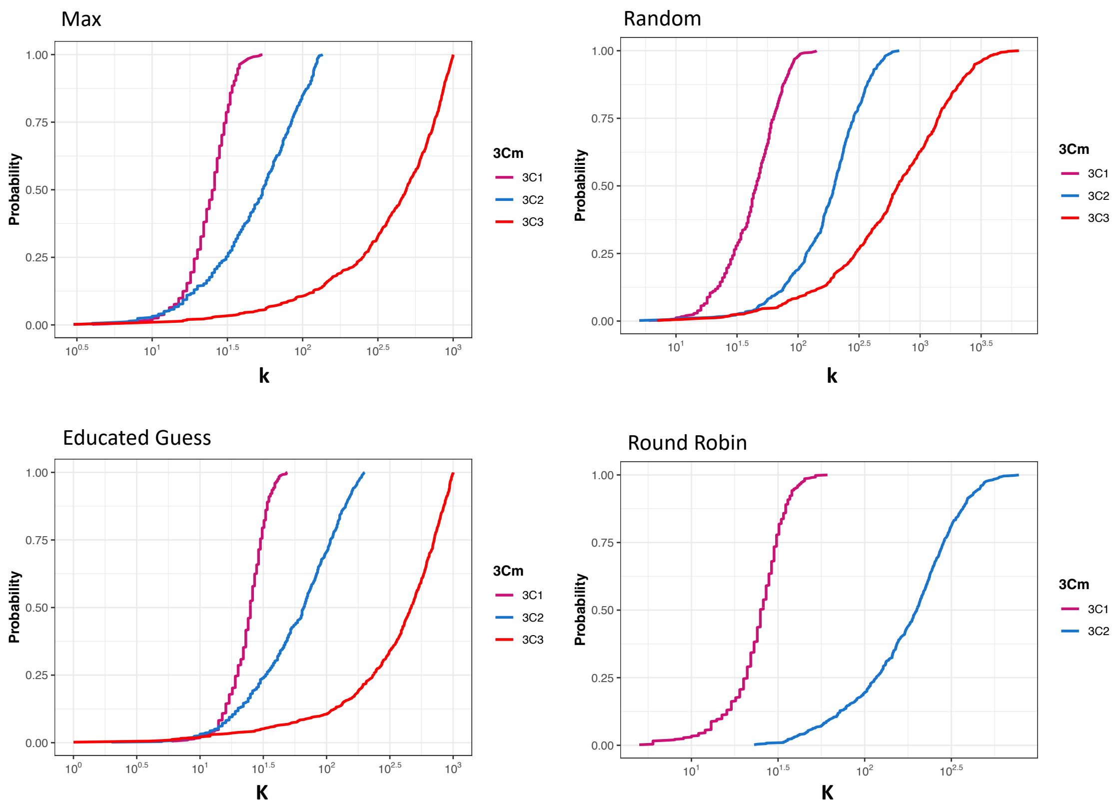


Figure B.15: Empirical CDF for all strategies ^3C_m, where k = guess.

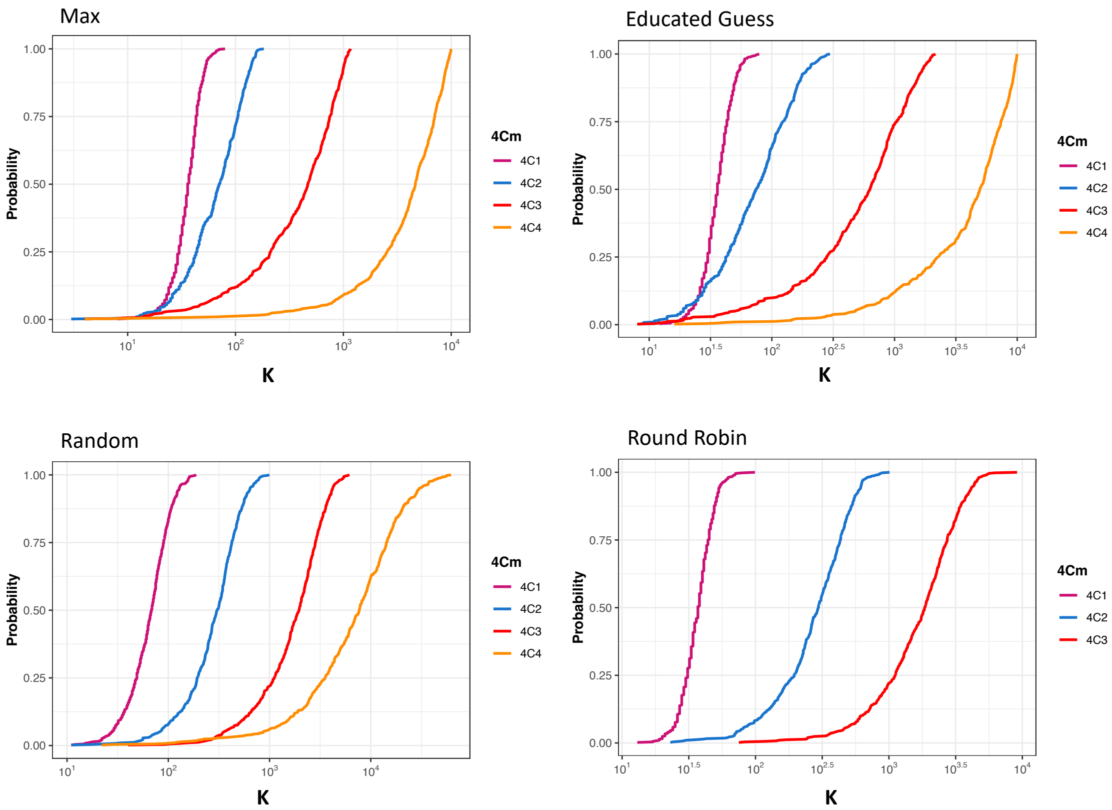


Figure B.16: Empirical CDF for all strategies ${}^4C_m$, where k = guess.

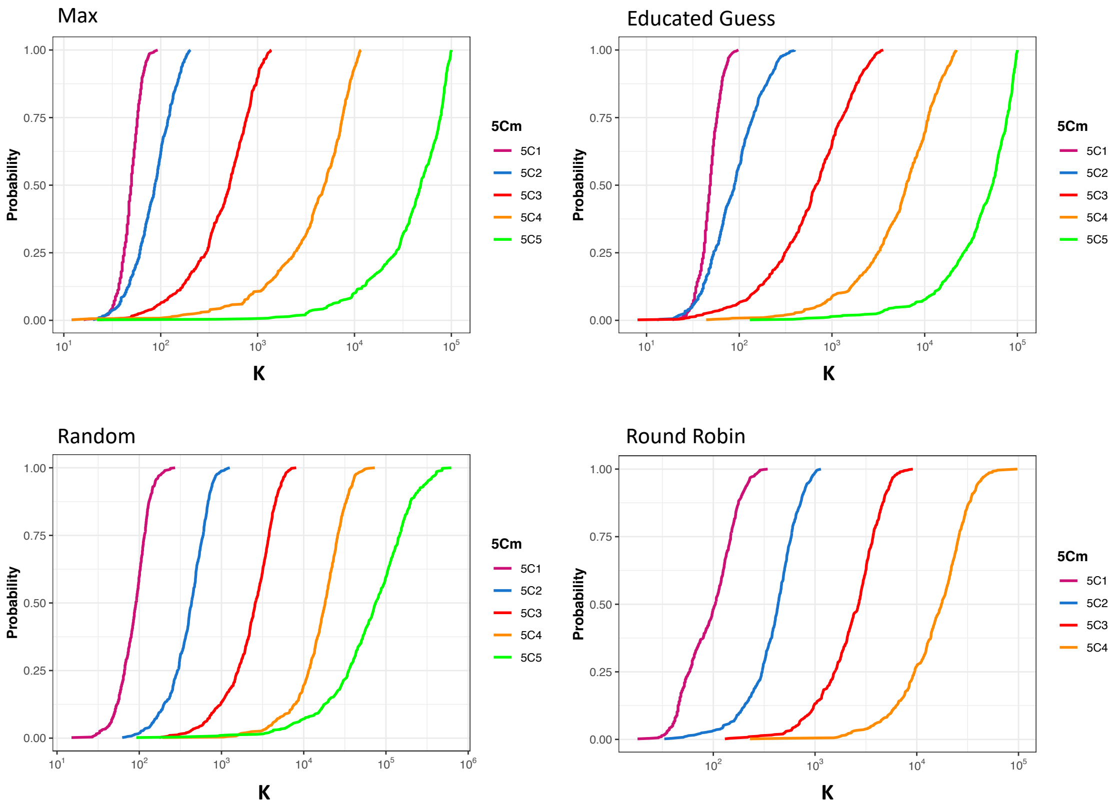


Figure B.17: Empirical CDF for all strategies ${}^5C_m$, where k = guess.

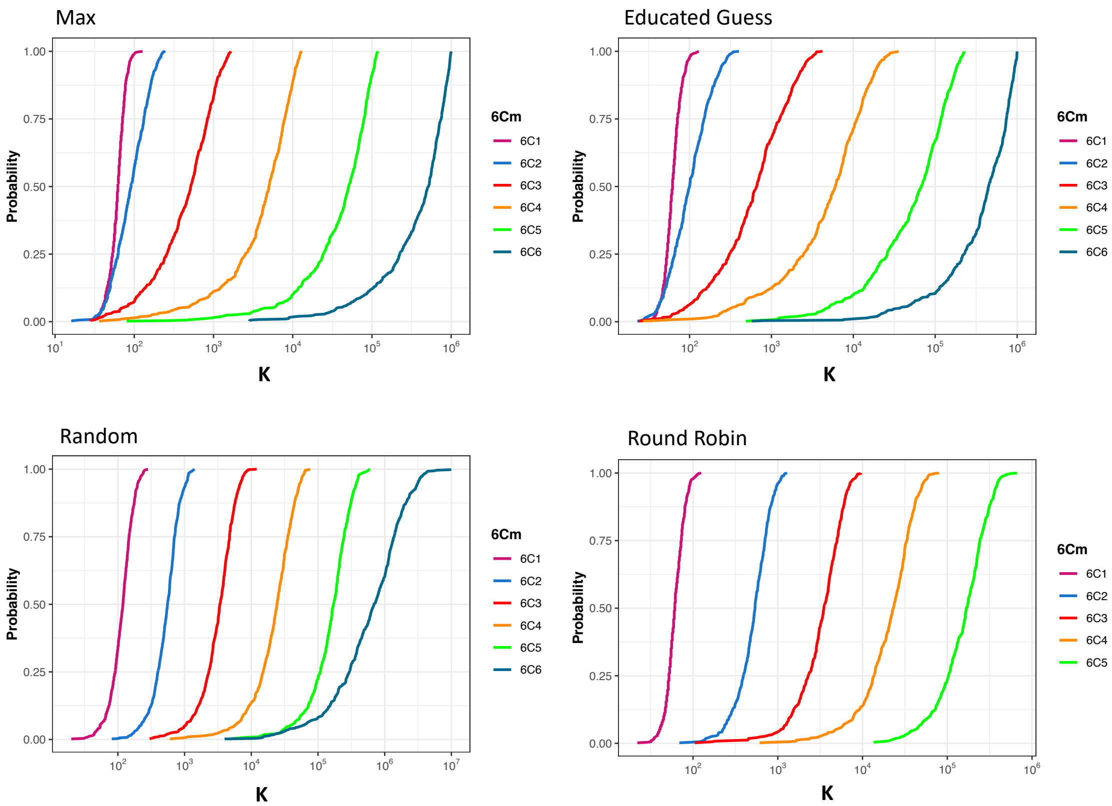


Figure B.18: Empirical CDF for all strategies ${}^6C_m$, where k = guess.

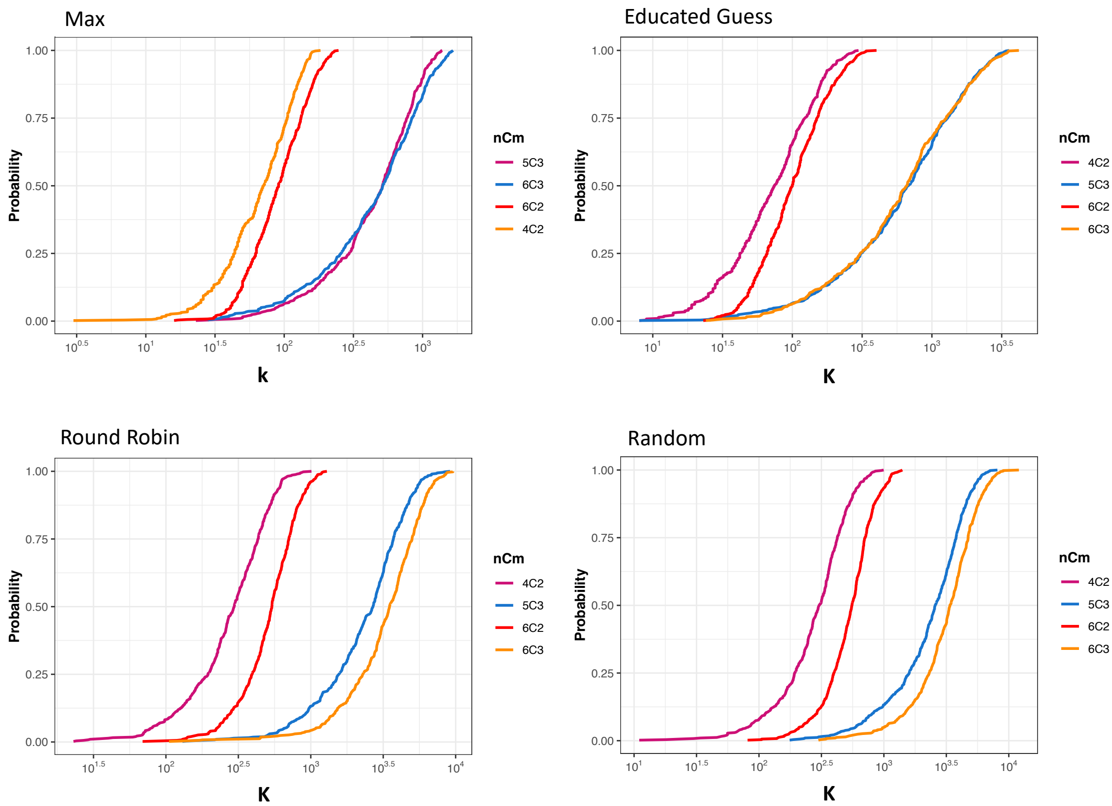


Figure B.19: Empirical CDF for all strategies comparing partial PIN ratios ${}^nC_m$, where k = guess.

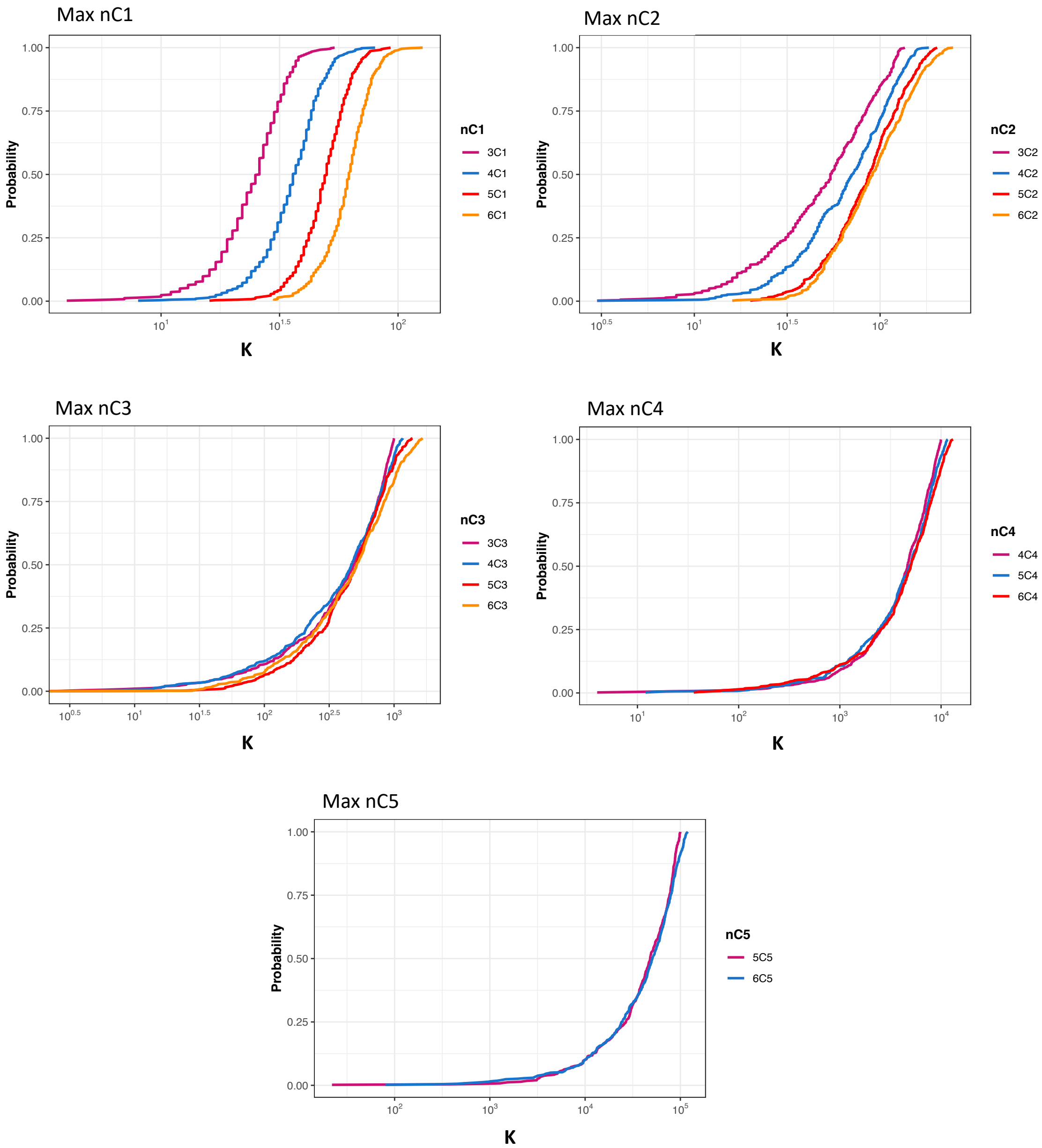


Figure B.20: Empirical CDF for Max method ${}^nC_1, {}^nC_2, {}^nC_3, {}^nC_4$ and ${}^nC_5$, with m fixed, where k = guess.

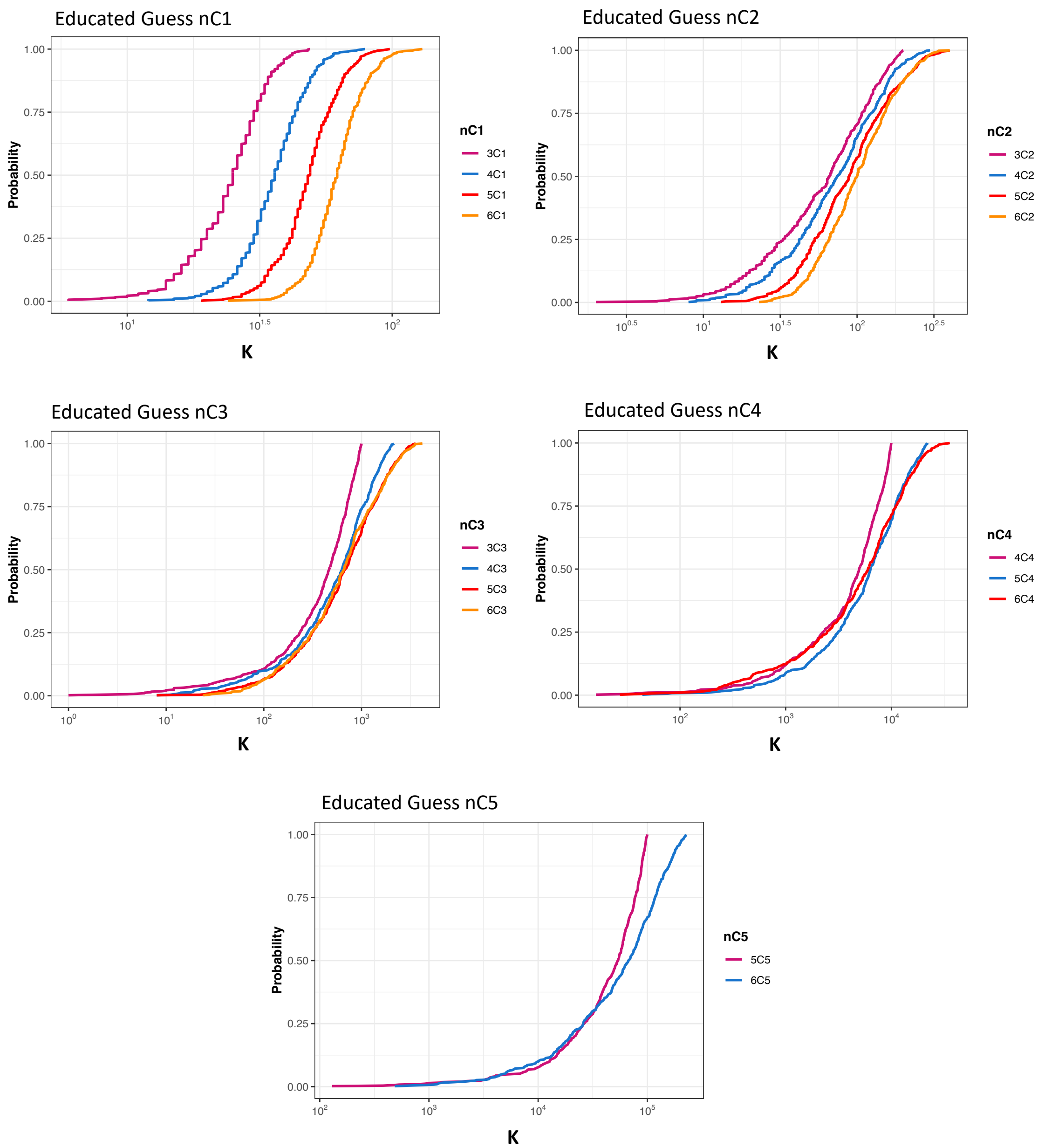


Figure B.21: Empirical CDF for Educated guess ${}^nC_1$,${}^nC_2$,${}^nC_3$,${}^nC_4$ and ${}^nC_5$, with m fixed where k = guess.

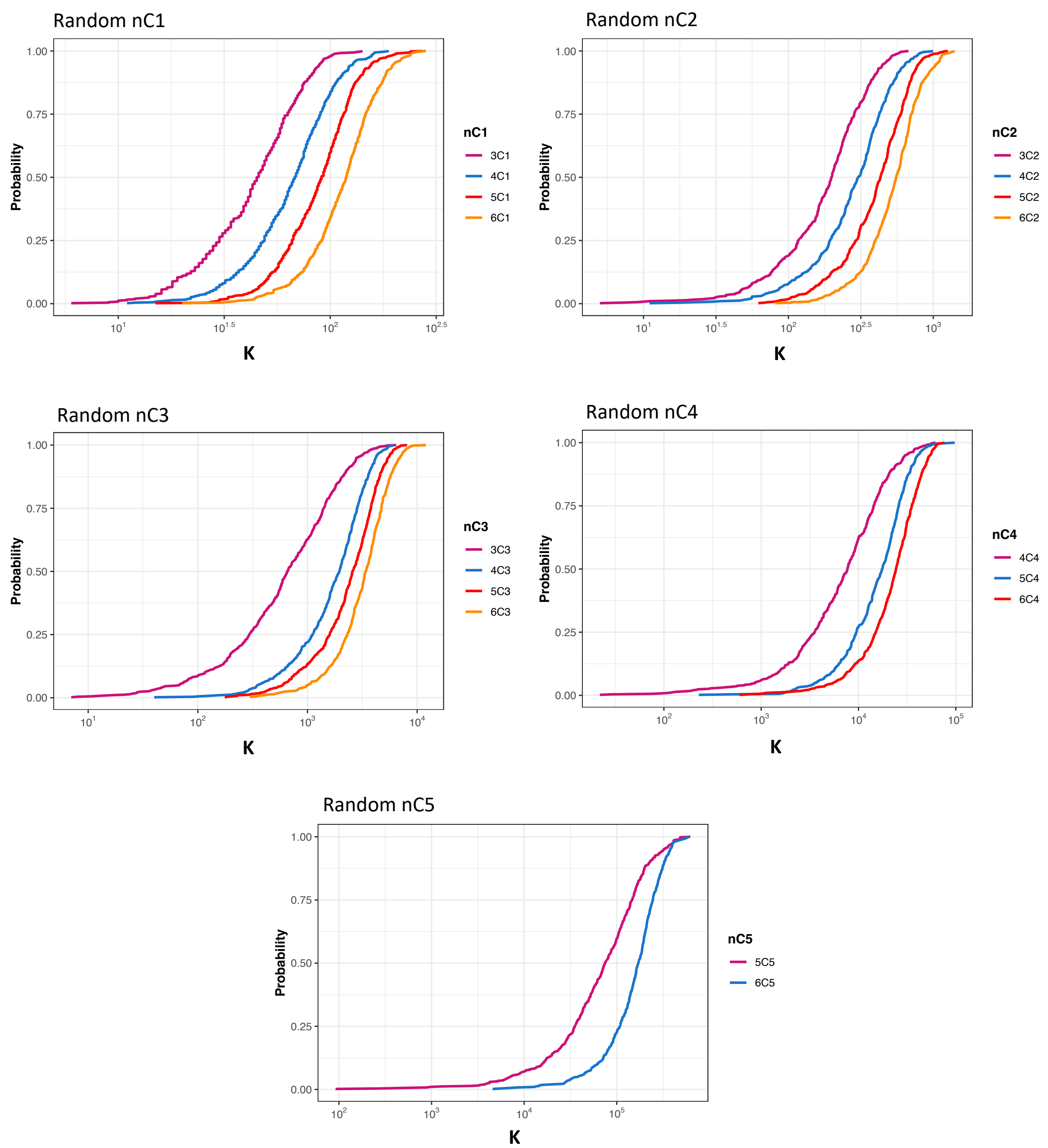


Figure B.22: Empirical CDF for Random method ${}^{n}C_1$,${}^{n}C_2$,${}^{n}C_3$,${}^{n}C_4$ and ${}^{n}C_5$, with m fixed, where k = guess.

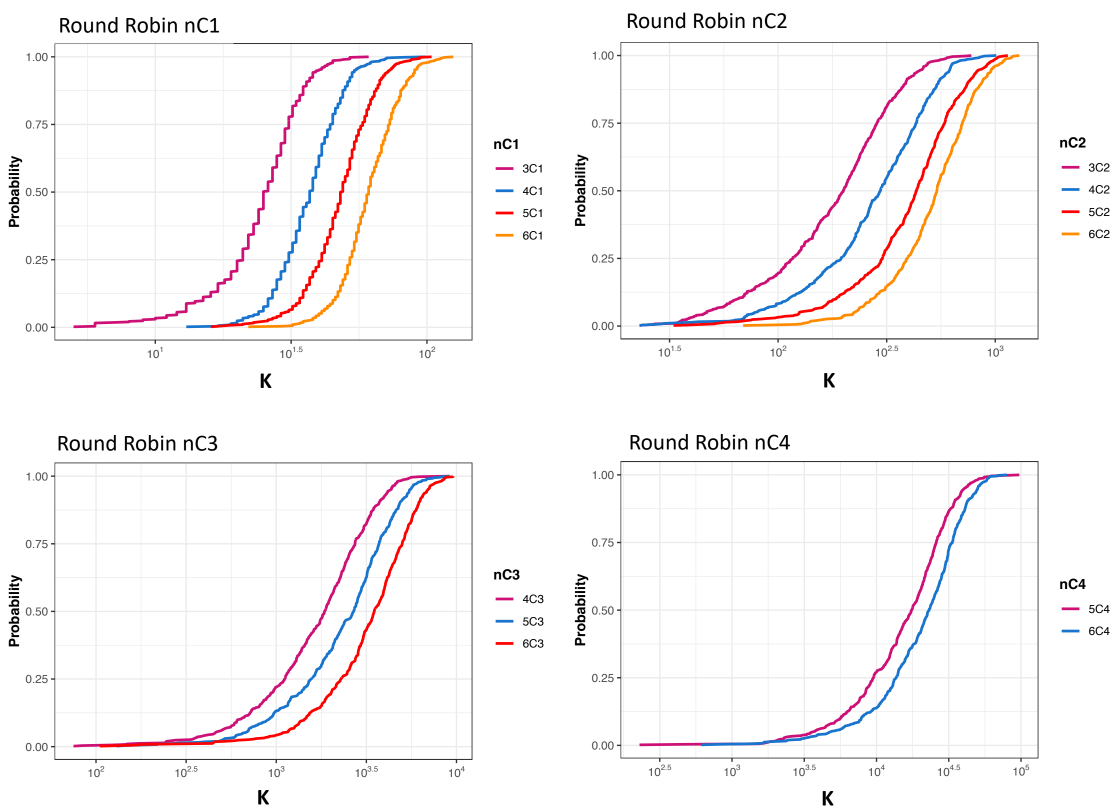


Figure B.23: Empirical CDF for Round Robin method ${}^nC_1$,${}^nC_2$,${}^nC_3$ and ${}^nC_4$, with m fixed, where k = guess.

B.3 Empirical Versus Theoretical CDF Results

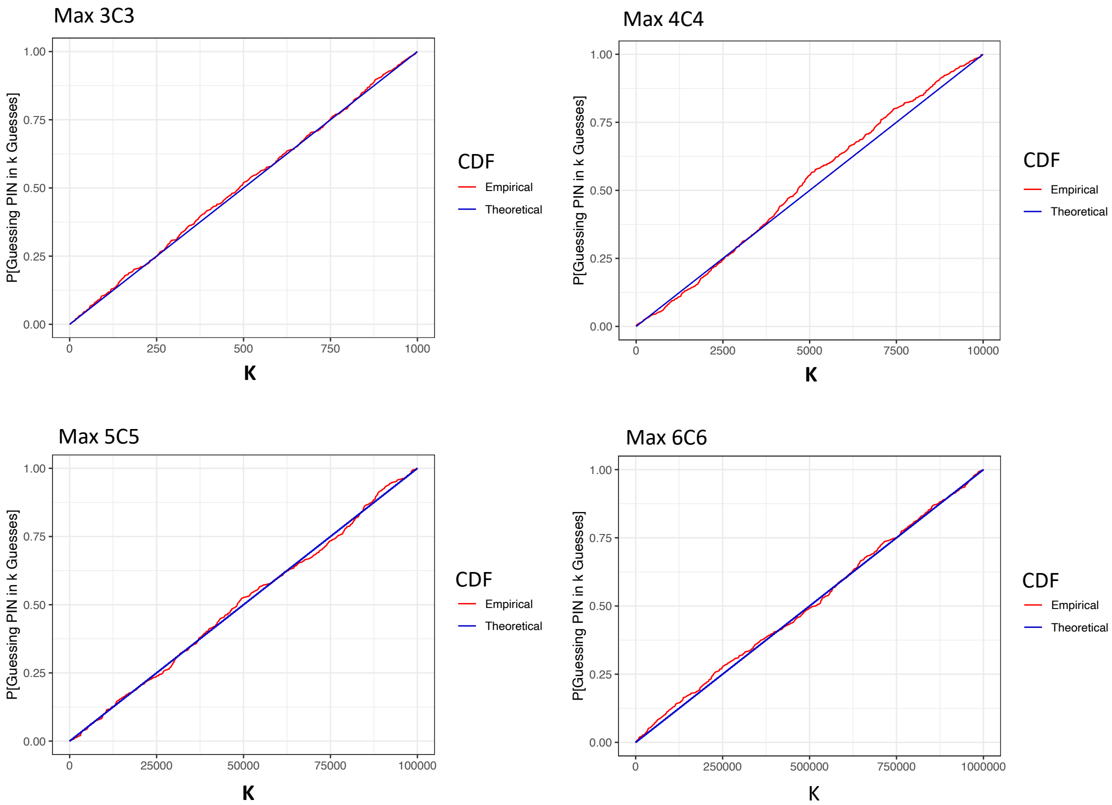


Figure B.24: Empirical versus theoretical CDF for Max method ${}^{n}C_{n}$, where $k =$ guess.

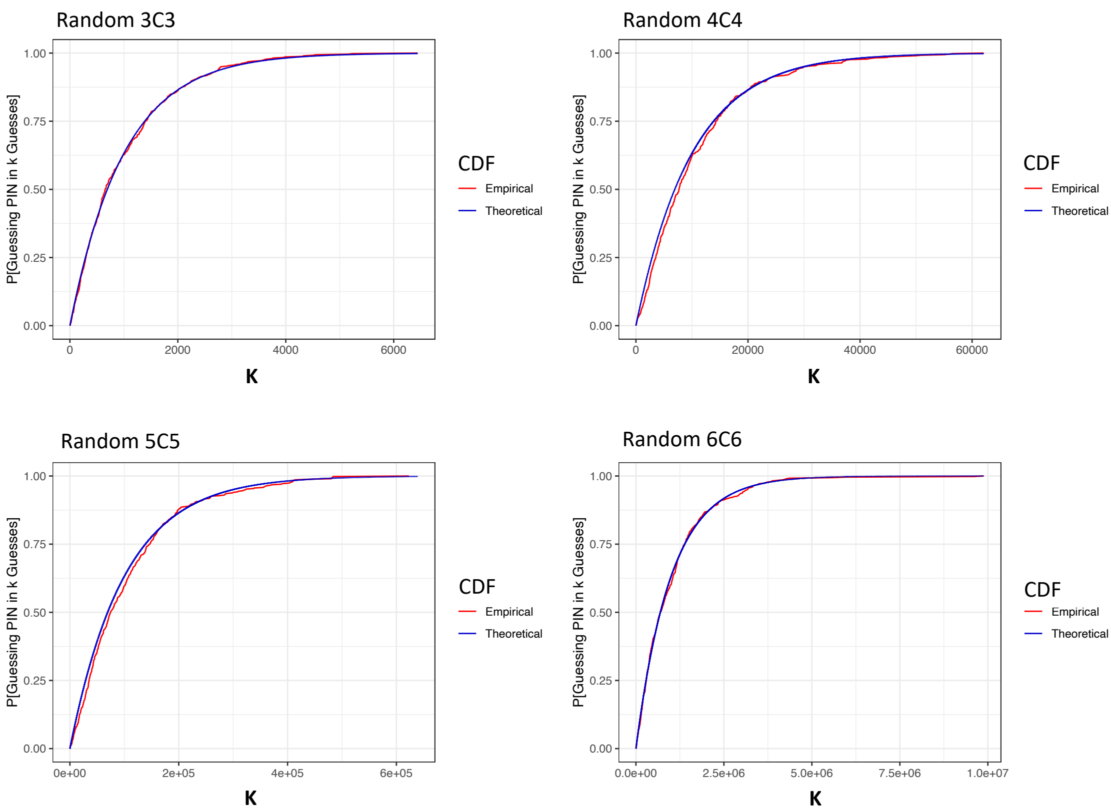


Figure B.25: Empirical versus theoretical CDF for Random method ${}^{n}C_{n}$, where k = guess.

B.4 All Strategies First & Final Log In Guess

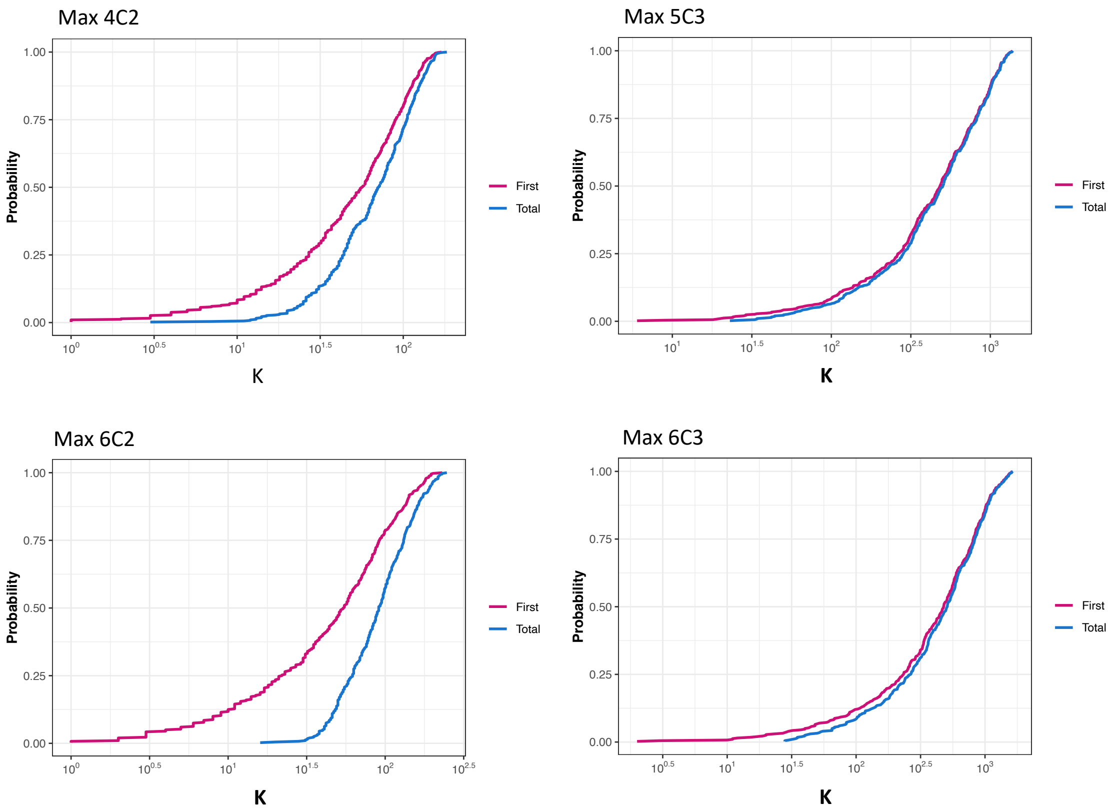


Figure B.26: Empirical CDF of Max method first & final log in for most used partial PIN ratios ${}^nC_m$, where k = guess.

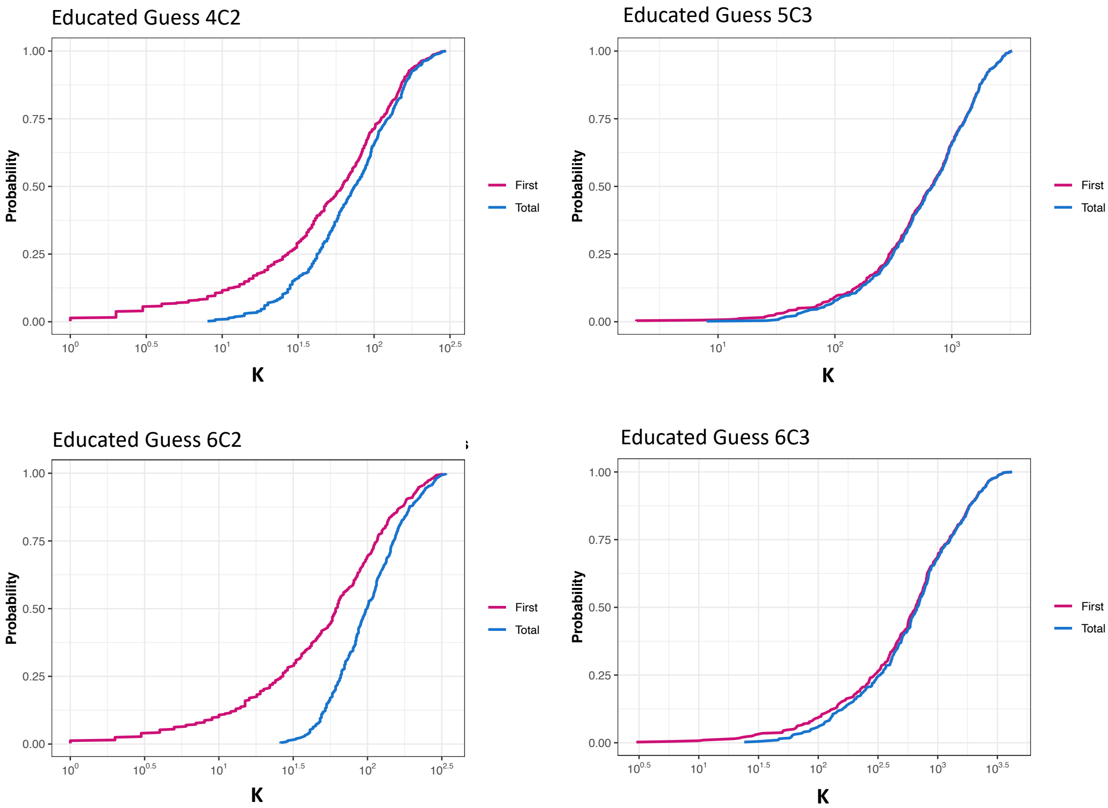


Figure B.27: Empirical CDF for Educated guess's first & final log in for most used partial PIN ratios ${}^{n}C_{m}$, where k = guess.

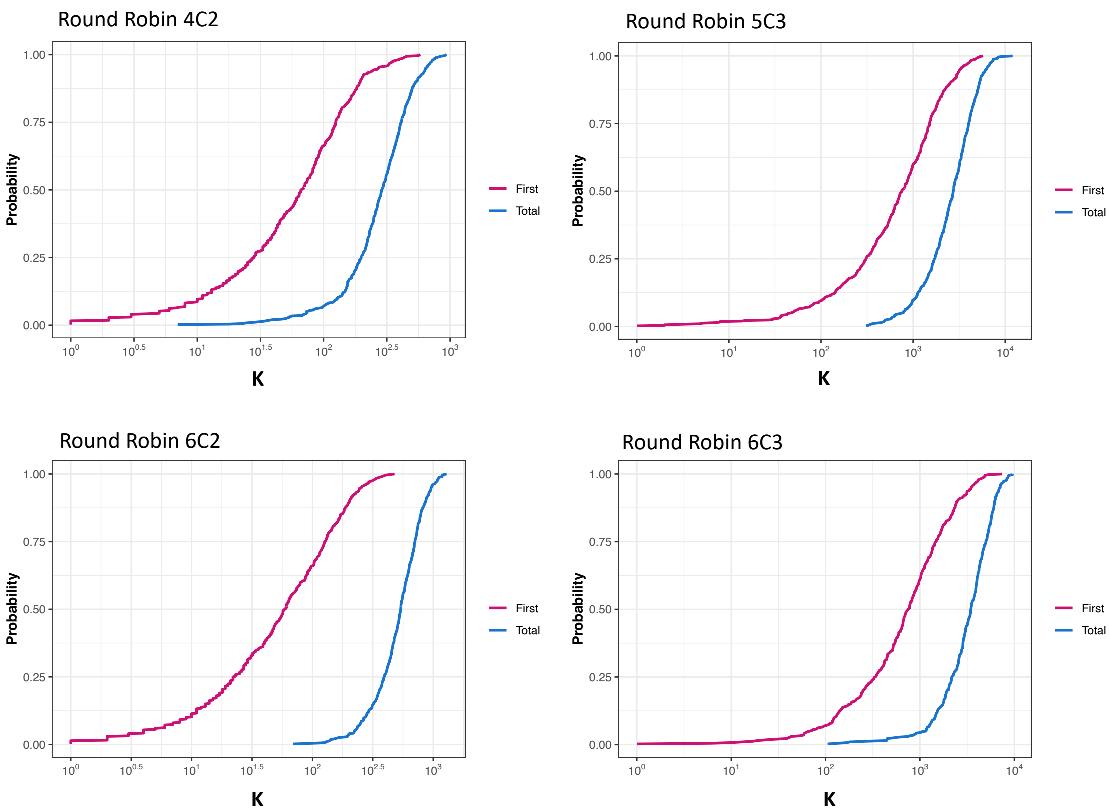


Figure B.28: Empirical CDF for Round Robin's first & final log in for most used partial PIN ratios ${}^nC_m$, where k = guess.

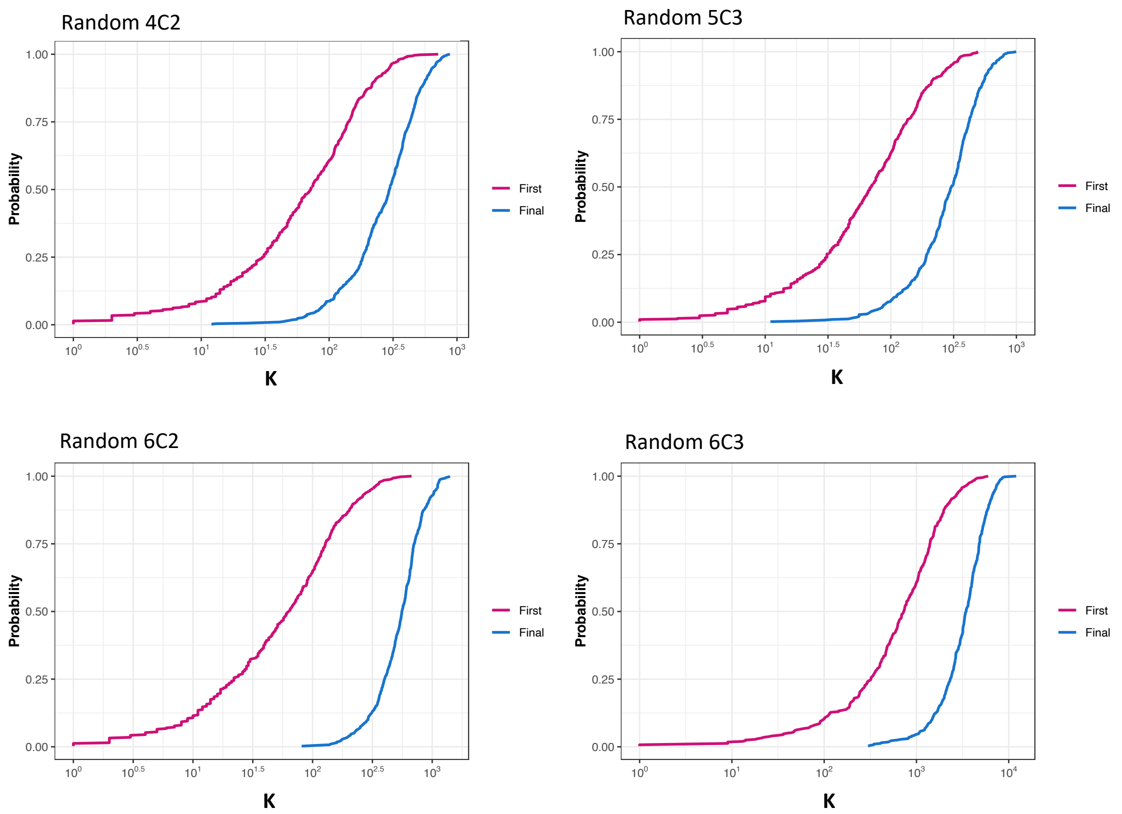


Figure B.29: Empirical CDF for Random's first & final log in for most used partial PIN ratios ${}^{n}C_{m}$, where k = guess.

APPENDIX C

Guessing Time Based One Time Passwords

C.1 Introduction

In the process of mathematically analysing the guessing of partial PINs, we considered whether this analysis could be extended to other forms of authentication. Here, through a thought experiment, we pose the question:

RQ: How our partial PIN guessing methods might be applied to guessing time-based one-time passwords (TOTP).

C.1.1 TOTP Background

Time-based One-Time Password algorithm (TOTP) is an extension of the HMAC-based One-time Password algorithm (HOTP). Generating a one-time password from the current time instead of a counter.

C.1.1.1 TOTP Protocol

The TOTP algorithm employs a shared secret key (K) and the current time to produce a distinctive password that alters (usually) every 30 seconds . This password is generated by an authenticator app, examples of which include, Microsoft

Authenticator, Authy, and Google Authenticator. This app is synchronized with the server responsible for authenticating the user's credentials. It adheres to the following protocol (see Fig.C.1):

1. The user provides their username and password.
2. The server generates a random secret key (K) and sends it to the user's phone.
3. The user's device uses the secret key and the current time to generate a unique one-time password.
4. The user enters the one-time password into the authentication system within the given time frame.
5. The server checks the one-time password against the one it generated using the same secret key and time frame. If they match, the user is authenticated.

C.1.1.2 TOTP Algorithm

The algorithm is much the same as the HOTP, except we replace our C for counter with C_T based on the time. Here again K is our shared secret.

$$TOTP_v = HOTP(K, C_T)$$

$$C_T = \left\lfloor \frac{T - T_0}{T_X} \right\rfloor$$

Where: C_T is the floor[1] of the number of durations T_X between a unique epoch T_0 and current time T in seconds.

[1]Floor function is a mathematical operation that, when applied to a real number x, yields the largest integer that is less than or equal to x.

C.1.1.3 TOTP Usability & Security

As TOTP does not rely on a network service to provide a code it is therefore safe against 'man in the middle' attacks and sim-jacking[2]. In terms of usability, given that the unique TOTP (Time-Based One-Time Password) has a duration of (usually) 30 seconds, users therefore, have a 30-second window to input the code, which increases the possibility of incorrect input [249]. This could potentially be difficult for users who have certain movement impairments. In a user study testing usability of two factor authentication, 8 out the 12 participants mentioned they had problems entering the code before the 30 seconds were up [249]. The recommended time length is 30 seconds in terms of usability and security [112], but it can be range from 30 to 120 seconds [34].

Time-based One-Time Password algorithm (TOTP) is an extension of the HMAC-based One-time Password algorithm (HOTP). Generating a one-time password from the current time instead of a counter.

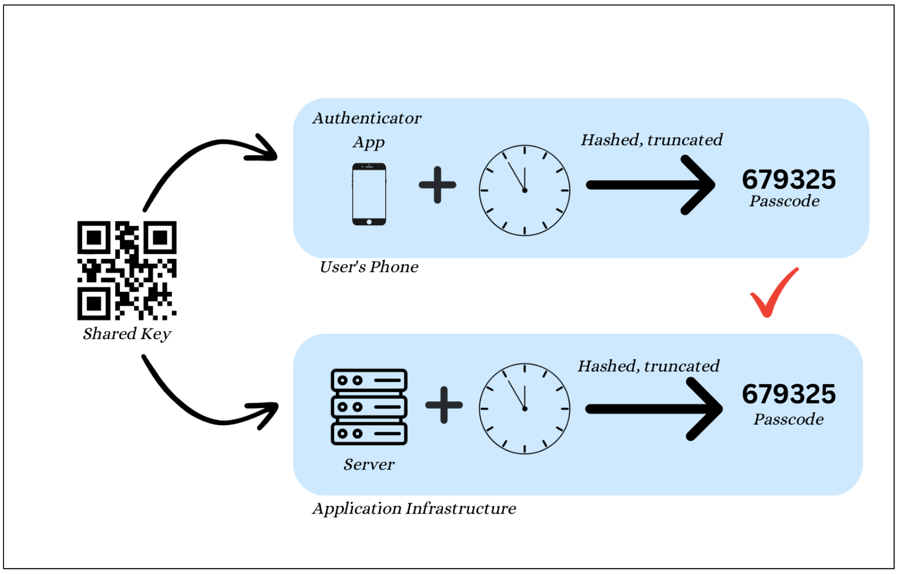


Figure C.1: Time based one time password (TOTP) protocol.

[2]SIM swapping is a form of identity theft that focuses on your phone number. Perpetrators employ SIM swapping to seize control of your mobile phone account, enabling them to acquire your personal data, such as text messages, contacts, and financial account details. Additionally, they can exploit this method to initiate calls and send text messages on your behalf [55].

C.1.2 Guessing TOTP Protocol

To compare guessing time based OTP to guessing PINs via partial PINs, we can use the following relations: our shared key or secret for TOTP is our PIN, the time stamp used in TOTP is equivalent to the subset requested by bank and the hash function applied by TOTP is equivalent to the digit selection. We assume that the secret part of the key is 256 bits, so there are 2^{256} possibilities making the PIN list for TOTP far larger, however. But in theory the same protocol can be applied in a situation where for example you snoop a TOTP code input, you would eliminate a large section of the PIN list (i.e., list of all possible secrets). Our in the wild scenario[3] in this case could see Eve sitting on a train and performing a *shoulder surfing* attack on the passenger beside her. Bob leaves his authenticator app open for three minutes and she sees six different codes. She notes the time and can look up the hash. Now she attempts to hash every key on the pin list which can be as big as 2^{256} in order to see if they match the codes she has acquired. If these don't match she can eliminate a these from the list. If for example, Eve observes the one time password 547982 at time t. We keep the secrets, k_i, where:

$$h_t(k_i) = 547982. \tag{C.1}$$

The chance of matching this one time codes is $\frac{1}{10^6}$. Since a good hash functions output will be independent and uniformly distributed, you can write the probability that the key k_i is still on list as:

$$\mathbb{P}[k_i \text{ still on list after G snoops}] = \frac{1}{10^d} \cdots \frac{1}{10^d} = \frac{1}{10^{dG}}. \tag{C.2}$$

With d the number of digits of the code, after G guesses (or snoops). The number of guesses, G, in this case to reduce our PIN list to the correct key could be estimated by finding the number of snoops required to get the expected number of secrets on the list to be about 1,

$$\frac{2^{256}}{10^{6G}} \approx 1. \tag{C.3}$$

[3]Admittedly highly unlikely, but useful for demonstrative purposes.

Solving Eq. C.3 gives us about thirteen snoops. This number is quite small considering the size of our potential PIN list.

Given the size of this list this attack would be computationally unfeasible, but guesses will eliminate big portions of this list.

APPENDIX D

Additional Cookie Study Material

D.1 Additional Banner Screenshots

Figure D.1: If you are not happy with `afloat.ie` using cookies, leave the page. This banner is displayed at the end of the home page.

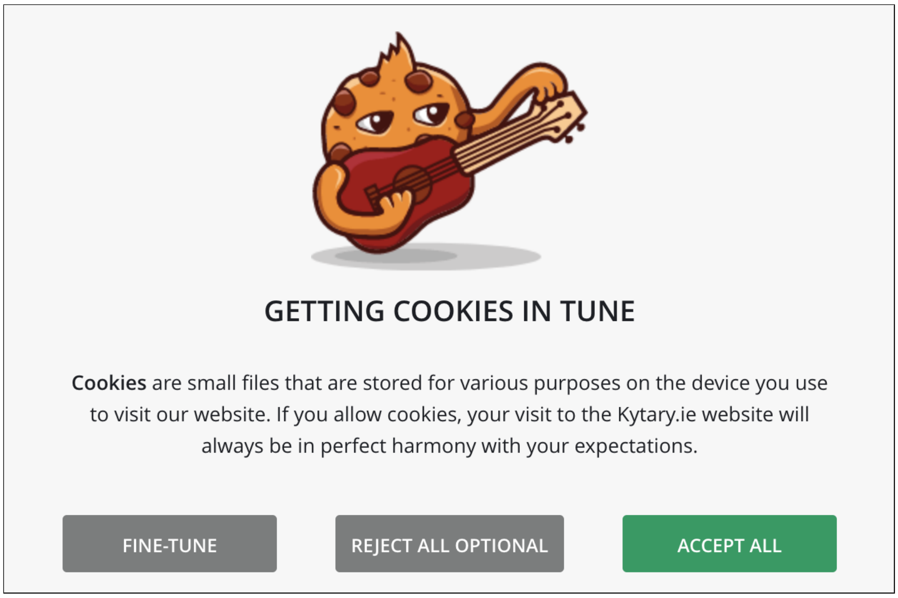


Figure D.2: `kytary.ie` musical instrument website's cookie banner uses musical references to describe choices for cookies.

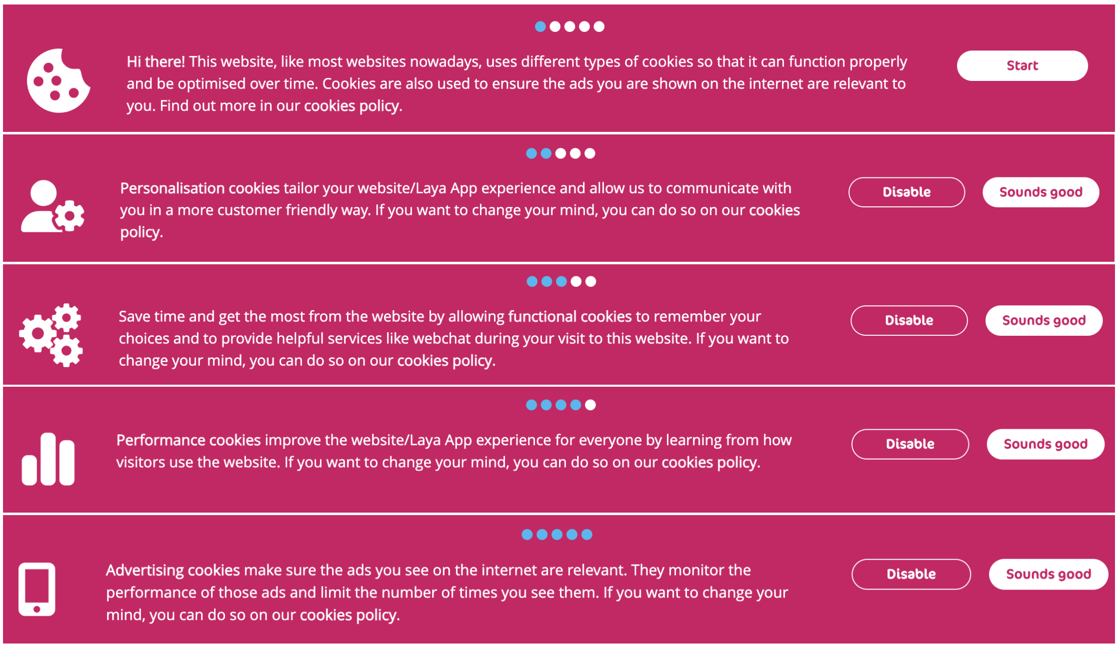


Figure D.3: To configure cookies on `layahealth.ie`, you must go through five levels whether you disable or accept.

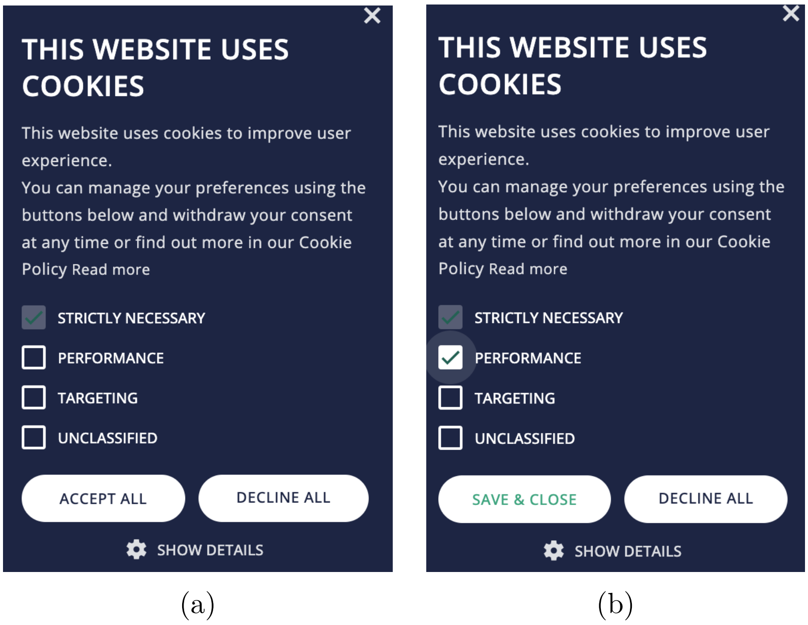


Figure D.4: The first image (a) shows choices for cookies with 'accept all' and 'decline all', there appears to be no option to accept what is currently ticked. In the next image (b) you can see that when you click one of the options the 'save and close' button now appears. You can now un-click the performance option and you are still left with the option to save and close with 'strictly necessary' cookies. This was only accidentally discovered. Otherwise you may feel accepting all or declining all is the only option. Taken from `weare.ie`

D.2 Manual Irish Website List

- donedeal.ie
- daft.ie
- independent.ie
- rte.ie
- boards.ie
- ebay.ie
- aib.ie
- irishtimes.com
- adverts.ie
- eir.ie
- lottery.ie
- thejournal.ie
- open24.ie
- argos.ie
- three.ie
- ryanair.com
- tripadvisor.ie
- discoverireland.ie

Table D.1: List of Irish websites manually gathered, which were not in the Tranco list.

APPENDIX E

Additional Subscription Material

E.1 Additional Subscription Screenshots

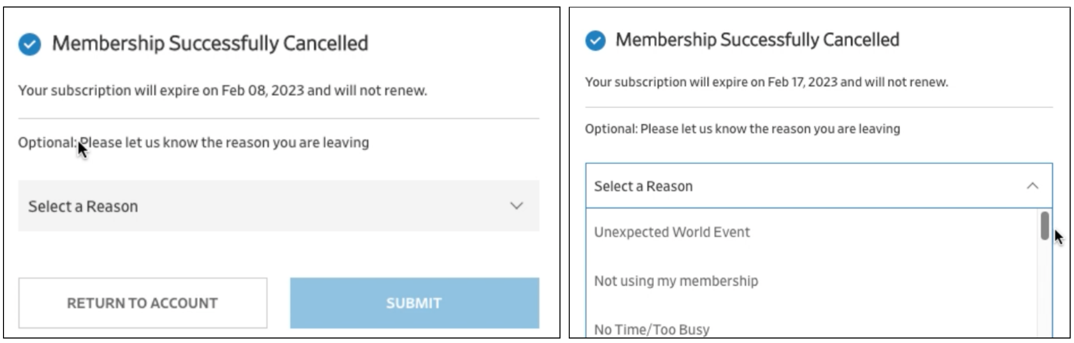
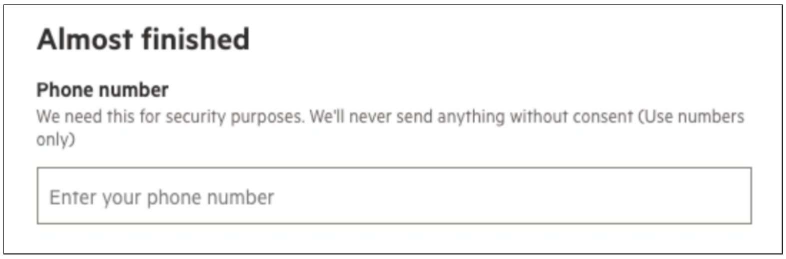
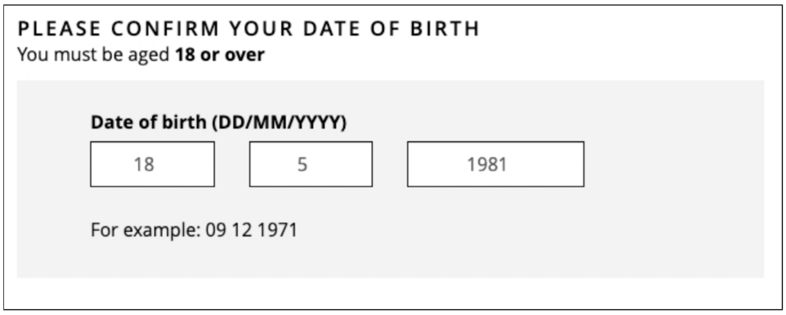


Figure E.1: You can not go further unless you answer ‘optional’ survey for WSJ & Barrons.



(a) Financial Times request for phone number



(b) Daily Mail request for DOB

Figure E.2: Examples of data requested when subscribing.

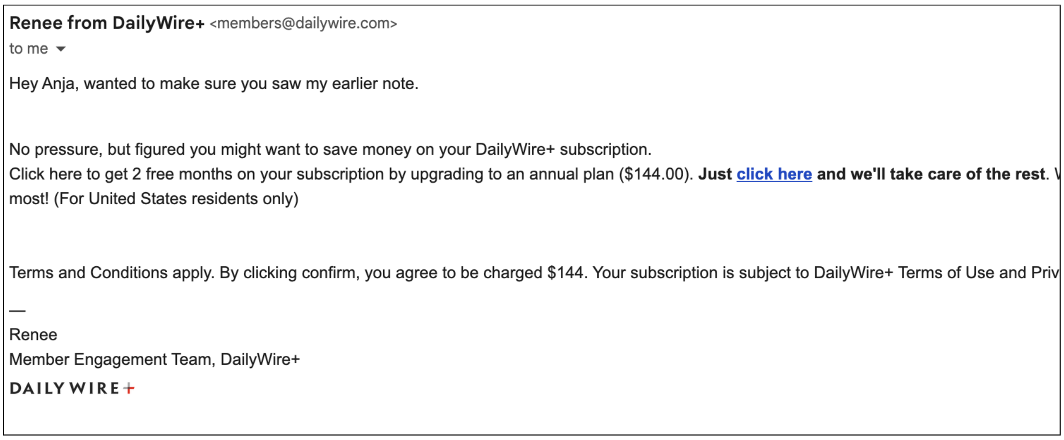
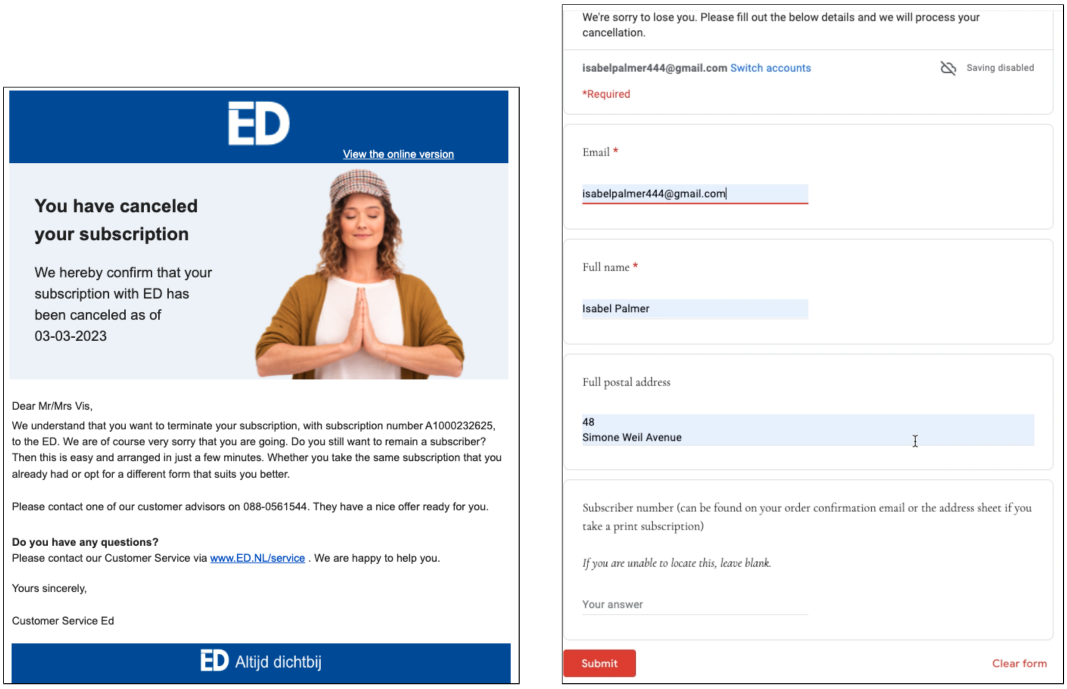


Figure E.4: Daily Wire's reminder email regarding previously sent promotional offer received one day after subscribing.



(a) Eindhovens Dagblad (NL)

(b) Spectator (UK)

Figure E.3: Example of a post cancellation email (a) and a cancellation form (b).

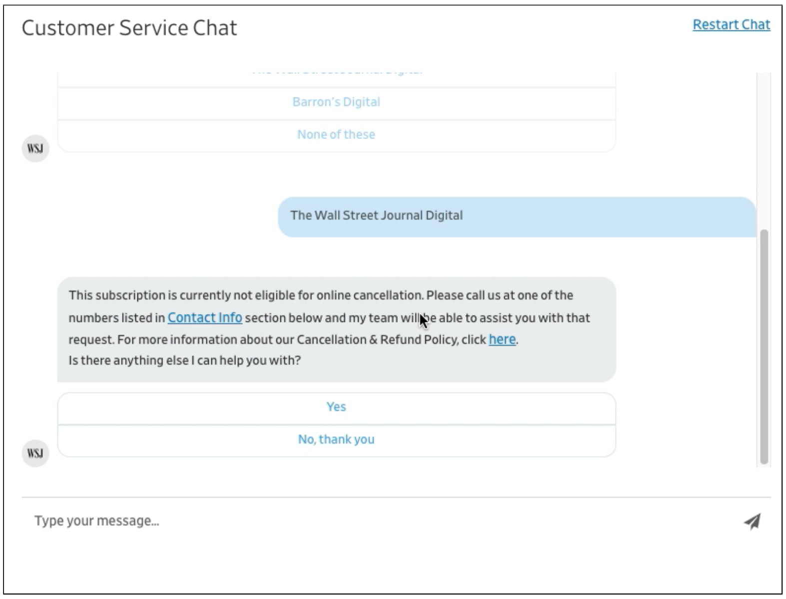
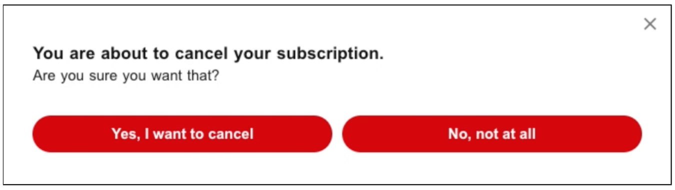


Figure E.5: Wall Street Journal's customer service chat informing our persona they need to call to cancel.

(a) NRC



(b) Het Algemeen Dagblad (AD)

Figure E.6: (a) NRC is the only Dutch newspaper that requires a phone call for cancelling subscriptions. (b) Het Algemeen Dagblad (AD) cancel notice with equal colours.

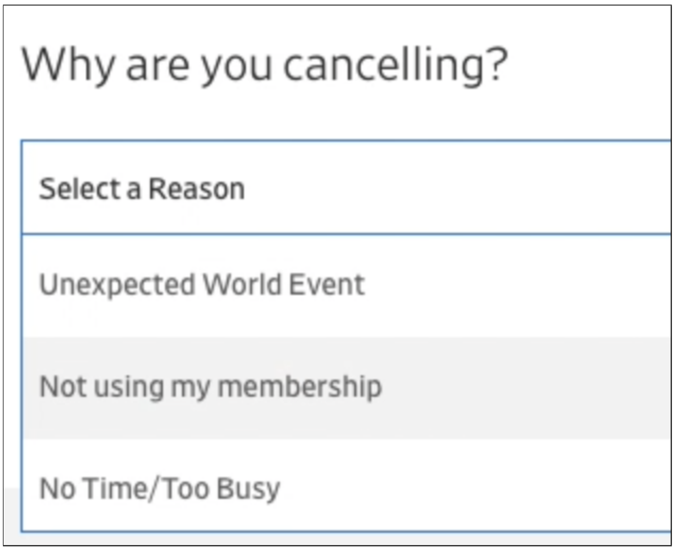


Figure E.7: Barron's unusual survey answer option.

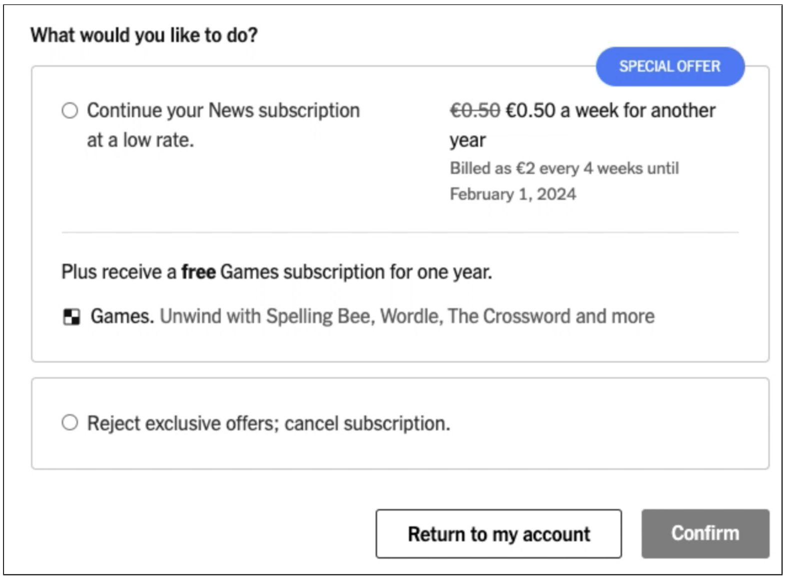


Figure E.8: The New York Times require you to click to reject their special offers before confirming that you are cancelling your subscription.

E.2 Additional Subscribing & Cancelling Results

Country	Media	Data
Germany	Bildplus	ENO
	WeltPlus	ENO
	Süddeutsche Zeitung+	ENO
	Frankfurter Allgemeine	ENO
	Heise+	ENO
	Rheinische Post+	EO
	Kieler Nachrichten+	ENOZ
	The Pioneer	ENO
Netherlands	Het Algemeen Dagblad (AD)	EN
	Telegraaf	DENP
	De Volkskrant	EN
	NRC	AENZ
	Trouw	EN
	Eindhovens Dagblad (ED)	EN
	Noordhollands Dagblad	EN
	Tubantia	EN
	PZC	EN
United Kingdom	Financial Times	ENOP
	The Telegraph	EN
	The Guardian	EN
	Tortoise	EN
	Mail +	DENO
	Spectator	ACENOZ
	The Economist	ACENOZ
	iNews	EN
United States of America	The New York Times	ENOZ
	Wall Street Journal	ACENOZ
	Washington Post	EOZ
	The Athletic	EN
	Substack	E
	Medium	E
	The Daily Wire	ACENOZ
	Barrons	ACENOZ
	Bloomberg Media	CENO

Table E.1: Data requested by each countries media website. Letters indicate required details — E: Email, N: Name, O: Country, Z: Zip code, D: DOB, A: Address, P: Phone, C: City.

US Media	**Texas USA**			**California USA**			**Germany**			**Netherlands**			**United Kingdom**		
	Clicks to Subscribe	Clicks to Cancel	Extra Clicks	Clicks to Subscribe	Clicks to Cancel	Extra Clicks	Clicks to Subscribe	Clicks to Cancel	Extra Clicks	Clicks to Subscribe	Clicks to Cancel	Extra Clicks	Clicks to Subscribe	Clicks to Cancel	Extra Clicks
The New York Times	4	7	3	4	7	3	5	7	2	4	7	3	5	7	2
Wall Street Journal	5	*	*	5	5	0	4	5	1	4	5	1	4	*	*
Washington Post	4	6	2	4	6	2	3	6	3	3	6	3	3	6	3
The Athletic	2	6	4	2	6	4	2	6	4	2	6	4	2	6	4
Substack	3	5	2	3	3	0	3	6	3	3	6	3	3	6	3
Medium	3	5	2	3	5	2	3	5	2	3	5	2	3	5	2
The Daily Wire	3	4	1	3	4	1	3	4	1	3	4	1	3	4	1
Barrons	5	5	0	5	5	0	*	*	*	*	*	*	*	*	*
Bloomberg Media	3	10	7	3	10	7	3	10	7	3	10	7	3	10	7
Average	3.5	6	2.6	3.5	5.6	2.1	3.3	6.1	2.9	3.1	6.1	3	3.3	6.3	3.1

Table E.2: Number of clicks required to subscribe & cancel to US media from our American and European personas.

E.3 Additional Study Parameters

Question	**Table**	**Description**
Cancellation phone call duration		When calling to cancel, how long does the whole process take to cancel your subscription
Other barriers/details		What other barriers were there to cancelling, any dark patterns?
Subscription price	5.1	What was the price of the subscription we signed up for?
Trials	5.1	If there is a trial offered, is it free or how much is it reduced and what is the trial period?
Trials post-cancellation		If a trial period is offered, does the trial continue after cancelling?
Payment method		Do you have to pay via credit card or direct debit?
Cookie paywall		Is there a cookie paywall on the interface when subscribing?
Auto-renew button		Is there a button you can toggle to turn off auto-renewal?
Auto-renew acknowledgement tick box		Is there a tick box to acknowledge your understanding of auto-renewal information?
Duration of subscription	5.1	Is the subscription offered weekly, monthly, yearly or other?
No. subscribers	5.1	How many subscribers according to [74]
Tranco rank	5.1	What rank is news site according to Tranco

Table E.3: Additional details which were noted when subscribing and cancelling all subscriptions. Also included is location of results.

E.4 Bloomberg Chatbot Transcript

Below is the Chatbot automated transcript for our German persona Anja. As mentioned in Chapter 5, all transcripts were identical for cancelling the Bloomberg subscription for all personas.

Support Chat (02/02/2023, 16:10:43): Hi Anja! I'm Bloomberg Media's Messaging Assistant. I am happy to help you today.

Support Chat (02/02/2023, 16:10:44): Please select one of the following topics:

Support Chat (02/02/2023, 16:10:45): Menu Options:

Manage my Subscription
Website Feedback
Technical Troubleshooting
Marketing Preferences
Market Data
Bloomberg Professional Services

Anja (02/02/2023, 16:10:48): Manage my Subscription

Support Chat (02/02/2023, 16:10:50): Please help me narrow down your issue:

Support Chat (02/02/2023, 16:10:52): Menu Options:

Invoice Request
Apple/Google Purchase
Billing/Payment Issue
Cancel Subscription
Change Subscription
Product Delivery
Update Mailing Address
Change Email Address

Other
Previous Menu

Anja (02/02/2023, 16:10:54): Cancel Subscription

Support Chat (02/02/2023, 16:10:57): Before you cancel, we would like to offer you the following promotion:

Support Chat (02/02/2023, 16:10:58): On 13-Feb-2023 we can renew your subscription at the special rate of only $14.99/month.

Support Chat (02/02/2023, 16:10:59): Your subscription will continue to renew monthly at this rate - saving you over 50% off the full price.

Support Chat (02/02/2023, 16:11:01): Do you want to claim the discounted offer?

Support Chat (02/02/2023, 16:11:02): Menu Options:

Yes
No

Anja (02/02/2023, 16:11:03): No

Support Chat (02/02/2023, 16:11:05): If we cancel today, your subscription will remain active and you will retain access to Bloomberg.com until the end of the current billing cycle on 13-Feb-2023. Please confirm if you still wish to cancel.

Support Chat (02/02/2023, 16:11:06): Menu Options:

Yes
No

Anja (02/02/2023, 16:11:08): Yes

Support Chat (02/02/2023, 16:11:10): To complete the cancellation, please select your main reason for canceling:

Support Chat (02/02/2023, 16:11:11): Menu Options:

I want to turn off auto renew
I only subscribed to read a story
Not enough coverage
I can find similar content for free
I didn't use the service enough
It is too expensive
Other: (Please specify reason)

Anja (02/02/2023, 16:11:15): I want to turn off auto renew

Support Chat (02/02/2023, 16:11:19): At your request, we processed your cancellation effective today. Your subscription will remain active and you will retain access to Bloomberg.com until the end of the current billing cycle on 13-Feb-2023

Support Chat (02/02/2023, 16:11:20): It was a pleasure assisting you today. Are you willing to take a brief survey about the service you received?

Support Chat (02/02/2023, 16:11:22): Menu Options:

Yes
No

Anja (02/02/2023, 16:11:24): No

Support Chat (02/02/2023, 16:11:26): Thank you for chatting, have a great day!

Bibliography

[1] Dark patterns: How online companies strive to keep your money and data when you try to leave. https://techxplore.com/news/2023-10-dark-patterns-online-companies-money.html, Accessed 18-10-2023. 6

[2] Partial password usability sucks. https://gaevoy.com/2019/03/06/partial-password-sucks.html, Accessed 03-05-2023. xiv, 16

[3] Problems with the cancellation button? https://www.verbraucherzentrale.de/probleme-mit-dem-kuendigungsbutton-76779, Accessed 1-12-2022. 100, 108, 128

[4] Security theater. https://en.wikipedia.org/wiki/Security_theater, Accessed 11-08-2023. 59

[5] The seven principles. https://universaldesign.ie/what-is-universal-design/the-7-principles/the-7-principles.html, Accessed 26-06-2023. 4, 50

[6] Shoulder surfing (computer security). https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security) Accessed: 24-07-2023. 17

[7] The top 10 types of product subscriptions in 2023 and how to set yours up. https://autoship.cloud/tutorials/product-subscriptions/, Accessed 14-08-2023. 95

[8] 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) (text with eea relevance), 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj. 86

[9] Restore Online Shoppers' Confidence Act, 2019. https://www.ftc.gov/legal-library/browse/statutes/restore-online-shoppers-confidence-act, Accessed 18-7-20223. 98

[10] Children's online learning program ABCmouse to pay $10 million to settle FTC charges of illegal marketing and billing practices, 2021. https://www.ftc.gov/news-events/news/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle-ftc-charges-illegal-marketing, Accessed 17-07-2023. 92

[11] Compliance principles for anti-virus software businesses that use auto-renewing contracts, 2021. https://www.gov.uk/government/publications/compliance-principles-for-anti-virus-software-firms/compliance-principles-for-anti-virus-software-businesses-that-use-auto-renewing-contracts, Accessed 08-08-2023. 101, 116

[12] Digital Services Act: agreement for a transparent and safe online environment | News | European Parliament, 2022. https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment, Accessed 11-07-2023. 92

[13] Digital Services Act (DSA), 2022. https://enterprise.gov.ie/en/what-we-do/the-business-environment/digital-single-market/eu-digital-single-market-aspects/digital-services-act/, Accessed 03-08-2023. 6

[14] FTC action against vonage results in $100 million to customers trapped by illegal dark patterns and junk fees when trying to cancel service, 2022. https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-action-against-vonage-results-100-million-customers-

trapped-illegal-dark-patterns-junk-fees-when-trying-cancel-service, Accessed 17-07-2023. 92

[15] Preamble 61-70, Digital Services Act (DSA), 2022. https://www.eu-digital-services-act.com/Digital_Services_Act_Preamble_61_to_70.html, Accessed 03-08-2023. 6

[16] Austria challenges EU newspapers' pay-or-cookie walls, 2023. https://www.euractiv.com/section/media/news/austria-challenges-eu-newspapers-pay-or-cookie-walls/, Accessed 31-07-2023. 59

[17] EUR-Lex - 32005L0029 - EN - EUR-Lex, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029, Accessed 13-07-2023. 99

[18] EUR-Lex - 52021XC1229(05) - EN - EUR-Lex, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021XC1229%2805%29, Accessed 13-07-2023. 99, 116

[19] Expensive, boring, and wrong: Here are all the news publications people canceled and why, 2023. https://www.niemanlab.org/2021/10/expensive-boring-and-wrong-here-are-all-the-news-publications-people-canceled-and-why, Accessed 18-7-2023. 92

[20] Germany fair consumer contracts, 2023. https://www.iubenda.com/en/help/60579-germany-fair-consumer-contracts, Accessed 02-08-2023. 100

[21] Get a whole new identity at the Fake Name Generator, 2023. https://www.fakenamegenerator.com, Accessed 18-7-20223. 113

[22] Guidelines on the protection of the online consumer, 2023. https://www.acm.nl/en/publications/information-for-companies/acm-guideline/guidelines-protection-online-consumer, Accessed 02-08-2023. 100, 116

[23] Mullvad VPN — Privacy is a universal right, 2023. https://mullvad.net/en, Accessed 18-7-2023. 113

[24] Negative reinforcement? FTC proposes amending negative option rule to include click-to-cancel and other protections, 2023. https://www.ftc.gov/business-guidance/blog/2023/03/negative-reinforcement-ftc-proposes-amending-negative-option-rule-include-click-cancel-other, Accessed 14-9-2023. 98, 116

[25] "Pay or Okay", the begining of the end?, 2023. https://noyb.eu/en/pay-or-okay-tech-news-site-heisede-illegal-decides-german-dpa, Accessed 28-07-2023. 59

[26] Rules for cancelling contracts online | ACM.nl, 2023. https://www.acm.nl/en/publications/information-for-companies/acm-guideline/guidelines-protection-online-consumer/rules-cancelling-contracts-online, Accessed 14-9-2023. 100, 116

[27] Trevor Noah on Twitter, 2023. https://web.archive.org/web/20230717145148/https://twitter.com/Trevornoah/status/1616164835992944647?lang=en, Accessed 17-07-2023. xv, 92

[28] Unfair and blacklisted commercial practices - Your Europe, 2023. https://europa.eu/youreurope/citizens/consumers/unfair-treatment/unfair-commercial-practices/index_en.htm, Accessed 13-07-2023. 99

[29] Will my subscription automatically renew?, 2023. https://support.substack.com/hc/en-us/articles/360045091251-Will-my-subscription-automatically-renew-, Accessed 18-7-20223. 121

[30] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3):1–41, 2017. 58

[31] Age Action. Older people need inclusive financial services, 2022. https://www.ageaction.ie/news/2022/04/27/older-people-need-inclusive-financial-services. 51

[32] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999. 3

[33] Consumer Affairs. Consumers still complain that some companies make it hard to cancel a service, 2023. https://www.consumeraffairs.com/news/consumers-still-complain-that-some-companies-make-it-hard-to-cancel-a-service-111522.html, Accessed 11-07-2023. 92

[34] Brendon Ainsworth. One-time password (OTP) authentication methods – HOTP + TOTP. https://www.sharetru.com/blog/one-time-password-otp-authentication-methods-you-should-know-hotp-totp, Accessed 11-08-2023. 199

[35] Reed Alexander. Streamers have a Gen Z problem: New data reveals why younger subscribers are more likely to cancel as inflation forces them to choose between netflix and necessities, 2023. https://www.businessinsider.com/deloitte-survey-millennial-gen-z-cancel-streaming-subscription-inflation-2023-4, Accessed 20-04-2023. 96

[36] David Aspinall and Mike Just. "Give me letters 2, 3 and 6!": Partial password implementations and attacks. In *International Conference on Financial Cryptography and Data Security*, pages 126–143. Springer, 2013. 14, 15, 24, 26, 35, 49, 50

[37] Competition Authority and Markets. What are super-complaints? *GOV*, 2015. https://www.gov.uk/government/publications/what-are-super-complaints/what-are-super-complaints, Accessed 17-07-2023. 101

[38] Competition Authority and Markets. 'Loyalty penalty' super-complaint. *GOV*, 2020. https://www.gov.uk/cma-cases/loyalty-penalty-super-complaint, Accessed 17-07-2023. 101

[39] MM Bailey. NRCLex (2019). https://github.com/metalcorebear/NRCLex Accessed: 03-11-2021. 78

[40] ING Bank. Questions and answers about pins & log-in. https://www.ing.de/hilfe/zugang/, Accessed 16-08-2023. 16, 146

[41] Banking & Payments Federation Ireland. PSD2 is coming. are you ready? 16

[42] Luiz Adolpho Baroni, Alisson Andrey Puska, Luciana Cardoso de Castro Salgado, and Roberto Pereira. Dark patterns: Towards a socio-technical approach. In *Proceedings of the XX Brazilian Symposium on Human Factors in Computing Systems*, pages 1–7, 2021. 106

[43] Susanne Barth and Menno DT De Jong. The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. *Telematics and informatics*, 34(7):1038–1058, 2017. 58

[44] Toras Pangidoan Batubara, Syahril Efendi, and Erna Budhiarti Nababan. Analysis performance bcrypt algorithm to improve password security from brute force. In *Journal of Physics: Conference Series*, volume 1811, page 012129. IOP Publishing, 2021. 18

[45] JM Bauer, R Bergstrøm, and R Foss-Madsen. Are you sure, you want a cookie? — The effects of choice architecture on users' decisions about sharing private online data. *Computers in Human Behavior*, 120:106729, 2021. 64, 69

[46] Anne Beade. Giving more bite to EU's cookie laws. https://www.khmertimeskh.com/501294996/giving-more-bite-to-eus-cookie-laws/ Accessed: 28-05-2023. 57

[47] Rachel Bell. ecommerce and the post-brexit state of play, 2021. https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/commercial/2021/ecommerce-and-the-post-brexit-state-of-play/, Accessed 09-08-2023. 99

[48] Jon Bentley and Colin Mallows. How much assurance does a pin provide? In *International Workshop on Human Interactive Proofs*, pages 111–126. Springer, 2005. 23, 25

[49] David Berend, Shivam Bhasin, and Bernhard Jungk. There goes your pin: Exploiting smartphone sensor fusion under single and cross user setting. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–10, 2018. 27

[50] David Berend, Bernhard Jungk, and Shivam Bhasin. Guessing your pin right: Unlocking smartphones with publicly available sensor data. In *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 363–368. IEEE, 2018. 27

[51] KB Bergman. Dark patterns: Malicious interface design from a users'perspective. Master's thesis, 2021. 93, 102, 105

[52] C Bermejo Fernandez, D Chatzopoulos, D Papadopoulos, and P Hui. This website uses nudging: Mturk workers' behaviour on cookie consent notices. *ACM on Human-Computer Interaction*, 5(CSCW2):1–22, 2021. 65, 69, 80

[53] Luca Bertuzzi. EU commission sets out voluntary pledges to phase out cookies. https://www.euractiv.com/section/platforms/news/eu-commission-sets-out-voluntary-pledges-to-phase-out-cookies/ Accessed: 27-05-2023. 150

[54] Luca Bertuzzi. EU consumer department to present voluntary pledge over 'cookie fatigue'. https://www.euractiv.com/section/data-privacy/news/eu-consumer-department-to-present-voluntary-pledge-over-cookie-fatigue/ Accessed: 27-05-2023. 150

[55] Pranav Bhardwaj. What is sim jacking and what can you do to protect yourself?, 2022. https://www.makeuseof.com/what-is-sim-jacking/, Accessed 15-11-2023. 199

[56] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. Counting clicks and beeps: Exploring numerosity based haptic and audio pin entry. *Interacting with computers*, 24(5):409–422, 2012. 26

[57] Farid Binbeshr, Lip Yee Por, ML Mat Kiah, AA Zaidan, and Muhammad Imam. Secure pin-entry method using one-time pin (otp). *IEEE Access*, 11:18121–18133, 2023. 28

[58] European Data Protection Board. Report of the work undertaken by the cookie banner taskforce. https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf Accessed: 31-06-2023. 57

[59] Mike Bond and Piotr Zieliński. Decimalisation table attacks for pin cracking. Technical report, University of Cambridge, Computer Laboratory, 2003. 25

[60] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. "I am definitely manipulated, even when i am aware of it. it's ridiculous!" - dark patterns from the end-user perspective. In *Designing Interactive Systems Conference 2021*, pages 763–776, 2021. 93, 102, 105

[61] Joseph Bonneau. *Guessing human-chosen secrets*. PhD thesis, University of Cambridge, 2012. 15, 26

[62] Joseph Bonneau and Sören Preibusch. The password thicket: Technical and market failures in human authentication on the web. In *WEIS*, 2010. 147

[63] Joseph Bonneau, Sören Preibusch, and Ross Anderson. A birthday present every eleven wallets? the security of customer-chosen banking pins. In *International Conference on Financial Cryptography and Data Security*, pages 25–40. Springer, 2012. 23, 24, 25, 49

[64] Marianne Borchgrevink-Brækhus and Hallvard Moe. The burden of subscribing: How young people experience digital news subscriptions. *Journalism Studies*, 24(8):1069–1086, 2023. 107

[65] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. Tales from the dark side: privacy dark strategies and privacy dark patterns. *Proc. Priv. Enhancing Technol.*, 2016(4):237–254, 2016. 104

[66] Harry Brignull. Deceptive design, 2022. https://www.deceptive.design/, Accessed 16-08-2022. 6, 8, 95, 102, 135

[67] Martin Brinkmann. Firefox may soon reject cookie prompts automatically. https://www.ghacks.net/2023/04/17/firefox-may-interact-with-cookie-prompts-automatically-soon/ Accessed: 31-06-2023. 150

[68] Barry Brown. Studying the internet experience. *HP laboratories technical report HPL*, 49, 2001. 58

[69] M Burgess. Why Amazon's £636m GDPR fine really matters. https://www.wired.co.uk/article/amazon-gdpr-fine Accessed: 23-09-2021. 57

[70] Christoph Busch. Updating EU consumer law for the digital subscription economy. 2022. 100, 139

[71] Christopher Buschow and Christian-Mathias Wellbrock. "spotify for news"? user perception of subscription-based content platforms for news media. *Journalism and Media*, 4(1):1–15, 2022. 107

[72] Liang Cai and Hao Chen. On the practicality of motion based keystroke inference attack. In *International Conference on Trust and Trustworthy Computing*, pages 273–290. Springer, 2012. 26

[73] Caroline Cakebread. You're not alone, no one reads terms of service agreements, 2017. https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=US&IR=T, Accessed 14-07-2023. 125

[74] Ryan Calo. Digital market manipulation. *Geo. Wash. L. Rev.*, 82:995, 2013. 6

[75] Matteo Cardaioli, Stefano Cecconello, Mauro Conti, Simone Milani, Stjepan Picek, and Eugen Saraci. Hand me your {PIN}! inferring {ATM}{PINs}

of users typing with a covered hand. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1687–1704, 2022. 28

[76] Matteo Cardaioli, Mauro Conti, Kiran Balagani, and Paolo Gasti. Your pin sounds good! augmentation of pin guessing strategies via audio leakage. In *Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part I 25*, pages 720–735. Springer, 2020. 28

[77] Robin Carlsson, Sampsa Rauti, and Timi Heino. Data leaks to third parties in web services for vulnerable groups. In *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, pages 1208–1212. IEEE, 2023. 61

[78] Maria Casimiro, Joe Segel, Lewei Li, Yigeng Wang, and Lorrie Faith Cranor. A quest for inspiration: How users create and reuse pins. *Who Are You*, pages 1–7, 2020. 13, 18

[79] Consumer Centre, 2022. `https://www.verbraucherzentrale.de/probleme-mit-dem-kuendigungsbutton-76779`, Accessed 1-12-2022. 116

[80] Seunghun Cha, Jaewoo Park, Geumhwan Cho, Jun Ho Huh, and Hyoungshick Kim. Poster: Wiping: Wi-fi signal-based pin guessing attack. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1835–1837, 2016. 27

[81] Inyoung Chae, Jihyeon Ha, and David A Schweidel. Paywall suspensions and digital news subscriptions. *Marketing Science*, 42(4):729–745, 2023. 107

[82] Susan Chandler. Subscriptions still on the rise at most newspapers in the medill subscriber engagement index, 2022. `https://localnewsinitiative.northwestern.edu/posts/2022/11/21/subscriptions-increasing/index.html`, Accessed 29-11-2022. 108

[83] Sen Chen, Lingling Fan, Guozhu Meng, Ting Su, Minhui Xue, Yinxing Xue, Yang Liu, and Lihua Xu. An empirical assessment of security risks of global android banking apps. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering*, pages 1310–1322, 2020. 21

[84] Sen Chen, Ting Su, Lingling Fan, Guozhu Meng, Minhui Xue, Yang Liu, and Lihua Xu. Are mobile banking apps secure? what can be improved? In *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pages 797–802, 2018. 21

[85] Tony Chen, Ken Fenyo, Sylvia Yang, and Jessica Zhang. Thinking inside the subscription box: New research on e-commerce consumers. *McKinsey & Company*, pages 1–9, 2018. 96

[86] Weiyue Chen and Esther Thorson. Perceived individual and societal values of news and paying for subscriptions. *Journalism*, 22(6):1296–1316, 2021. 107

[87] Sonia Chiasson and Paul C Van Oorschot. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography*, 77(2):401–408, 2015. 24

[88] Shruthi Sai Chivukula, Chris Watkins, Lucca McKay, and Colin M Gray. " nothing comes before profit" asshole design in the wild. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2019. 102, 104

[89] Mark M Christiansen and Ken R Duffy. Guesswork, large deviations, and Shannon entropy. *IEEE transactions on information theory*, 59(2):796–802, 2012. 47

[90] Google Chrome. Building a more private, open web. https://privacysandbox.com/ Accessed: 15-12-2021. 149

[91] Michael Chromik, Malin Eiband, Sarah Theres Völkel, and Daniel Buschek. Dark patterns of explainability, transparency, and user control for intelligent systems. In *IUI workshops*, volume 2327, 2019. 104

[92] Hsiang Iris Chyi and Yee Man Margaret Ng. Still unwilling to pay: An empirical analysis of 50 us newspapers' digital subscription results. *Digital journalism*, 8(4):526–547, 2020. 107

[93] Citizens Information. Charter of fundamental rights. https://www.citizensinformation.ie/en/government-in-ireland/data-protection/rights-under-general-data-protection-regulation/ Accessed: 27-09-2021. 56

[94] James M Clarke, Maryam Mehrnezhad, and Ehsan Toreini. Invisible, unreadable, and inaudible cookie notices: An evaluation of cookie notices for users with visual impairments. *ACM Transactions on Accessible Computing*, 17(1):1–39, 2024. 60, 81

[95] CMA. CMA secures refund rights for McAfee customers, 2021. https://www.gov.uk/government/news/cma-secures-refund-rights-for-mcafee-customers, Accessed 28-11-2022. 101

[96] CMA. Norton extends refund rights after CMA action, 2021. https://www.gov.uk/government/news/norton-extends-refund-rights-after-cma-action, Accessed 28-11-2022. 101

[97] Federal Trade Commision. Federal trade commission proposes rule provision making it easier for consumers to "click to cancel" recurring subscriptions and memberships, 2023. https://www.ftc.gov/news-events/news/press-releases/2023/03/federal-trade-commission-proposes-rule-provision-making-it-easier-consumers-click-cancel-recurring,Accessed 03/07/2023. 92, 93

[98] Federal Trade Commision. FTC takes action against amazon for enrolling consumers in amazon prime without consent and sabotaging their attempts to cancel, 2023. https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their, Accessed 27-06-2023. 92

[99] European Commission. Consumer protection: Amazon prime changes its cancellation practices to comply with EU consumer rules, 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4186, Accessed 07-07-2023. 92, 97

[100] Federal Trade Commission. Federal trade commission act, 2006. https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act, Accessed 30-11-2022. 98

[101] Federal Trade Commission. FTC to ramp up enforcement against illegal dark patterns that trick or trap consumers into subscriptions, 2021. https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions, Accessed 10-8-2022. 98

[102] Competition and Consumer portection Commission. CCPC participates in EU-wide sweep of websites to identify dark patterns, 2023. https://www.ccpc.ie/business/ccpc-participates-in-eu-wide-sweep-of-websites-to-identify-dark-patterns/, Accessed 16-08-2023. 148

[103] Finnish Competition and Consumer Authority. FCCA report: Consumers loose millions of euros each year due to subscription traps, 2018. https://www.kkv.fi/en/current/press-releases/fcca-report-consumers-lose-millions-of-euros-each-year-due-to-subscription-traps/, Accessed 17-08-2022. 92

[104] Intersoft Consulting. GDPR-definitions. https://gdpr-info.eu/art-4-gdpr/ Accessed: 31=05-23. 57, 80

[105] Reddit contributors. reddit.com: search results - cancel subscription, 2023. https://web.archive.org/web/20230711205425/https://www.reddit.com/r/assholedesign/search/?q=cancel%20subscription&restrict_sr=1, Accessed 11-07-2023. 92

[106] Contributors to Wikimedia projects. Amazon Prime - Wikipedia, 2023. https://en.wikipedia.org/w/index.php?title=Amazon_Prime, Accessed 14-9-2023. 96

[107] Contributors to Wikimedia projects. Substack - Wikipedia, 2023. https://en.wikipedia.org/w/index.php?title=Substack&oldid=1164027880, Accessed 17-07-2023. 112

[108] CookieYes. Cookie wall: Is it gdpr compliant?, 2023. https://www.cookieyes.com/blog/cookie-wall/, Accessed 15-11-2023. 59

[109] The Norwegian Consumer Council. You can log out, but you can never leave, 2021. https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf, Accessed 11-07-2023. 92

[110] Cobb & Counsel. Why is it so hard to cancel subscription services?, 2022. https://cobbxcounsel.com/2022/03/why-is-it-so-hard-to-cancel-subscription-services/, Accessed 31-05-2023. 99

[111] Court of Justice of the European Union. Panet49 case ruling. https://curia.europa.eu/juris/document Accessed: 18-10-2021. 81, 86

[112] M. Pei D. M'Raihi, S. Machani and J. Rydell. TOTP: Time-based one-time password algorithm. https://datatracker.ietf.org/doc/html/rfc6238?ref=blog.passwork.pro#page-6, Accessed 11-08-2023. 199

[113] Data Protection Commission. Report by the Data Protection Commission on the use of cookies and other tracking technologies. https://www.dataprotection.ie/en/news-media/press-releases/report-dpc-use-cookies-and-other-tracking-technologies Accessed: 18-10-2021. 63, 64, 79, 80, 86, 87, 148

[114] Heidar Davoudi, Morteza Zihayat, and Aijun An. Time-aware subscription prediction model for user acquisition in digital news media. In *Proceedings of the 2017 SIAM International Conference on Data Mining*, pages 135–143. SIAM, 2017. 107

[115] Alexander De Luca, Katja Hertzschuch, and Heinrich Hussmann. Colorpin: Securing pin entry through indirect input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1103–1106, 2010. 25

[116] M Degeling, C Utz, C Lentzsch, He Hosseini, F Schaub, and T Holz. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. *arXiv preprint arXiv:1808.05096*, 2018. 62, 67

[117] NDP Delivery Department of Public Expenditure and Reform. Digital for good: Ireland's digital inclusion roadmap, 2023. `https://www.gov.ie/en/publication/b90af-digital-for-good-irelands-digital-inclusion-roadmap/`. 3, 8

[118] Devoteam. Ensuring cybersecurity with cookies: Best practices and tips. `https://www.devoteam.com/expert-view/cybersecurity-cookies/`, Accessed: 26-08-2024. 154

[119] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. UI dark patterns and where to find them: a study on mobile applications and user perception. In *Proceedings of the 2020 CHI conference on human factors in computing systems*, pages 1–14, 2020. 93, 102

[120] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. Ui dark patterns and where to find them: a study on mobile applications and user perception. In *Proceedings of the 2020 CHI conference on human factors in computing systems*, pages 1–14, 2020. 104

[121] Ken R Duffy. Guesswork. *London Mathematical Society Newsletter*, 497:30–35, 2021. 47

[122] Chris Eastham. Changes to consumer subscription contracts, 2023. `https://www.fieldfisher.com/en/insights/changes-to-consumer-subscription-contracts`, Accessed 14-09-2023. 93

[123] Liran Einav, Benjamin Klopack, and Neale Mahoney. Selling subscriptions. Technical report, National Bureau of Economic Research, 2023. 96, 103

[124] Liran Einav, Benjamin Klopack, and Neale Mahoney. Selling subscriptions. Technical report, National Bureau of Economic Research, 2023. 106

[125] S Englehardt and A Narayanan. Online tracking: A 1-million-site measurement and analysis. In *2016 ACM SIGSAC conference on computer and communications security*, pages 1388–1401, 2016. 62, 67

[126] S Englehardt and A Narayanan. Online tracking: A 1-million-site measurement and analysis. In *ACM CCS 2016*, 2016. 70

[127] Lukas Erbrich, Christian-Mathias Wellbrock, Frank Lobigs, and Christopher Buschow. Bundling digital journalism: Exploring the potential of subscription-based product bundles. *Media and Communication*, 12, 2024. 107

[128] Polly Mackenzie & Katie Evans. Subscription retail: an expensive trap, 2017. http://www.moneyandmentalhealth.org/wp-content/uploads/2017/04/20170306-Subscription-retail-paper-3.pdf, Accessed 28-11-2022. 97

[129] Security For Everyone. Top 10 open source web crawler in 2024, 2024. https://www.linkedin.com/pulse/top-10-open-source-web-crawler-2024-secforeveryone-wq1mf/. 70

[130] faegredrinker. Automatic renewal laws in all 50 states: An updated guide, 2018. https://www.faegredrinker.com/en/insights/publications/2018/8/automatic-renewal-laws-in-all-50-states-an-updated-guide, Accessed 30-11-2022. 113

[131] Richard Fletcher and Rasmus Kleis Nielsen. Paying for online news: A comparative analysis of six countries. *Digital Journalism*, 5(9):1173–1191, 2017. 107

[132] Sara Fischer & Kerry Flynn. Google gives up trying to eliminate cookies. https://www.axios.com/2024/07/22/google-chrome-keeps-cookie-policy. 149

[133] Riccardo Focardi and Flaminia L Luccio. Guessing bank PINs by winning a mastermind game. *Theory of Computing Systems*, 50(1):52–71, 2012. 23, 25, 30

[134] Department for Business and Trade. Digital markets, competition and consumers bill, 2023. https://publications.parliament.uk/pa/bills/cbill/58-03/0294/220294.pdf, Accessed 29/06/2023. 101

[135] The Netherlands Authority for Consumers and Markets. Consumers should be able to cancel online any subscriptions that have been taken out online, 2021. https://www.acm.nl/en/publications/acm-consumers-should-be-able-cancel-online-any-subscriptions-have-been-taken-out-online, Accessed 22/11/2022. 109

[136] European Union Agency for Cybersecurity. What are cookies ? https://www.enisa.europa.eu/about-enisa/cookies, Accessed 11-08-2023. 8

[137] I Fouad, C Santos, F Al Kassar, N Bielova, and S Calzavara. On compliance of cookie purposes with the purpose specification principle. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 326–333. IEEE, 2020. 62, 68

[138] M Fredrikson and B Livshits. Repriv: Re-imagining content personalization and in-browser privacy. In *2011 IEEE Symposium on Security and Privacy*, pages 131–146. IEEE, 2011. 150

[139] Natasha Frost. Why call-to-cancel policies are an accessibility nightmare, 2022. https://www.modernretail.co/retailers/why-call-to-cancel-policies-are-an-accessibility-nightmare/, Accessed 14-07-2023. 97

[140] Alexander Gebhard. Germany: New provisions for consumer contracts, 2021. https://brsa.lawfed.com/germany-new-provisions-for-consumer-contracts/, Accessed 30-11-2022. 100, 116

[141] D Geradin, D Katsifis, and T Karanikioti. Google as a de facto privacy regulator: analysing the privacy sandbox from an antitrust perspective. *European Competition Journal*, pages 1–65, 2021. 149

[142] Nadine Ghiran. Subscriptions are reshaping industries during the pandemic, 2021. https://subta.com/subscriptions-are-reshaping-industries-during-the-pandemic/,Accessed 30/06/2023. 96

[143] Lais Glaser. What is the optimal unsubscribing journey for paid video streaming services? Master's thesis, 2022. Utrecht Uinversity. 103, 106

[144] Lomas Gong, Mark A Lomas, Roger M Needham, and Jerome H Saltzer. Protecting poorly chosen secrets from guessing attacks. *IEEE journal on Selected Areas in Communications*, 11(5):648–656, 1993. 25

[145] PAJ Graßl, HK Schraffenberger, FJ Zuiderveen Borgesius, and MA Buijzen. Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, 3(1), 2021. 65, 69, 86

[146] CM Gray, C Santos, N Bielova, M Toth, and D Clifford. Dark patterns and the legal requirements of consent banners: an interaction criticism perspective. In *2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2021. 86, 106

[147] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–14, 2018. 96, 102, 104

[148] Marthie Grobler, Raj Gaire, and Surya Nepal. User, usage and usability: Redefining human centric cyber security. *Frontiers in big Data*, 4:583723, 2021. 3

[149] Nicolas Gueguen and Alexandre Pascual. Evocation of freedom and compliance: The "but you are free of..." technique. *Current research in social psychology*, 5(18):264–270, 2000. 58

[150] S Guha, B Cheng, and P Francis. Privad: Practical privacy in online advertising. In *USENIX conference on Networked systems design and implementation*, pages 169–182, 2011. 150

[151] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. A comparative study of dark patterns across web and mobile modalities. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–29, 2021. 106

[152] H Habib, Y Zou, A Jannu, N Sridhar, C Swoopes, A Acquisti, LF Cranor, N Sadeh, and F Schaub. An empirical analysis of data deletion and opt-out choices on 150 websites. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, pages 387–406, 2019. 65, 67, 79

[153] Hana Habib and Lorrie Faith Cranor. Evaluating the usability of privacy choice mechanisms. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 273–289, 2022. 60

[154] Andrew J. Hawkins. The future of cars is a subscription nightmare. `https://www.theverge.com/2022/7/13/23206999/car-subscription-nightmare-heated-seats-remote-start`, Accessed 14-08-2023. 96

[155] Sameer Hayikader, FN Hadi, and Jamaludin Ibrahim. Issues and security measures of mobile banking apps. *International Journal of Scientific and Research Publications*, 6(1):36–41, 2016. 21

[156] Kirsi Helkala. Disabilities and authentication methods: Usability and security. In *2012 Seventh International Conference on Availability, Reliability and Security*, pages 327–334. IEEE, 2012. xiv, 19, 20

[157] Annette Groen & Nanne Houtsma. Subscription report 2021, 2021. `https://www.nibud.nl/onderzoeksrapporten/rapport-abonnementen-2021/`, Accessed 15-06-2023. 109

[158] Mark Huffman. Consumers still complain that some companies make it hard to cancel a service, 2022. `https://www.consumeraffairs.com/news/consumers-still-complain-that-some-companies-make-it-hard-to-cancel-a-service-111522.html`, Accessed 12-07-2023. 92

[159] Jun Ho Huh, Hyoungshick Kim, Rakesh B Bobba, Masooda N Bashir, and Konstantin Beznosov. On the memorability of system-generated pins: Can chunking help? In *SOUPS*, volume 15, pages 197–209, 2015. 20

[160] Imperva. Credential stuffing. `https://www.imperva.com/learn/application-security/credential-stuffing`, Accessed: 05-07-2024. 18

[161] Mariia Iskorkina. Are free subscription trials more effective than paid ones?, 2021. https://whatsnewinpublishing.com/are-free-subscription-trials-more-effective-than-paid-ones/, Accessed 25-04-2023. 109

[162] Luiza Jarovsky. Transparency by design: Reducing informational vulnerabilities through ux design. *Available at SSRN 4119284*, 2022. 3

[163] Jeff Johnson and Kate Finn. *Designing user interfaces for an aging population: Towards universal design*. Morgan Kaufmann, 2017. 4

[164] Nathan Jolly. Opinionremember when you only had to buy things once? subscriptions are killing us in a cost-of-living crisis. https://mumbrella.com.au/the-weekend-mumbo-remember-when-you-only-had-to-buy-things-once-subscriptions-are-killing-us-in-a-cost-of-living-crisis-836519, Accessed: 18-09-2024. 153

[165] Ellen Judson and Victoria Baines. Accept all: Unacceptable? Tracking the experience of trying to reclaim personal data - and what government, businesses and citizens can learn from it. https://demos.co.uk/wp-content/uploads/2023/04/accept-all-unacceptable-demos-march-2023.pdf Accessed: 26-05-2023. 66

[166] Charles Jun. I canceled 22 digital newspaper subscriptions. here's what i learned about digital retention strategies, 2023. https://www.lenfestinstitute.org/solutions-resources/i-canceled-22-digital-newspaper-subscriptions-heres-what-i-learned-about-digital-retention-strategies/. 108

[167] Junade Ali. Banking-grade credential stuffing: The futility of partial password validation. 18, 19

[168] G Kampanos and SF Shahandashti. Accept all: The landscape of cookie banners in Greece and the UK, 2021. 8, 62, 68, 70, 71, 78, 86, 89, 147

[169] Erol Kazan, Tuure Tuunanen, Hadi Ghanbari, and Mengcheng Li. The design towards a news aggregator subscription service: Results from an online

experiment. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. University of Hawai'i at Manoa, 2021. 107

[170] Ansgar Kellner, Micha Horlboge, Konrad Rieck, and Christian Wressnegger. False sense of security: A study on the effectivity of jailbreak detection in banking apps. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 1–14. IEEE, 2019. 21

[171] Nicole Kar & Elisha Kemp. The trial period is over: updated consumer laws for the digital economy, 2022. https://www.linklaters.com/en/insights/blogs/linkingcompetition/2022/june/the-trial-period-is-over_updated-consumer-laws-for-the-digital-economy, Accessed 28-11-2022. 109

[172] Hassan Khan, Jason Ceci, Jonah Stegman, Adam J Aviv, Rozita Dara, and Ravi Kuber. Widely reused and shared, infrequently updated, and sometimes inherited: A holistic view of pin authentication in digital lives and beyond. In *Annual Computer Security Applications Conference*, pages 249–262, 2020. 18

[173] Hyoungshick Kim and Jun Ho Huh. Pin selection policies: Are they really effective? *computers & security*, 31(4):484–496, 2012. 25

[174] Su Jung Kim, Xiaohan Wang, and Edward C Malthouse. Digital news readership and subscription in the united states during covid-19: A longitudinal analysis of clickstream and subscription data from a local news site. *Digital Journalism*, 10(6):1015–1036, 2022. 107

[175] Chris Kimble. ICO takes action against deceptive cookie banners. https://www.talk-finance.co.uk/moderntech/ico-takes-action-against-deceptive-cookie-banners/, Accessed 14-08-2023. 61

[176] Daniel Kirkwood, Cagdas Tombul, Calum Firth, Finn Macdonald, Konstantinos Priftis, Florian Mathis, Mohamed Khamis, and Karola Marky. Pin scrambler: Assessing the impact of randomized layouts on the usability and security of pins. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia*, pages 83–88, 2022. 28

[177] Donald E Knuth. The computer as Master Mind. *Journal of Recreational Mathematics*, 9(1):1–6, 1976. 23

[178] R Koch. Cookies, the GDPR, and the eprivacy directive. https://gdpr.eu/cookies/ Accessed: 29-10-2021. 54

[179] Leonie Schneider Konstantin Ewald and Felix Hilgert. Enforcement alert: "termination button" in Germany, 2022. https://gameslaw.org/enforcement-alert-termination-button-in-germany/, Accessed 1-12-2022. 108

[180] Robert V Krejcie and Daryle W Morgan. Determining sample size for research activities. *Educational and psychological measurement*, 30(3):607–610, 1970. 74

[181] Kristina Ehle & Stephen Kreß. New "two-click cancellation" button – german exceptionalism for subscription terminations, 2021. https://www.mofo.com/resources/insights/211006-new-two-click-cancellation-button, Accessed 04-09-2023. 92, 100

[182] Ch Krisam, He Dietmann, M Volkamer, and O Kulyk. Dark patterns in the wild: Review of cookie disclaimer designs on top 500 german websites. In *European Workshop on Usable Security (EuroUSEC)*, 2021. 57, 65, 69, 79, 86, 147

[183] Markus Kuhn. Probability theory for pickpockets—ec-PIN guessing. In *Workshop on Cryptography and Network Security. DIMACS Research and Education Institute*, 1997. 23, 48

[184] O Kulyk, A Hilt, N Gerber, and M Volkamer. "This website uses cookies": Users' perceptions and reactions to the cookie disclaimer. In *European Workshop on Usable Security (EuroUSEC)*, 2018. 54, 55

[185] Thomas Köhler. Cookie consent: Most popular tools in 2023, 2023. https://www.experte.com/website/cookie-consent, Accessed 27-10-2023. 60

[186] Inclusion & Accessibilty Labs. Ia labs launches digital accessibility index 2023, 2023. https://ialabs.ie/ia-labs-launches-dai-2023/. 3

[187] V Le Pochat, T Van Goethem, S Tajalizadehkhoob, M Korczyński, and W Joosen. Tranco: A research-oriented top sites ranking hardened against manipulation. In *26th Annual Network and Distributed System Security Symposium*, NDSS 2019, February 2019. 72

[188] Mun-Kyu Lee. Security notions and advanced method for human shoulder-surfing resistant pin-entry. *IEEE transactions on information forensics and security*, 9(4):695–708, 2014. 26

[189] Jiange Li. Large deviations for conditional guesswork. *Statistics & Probability Letters*, 153:7–14, 2019. 47

[190] ZS Li, C Werner, N Ernst, and D Damian. GDPR compliance in the context of continuous integration. *arXiv preprint arXiv:2002.06830*, 2020. 63, 68

[191] Irish Council For Civil Liberties. Europe's enforcement paralysis, 2021. https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf. 59

[192] Ximing Liu, Yingjiu Li, Robert H Deng, Bing Chang, and Shujun Li. When human cognitive modeling meets pins: User-independent inter-keystroke timing attacks. *Computers & Security*, 80:90–107, 2019. 27

[193] Alex Lomas. Partial passwords, 2018. https://www.alexlomas.com/blog/2018/04/partial-passwords/. 18

[194] Jamie Luguri and Lior Jacob Strahilevitz. Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1):43–109, 2021. 102, 105

[195] Jenna Lyons. eHarmony to pay out millions in settlement to customers. 2018. https://www.sfgate.com/bayarea/article/eHarmony-to-pay-out-millions-in-settlement-to-12485546.php, Accessed 17-07-2023. 92

[196] Aditi M. Bhoot, Mayuri A. Shinde, and Wricha P. Mishra. Towards the identification of dark patterns: An analysis based on end-user reactions. In *In-*

diaHCI'20: Proceedings of the 11th Indian Conference on Human-Computer Interaction, pages 24–33, 2020. 102, 105

[197] Dominique Machuletz and Rainer Böhme. Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *arXiv preprint arXiv:1908.10048*, 2019. 64, 66, 67, 68

[198] David Mack. The sneaky sticker shock of subscription culture, 2023. https://www.nytimes.com/2023/11/19/opinion/subscriptions-netflix-apple-cost.html, Accessed 15-11-2023. 152

[199] Maximilian Maier. Dark patterns–an end user perspective, 2019. 104

[200] Maximilian Maier and Rikard Harr. Dark design patterns: An end-user perspective. *Human Technology*, 16(2):170, 2020. 93, 102

[201] Anil Malhotra. Subscription wars: the subscriber strikes back, 2022. https://mobile-magazine.com/articles/72-believe-there-are-too-many-subscription-services-72, Accessed 03-05-2023. 92

[202] David Malone and Kevin Maher. Investigating the distribution of password choices. In *Proceedings of the 21st international conference on World Wide Web*, pages 301–310, 2012. 22, 49

[203] Laura Koewler Marion. Automatic renewal laws in all 50 states, 2019. https://www.faegredrinker.com/-/media/files/collateral-pieces/automatic-renewal-laws-in-all-50-states-march-26-2019.pdf, Accessed 30-11-2022. 99

[204] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. This PIN can be easily guessed: Analyzing the security of smartphone unlock PINs. In *IEEE Symposium on Security and Privacy*, SP '20, pages 1525–1542, San Francisco, California, USA, May 2020. IEEE. xii, 15, 23, 28

[205] David Martínez, Eusebi Calle, Albert Jové, and Cristina Pérez-Solà. Web-tracking compliance: websites' level of confidence in the use of information-

gathering technologies. *Computers & Security*, 122:102873, 2022. 62, 70, 147

[206] Arunesh Mathur, Gunes Acar, Michael J Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–32, 2019. xiii, 6, 93, 102, 104, 134, 135

[207] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI conference on human factors in computing systems*, pages 1–18, 2021. 6, 64, 101, 102, 105, 155

[208] C Matte, N Bielova, and C Santos. Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 791–809. IEEE, 2020. 63, 68, 81

[209] Carter McCants. Canceling difficult cancellation: An analysis of recent regulatory efforts to make canceling subscriptions easier. *Wm. & Mary Bus. L. Rev.*, 14:463, 2022. 95, 96, 98, 99, 124

[210] Aleecia M McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *Isjlp*, 4:543, 2008. 66

[211] Katharine Miller. Can't unsubscribe? blame dark patterns. `https://hai.stanford.edu/news/cant-unsubscribe-blame-dark-patterns`, Accessed 14-08-2023. 97

[212] Klaus M Miller, Navdeep S Sahni, and Avner Strulov-Shlain. Sophisticated consumers with inertia: Long-term implications from a large-scale field experiment. *Available at SSRN 4065098*, 2023. 103, 106

[213] Wendy Moncur and Greogry Leplatre. Pins, passwords and human memory. *Digital Evidence & Elec. Signature L. Rev.*, 6:116, 2009. 19

[214] Alberto Monge Roffarello and Luigi De Russis. Towards understanding the dark patterns that steal our attention. In *Chi conference on human factors in computing systems extended abstracts*, pages 1–7, 2022. 106

[215] Victor Morel, Cristiana Santos, Yvonne Lintao, and Soheil Human. Your consent is worth 75 euros a year-measurement and lawfulness of cookie paywalls. In *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, pages 213–218, 2022. xvi, 127, 128

[216] B Morrison, C Sengul, M Springett, J Taylor, and K Renaud. Mental models of dark patterns. https://spritehub.org/2021/12/08/revealing-young-learners-mental-models-project-team-publish-white-paper Accessed: 9-12-2021. 85

[217] Theodosis Mourouzis, Marcin Wojcik, and Nikos Komninos. On the security evaluation of partial password implementations. *arXiv preprint arXiv:1701.00104*, 2016. 18, 27

[218] Paul Scully MP. New rules to protect consumers' hard-earned cash, 2022. https://www.gov.uk/government/news/new-rules-to-protect-consumers-hard-earned-cash, Accessed 22-11-2022. 101

[219] Rt Hon Kwasi Kwarteng MP. Reforming competition and consumer policy: government response, 2022. https://www.gov.uk/government/consultations/reforming-competition-and-consumer-policy/outcome/reforming-competition-and-consumer-policy-government-response, Accessed 23-11-2022. 101, 109

[220] Coimisiún na Meán. Digital news report ireland 2024, 2024. https://www.cnam.ie/dnr-2024/. 107

[221] Jun-mo Nam. Sample size determination for case-control studies and the comparison of stratified and unstratified analyses. *Biometrics*, pages 389–395, 1992. 74

[222] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. Dark patterns: Past, present, and future: The evolution of tricky user interfaces. *Queue*, 18(2):67–92, 2020. 105

[223] L Narayanan. *Cookies'n'consent: An empirical study on the factors influencing customer attitudes towards cookie consent among Internet users in EU.* PhD thesis, Dublin Business School, 2020. 55, 149

[224] Szymon Grzesiak Natalia Chronowska. Comparison of 10 leading consent management platforms, 2024. https://piwik.pro/blog/consent-management-platforms-comparison/. 60

[225] United Nations. World population ageing, 2017. https://www.un.org/en/development/desa/population/publications/pdf/ageing/WPA2017_Report.pdf. 3

[226] Efrat Nechushtai and Lior Zalmanson. 'stay informed','become an insider'or 'drive change': Repackaging newspaper subscriptions in the digital age. *Journalism*, 22(8):2035–2052, 2021. 107

[227] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI conference on human factors in computing systems*, pages 1–13, 2020. 66, 86

[228] Mia Nummila. Consumers' attitudes towards data privacy: differences between younger and older consumers. 2019. 154

[229] DaeHun Nyang, Hyoungshick Kim, Woojoo Lee, Sung-bae Kang, Geumhwan Cho, Mun-Kyu Lee, and Aziz Mohaisen. Two-thumbs-up: Physical protection for pin entry secure against recording attacks. *computers & security*, 78:1–15, 2018. 27

[230] Federal Office of Justice, 2021. https://www.gesetze-im-internet.de/englisch_bgb/, Accessed 30-11-2022. 116

[231] Federal Office of Justice. German civil code, 2021. https://www.gesetze-im-internet.de/englisch_bgb/, Accessed 30-11-2022. 100

[232] International Federation of Periodical Publishers. Global digital subscription snapshot, 2022. https://www.fipp.com/wp-content/uploads/2022/06/GDS-Snapshot-Q2-2022.pdf, Accessed 02-01-2023. 112

[233] International Federation of Periodical Publishers. Global digital subscription snapshot (2022 q4), 2022. https://www.fipp.com/resource-type/global-digital-subscription-snapshot/, Accessed 02-01-2023. 112, 141

[234] Trinity School of Social Work and Social Policy. Research with groups at risk of vulnerability and sensitive topics, 2023. https://www.tcd.ie/swsp/research/vulnerable-groups.php. 10

[235] United States District Court Western District of Washington. Complaint for permanent injunction, civil penalties, monetary relief, and other equitable relief, 2023. https://www.ftc.gov/system/files/ftc_gov/pdf/amazon-rosca-public-redacted-complaint-to_be_filed.pdf, Accessed 28-06-2023. 96, 97

[236] None of Your Business. "pay or okay" on tech news site heise.de illegal decides german dpa. https://noyb.eu/en/pay-or-okay-tech-news-site-heisede-illegal-decides-german-dpa Accessed: 28-05-2023. 59

[237] Online official information on GDPR. 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1685467979294 Accessed: 31-08-2021. 56

[238] Carlton Daniel & Ailin O'Flaherty. Consumer law focus: Subscription auto-renewals, new CMA guidance, 2022. https://www.iptechblog.com/2022/02/consumer-law-focus-subscription-auto-renewals-new-cma-guidance/, Accessed 28-11-2022. 101

[239] National Commission on Informatics and 2020. Liberty (CNIL). Shaping choices in the digital world. https://www.cnil.fr/sites/default/

files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf, Accessed 11-4-2023. 58, 63

[240] John L O'Neill. Accessibility for all abilities: How universal design, universal design for learning, and inclusive design combat inaccessibility and ableism. *J. Open Access L.*, 9:1, 2021. 156

[241] World Health Organisation. Active ageing a policy framework, 2002. https://iris.who.int/bitstream/handle/10665/67215/WHO?sequence=1#page=19.10. 3

[242] Şebnem Özdemir. Digital nudges and dark patterns: The angels and the archfiends of digital communication. *Digital Scholarship in the Humanities*, 35(2), 2020. 65

[243] E Papadogiannakis, P Papadopoulos, N Kourtellis, and EP Markatos. User tracking in the post-cookie era: How websites bypass GDPR consent to track users. In *Web Conference 2021*, pages 2130–2141, 2021. 63, 69

[244] Adithya Pattabhiramaiah, Eric Overby, and Lizhen Xu. Spillovers from online engagement: how a newspaper subscriber's activation of digital paywall access affects her retention and subscription revenue. *Management Science*, 68(5):3528–3548, 2022. 107

[245] C Pope. 400 yes, 400! Irish retailers for all your online christmas shopping. https://www.irishtimes.com/news/consumer/400-yes-400-irish-retailer-for-all-your-online-christmas-shopping, Accessed 27-8-2021. 55

[246] B Power. Shop local from food to fashion to fitness: County by county guide to the best Irish websites for supporting local businesses this Christmas. https://www.independent.ie/irish-news/from-food-to-fashion-to-fitness-county-by-county-guide-to-the-best-irish-websites-for-supporting-local-businesses-this-christmas, Accessed: 27-8-2021. 55

[247] Owen Ray. Tracking cookies are dead: What marketers can do about it. https://www.invoca.com/blog/tracking-cookies-are-dead-what-marketers-can-do-about-it Accessed: 01-09-2021. 54

[248] Recurly. Study on subscription services: Large majority of German consumers pay up to EUR 100 a month, 2022. https://recurly.com/press/german-consumers-pay/, Accessed 31-05-2023. 109

[249] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A usability study of five {two-factor} authentication methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 357–370, 2019. 199

[250] Karen Renaud, Kenneth C Scott-Brown, and Andrea Szymkowiak. Designing authentication with seniors in mind. 2018. 51

[251] Opinium Research. Usage of subscription services: key findings of survey (opinium, november 2021), 2023. https://www.gov.uk/government/publications/subscriptions-types-offered-by-business-and-numbers-held-by-consumers/usage-of-subscription-services-key-findings-of-survey-opinium-november-2021, Accessed 02-06-2023. 110

[252] Gerard Reynolds and Seamus Dowling. An analysis of ireland's homecare companies' cookie practices in terms of gdpr compliance. In *2022 Cyber Research Conference-Ireland (Cyber-RCI)*, pages 1–7. IEEE, 2022. 61

[253] Christine Rigden. 'the eye of the beholder'-designing for colour-blind users. *British Telecommunications Engineering*, 17:291–295, 1999. 81

[254] Chelsea Ritschel. 'Really and truly scammed me': Rihanna's lingerie company Savage X Fenty accused of deceptive marketing. *Independent*, 2020. https://www.independent.co.uk/life-style/rihanna-lingerie-savage-x-fenty-scam-reviews-a9334071.html, Accessed 17-07-2023. 92

[255] Dr Craig T. Robertson. How much do people pay for online news? and what might encourage more people to pay? https://reutersinstitute.

politics.ox.ac.uk/digital-news-report/2024/how-much-do-people-pay-online-news-what-might-encourage-others-pay. 108

[256] RocketMoney. The money app that works for you, 2023. https://www.rocketmoney.com/, Accessed 28/02/2023. xv, 95

[257] Claire Quinn & Celeste Rollason. Cookies, consent & children prove a challenge. https://www.privo.com/blog/cookies-consent-children-prove-a-challenge, Accessed: 26-09-2024. 154

[258] Wilson Sonsini Goodrich & Rosati. Amended california automatic renewal law (ARL) takes effect in 2022, 2021. https://www.jdsupra.com/legalnews/amended-california-automatic-renewal-6661081/, Accessed 03-07-2023. 99

[259] Volker Roth, Kai Richter, and Rene Freidinger. A pin-entry method resilient against shoulder surfing. In *Proceedings of the 11th ACM conference on Computer and communications security*, pages 236–245, 2004. 25

[260] I Sanchez-Rola, M Dell'Amico, P Kotzias, D Balzarotti, L Bilge, P-A Vervier, and I Santos. Can I opt out yet? GDPR and the global illusion of cookie control. In *ACM Asia Conference on Computer and Communications Security*, pages 340–351, 2019. 85

[261] C Santos, N Bielova, and C Matte. Are cookie banners indeed compliant with the law? deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *arXiv preprint arXiv:1912.07144*, 2019. 60, 62, 67

[262] Cristiana Santos, Arianna R, Lorena S Chamorro, K Bongard-Blanchy, and R Abu-Salma. Cookie banners, what's the purpose? Analyzing cookie banner text through a legal lens. *arXiv preprint arXiv:2110.02597*, 2021. 62, 69, 79, 80

[263] Florian Schaub and Lorrie Faith Cranor. Usable and useful privacy interfaces. *An introduction to privacy for technology professionals*, pages 176–299, 2020. 60

[264] Stuart Schechter and Joseph Bonneau. Learning assigned secrets for unlocking mobile devices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 277–295, 2015. 26

[265] Barry Schwartz. *The paradox of choice: Why more is less*. Harper Perenial, 2004. 61

[266] Paola Serafino. Exploring the uk's digital divide, 2019. https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/articles/exploringtheuksdigitaldivide/2019-03-04. 3

[267] Akash Sharma, Sunil K Singh, Sudhakar Kumar, Anureet Chhabra, and Saksham Gupta. Security of android banking mobile apps: Challenges and opportunities. In *International Conference on Cyber Security, Privacy and Networking*, pages 406–416. Springer, 2021. 21

[268] Ashley Sheil, Gunes Acar, Hanna Schraffenberger, Raphaël Gellert, and David Malone. Staying at the roach motel: Cross-country analysis of manipulative subscription and cancellation flows. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2024. 107

[269] Ashley Sheil and David Malone. Fianán, cuacha: Irish cookie banners. In *2022 33rd Irish Signals and Systems Conference (ISSC)*, pages 1–8. IEEE, 2022. 70

[270] Ashley Sheil and David Malone. Guessing pins, one partial pin at a time. *Entropy*, 24(9):1224, 2022. 28

[271] Diksha Shukla, Rajesh Kumar, Abdul Serwadda, and Vir V Phoha. Beware, your hands reveal your secrets! In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 904–917, 2014. 26

[272] Laurent Simon and Ross Anderson. Pin skimmer: Inferring pins through the camera and microphone. In *Proceedings of the Third ACM workshop on*

Security and privacy in smartphones & mobile devices, pages 67–78, 2013. 26

[273] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. Circumvention by design-dark patterns in cookie consent for online news outlets. In *Proceedings of the 11th nordic conference on human-computer interaction: Shaping experiences, shaping society*, pages 1–12, 2020. 61, 65, 66, 68

[274] Jeff Sonderman and Gwen Vargo. What news publishers do to retain subscribers, 2021. https://www.americanpressinstitute.org/publications/reports/survey-research/what-news-publishers-do-to-retain-subscribers/, Accessed 22-11-2022. 107, 108

[275] J Sørensen and S Kosta. Before and after GDPR: The changes in third party presence at public and private european websites. In *The World Wide Web Conference*, pages 1590–1600, 2019. 54, 71

[276] Raphael Spreitzer. Pin skimming: exploiting the ambient-light sensor in mobile devices. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, pages 51–62, 2014. 26

[277] Rajarajan Srinivasan. Dragpin: A secured pin entry scheme to avert attacks. *Int. Arab J. Inf. Technol.*, 15(2):213–223, 2018. 27

[278] Brave standards team. "web environment integrity": Locking down the web, 2023. https://brave.com/web-standards-at-brave/9-web-environment-integrity/, Accessed 01-11-2023. 155

[279] L'ubica Staneková and Martin Stanek. Analysis of dictionary methods for pin selection. *Computers & security*, 39:289–298, 2013. 25

[280] Graham Steel. Formal analysis of pin block attacks. *Theoretical Computer Science*, 367(1-2):257–270, 2006. 25

[281] Emily Stevens. 15 inspirational ux design quotes that every designer should read. https://careerfoundry.com/en/blog/ux-design/15-

inspirational-ux-design-quotes-that-every-designer-should-read/, Accessed: 03-08-2024. 156

[282] RA Sugden, TMF Smith, and RP Jones. Cochran's rule for simple random sampling. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 62(4):787–793, 2000. 74

[283] Mark Sweney. UK homes cancelled 2m streaming services last year as cost of living soared, 2023. https://www.theguardian.com/media/2023/jan/30/uk-homes-cancelled-2m-streaming-services-cost-of-living-netflix, Accessed 31/01/2023. 96

[284] Franklin P Tamborello and Kristen K Green. Memory and motor processes of password entry error. In *Proceedings of the human factors and ergonomics society annual meeting*, volume 59, pages 672–676. SAGE Publications Sage CA: Los Angeles, CA, 2015. 14

[285] PBN Team. Designing cookie banners on websites: Legal ambiguity prevails. https://www.parisbeacon.com/designing-cookie-banners-on-websites-legal-ambiguity-prevails/ Accessed: 31-06-2023. 58

[286] Mustafa Agah Tekındal, Ozlem Gullu, Yasemin Yavuz, et al. The cochran-armitage test to estimate the sample size for trend of proportions for biological data. *Turkish journal of field crops*, 21(2):286–297, 2016. 74

[287] Tessian. 20 biggest GDPR fines of 2019, 2020, and 2021 (so far). https://www.tessian.com/blog/biggest-gdpr-fines-2020/ Accessed: 23-09-2021. 57

[288] Richard H Thaler and Cass R Sunstein. *Nudge: Improving decisions about health, wealth, and happiness*. Penguin, 2009. 6, 59

[289] The Data Protection Commission. Safeguarding data protection rights by driving compliance through guidance, supervision and enforcement. https://www.dataprotection.ie Accessed: 29-08-2021. 57

[290] Mary Theofanos. Is usable security an oxymoron? *Computer*, 53(2):71–74, 2020. 3

[291] Thomas Claburn. Google ready to kick the cookie habit by q3 2024, for real this time. https://www.theregister.com/2023/02/01/google_cookie_sandbox/ Accessed: 30-05-2023. xvii, 149

[292] V Toubiana, A Narayanan, D Boneh, H Nissenbaum, and S Barocas. Adnostic: Privacy preserving targeted advertising. In *Network and Distributed System Symposium*, 2010. 150

[293] Hannah Towey and Eugene Kim. Amazon used a sneaky tactic to make it harder to quit prime and cancellations dropped 14%, according to leaked data, 2023. https://www.businessinsider.com/amazon-project-iliad-made-cancel-prime-membership-harer-leaked-data-2022-3, Accessed 20-04-2023. 92

[294] Financial Services Union. Stronger consumer protection, 2023. https://www.centralbank.ie/docs/default-source/publications/discussion-papers/discussion-paper-10/financial-services-union---response-to-dp10.pdf?sfvrsn=9a329f1d_2. 51

[295] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 acm sigsac conference on computer and communications security*, pages 973–990, 2019. 65, 66, 67

[296] Alfonso Vara-Miguel, Charo Sádaba, Samuel Negredo, and Cristina Sánchez-Blanco. Revenue diversification strategies of online news organisations: subscriptions and memberships. *Profesional de la información*, 32(2), 2023. 107

[297] James Vincent. Bmw starts selling heated seat subscriptions for $18 a month, 2023. https://www.theverge.com/2022/7/12/23204950/bmw-subscriptions-microtransactions-heated-seats-feature, Accessed 31-10-2023. xvii, 152, 153

[298] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang. Understanding human-chosen pins: characteristics, distribution and security. In *Proceedings*

of the 2017 ACM on Asia Conference on Computer and Communications Security, pages 372–385, 2017. 27

[299] Dr. John A. Weafer and Dr. Fergal Rhatigan. A review of older people's capacity to access financial services online and to independently conduct their own financial affairs. https://www.citizensinformationboard.ie/downloads/social_policy/Accessing_financial_services_online_report.pdf. 153

[300] Adrian Weckler. Major irish websites inaccessible to thousands with disabilities, 2023. https://www.independent.ie/business/technology/major-irish-websites-inaccessible-to-thousands-with-disabilities/a1042607582.html. 3

[301] Wikipedia. Stochastic dominance. https://en.wikipedia.org/wiki/Stochastic_dominance, Accessed: 06-08-2024. 45

[302] Wikipedia. Dutch newspapers, 2022. https://en.wikipedia.org/wiki/List_of_newspapers_in_the_Netherlands, Accessed 06-11-2022. 112

[303] Wikipedia. English newspapers, 2022. https://en.wikipedia.org/wiki/List_of_newspapers_in_the_United_Kingdom, Accessed 06-11-2022. 112

[304] Wikipedia. Web environment integrity, 2023. https://en.wikipedia.org/wiki/Web_Environment_Integrity, Accessed 01-11-2023. 22, 155

[305] PTJ Wolters and BPF Jacobs. The security of access to accounts under the PSD2. *Computer law & security review*, 35(1):29–41, 2019. 16

[306] Robert F Woolson, Judy A Bean, and Patricio B Rojas. Sample size for case-control studies using cochran's statistic. *Biometrics*, pages 927–932, 1986. 74

[307] Mike Yi. What is a box plot? https://www.atlassian.com/data/charts/box-plot-complete-guide, Accessed:10-08-2024. 39

[308] Alisa Zezulak, Faiza Tazi, and Sanchari Das. Sok: Evaluating privacy and security concerns of using web services for the disabled population. *arXiv preprint arXiv:2302.13261*, 2023. 3, 4

[309] Mary Ellen Zurko and Richard T Simon. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms*, pages 27–33, 1996. 3