A Multiphase Mixed Methods Analysis of UK E-Commerce Privacy Policies

By

David Johnson

A Doctoral Thesis

Submitted in Partial Fulfilment of the
Requirements for the Award of
Doctor of Philosophy
of Loughborough University

2019

Acknowledgements

I would like to thank my supervisors Professor Adrienne Muir, Professor Louise Cooke and Dr Steve Probets for supporting and guiding me through this research. Without your expertise, your encouragement and your patience this work would not have been possible. I have enjoyed working with you all and I am very grateful for the opportunities that you have provided me while I have been studying at Loughborough University. I would also like to thank my parents, Trevor and Lorraine, for supporting me for many years whilst this research took place. Your support has been immensely helpful and has played a significant role in enabling me to carry out this research. Thank you for taking the time to listen to my thoughts about this research.

In addition, I would like to thank those that gave up their time to participate in this research. Your honesty and input were much appreciated at each stage of this research. Finally, I would like to thank those faculty members and PhD students that I have had the privilege to work with and meet along the way. My thanks go to Professor Graham Matthews, Professor Anne Goulding and Ian Murray for providing insightful and constructive comments about this research. Each instance of being able to discuss this research with others helped to provoke thought and in doing so provided the opportunity to reflect on the broader context of research.

Abstract

Database technology and advanced statistical processes have rendered it possible to process unprecedented volumes of personal data. However, tension exists between the rights of those that are the subject of personal data processing and the interests of commercial organisations and governments. Privacy policies are supposed to describe how and why personal data is processed. The aim of this research was to explore how these statements could be improved in the context of UK e-commerce. A novel, mixed method phased approach was adopted to address the research aim. In phase one a content analysis of UK e-commerce privacy policies was carried out. Findings showed UK e-commerce privacy policies do not consistently follow good practice guidelines. Moreover, results revealed several information gaps that need to be addressed considering the transparency obligations outlined in the General Data Protection Regulation. Phase two explored user attitudes towards UK e-commerce privacy policies. Barriers to readership and heuristics are outlined along with perceived positive and negative characteristics of UK e-commerce privacy policies. Phase three examined user attitudes towards a layered prototype privacy policy revealing preferences for summary and full layered notices. Phase four demonstrated perceived ease of use and perceived efficiency differences in support of the prototype layered privacy policy compared to a typical privacy. In addition, findings highlighted user support for privacy policy standardisation. Findings from phases one to four are synthesised and evidence-based recommendations are made that are aimed at improving UK e-commerce privacy policies in the short and long term.

Table of Contents

Table of Figures

Table of Tables

Chapter 1 - Introduction

1.1 Research Context

It is difficult to argue that the processing of personal data is not ubiquitous; so much so that personal data is regarded by some as “the world’s most valuable resource” (The Economist, 2017, n.p). Database technology has underpinned a shift in personal data processing (Nissenbaum, 2010). Modern systems enable, with ease, data to be transferred from one geographic location to another. Limits on the accessibility of data have been removed. Connected networks support the combination, aggregation and analysis of data allowing humans to glean predictive insight from advanced statistical techniques. That said, these transformations have brought about a contemporary debate. Acquisti, Brandimarte and Loewenstein (2015) summarise two sides of the argument. One side of the argument suggests that the collection and processing of personal data should be positively embraced. This is because there exists the potential opportunity for society to benefit from the analysis of interconnected data. The other side of the argument highlights the potential for personal data to be misused. Those on this side of the argument suggest that the interests and rights of individuals should be balanced against the desires of commercial organisations and governments.

1.2 Research Topic

In the United Kingdom (UK), those bodies that process personal data are required to provide specific information to individuals about the collection and use of personal data. Organisations usually publish information about the processing of personal data in a privacy policy. Privacy policies are *supposed* to provide data subjects with a comprehensive and clear description of why and how personal data is processed. That said, research is largely critical of these policies. Academics have found that the privacy policies of large international organisations rarely comply with the fair information practices of notice, choice, access and security (Peslak and Jurkiewicz 2008; Li and Zhang 2009; Cha 2011). In addition, evidence suggests that organisations “sugar coat” their personal data handling practices by emphasising positive aspects of personal data processing and downplaying possible invasions of privacy (Pollach, 2005; Pollach, 2007, p. 106; Bhatia *et al.*, 2016). Further to this, data suggests that privacy policies are difficult to read (Sumeeth, Singh and Miller, 2010) and are subject to misinterpretation (Martin, 2015; Reidenberg *et al.*, 2015). However, privacy policies play an important strategic role in building trust. Websites with privacy policies that disclose fair information practices are perceived to be more trustworthy than those websites that do not disclose fair information practices (Lauer and Deng, 2007). Likewise users are more likely to place trust in a website where a privacy policy provides adequate assurance of notice, choice, access and security (Bansal, Zahedi and Gefen, 2015).

1.3 Research Aim and Questions

The aim of this research was: **to explore how UK e-commerce privacy policies could be improved**. This aim was intentionally broad in nature. The findings from seven research questions contributed towards addressing the research aim. Research question one was devised at the outset of the research. Research question one was:

To what extent do UK e-commerce privacy policies follow good practice guidelines?

Research questions two and three emerged based on the findings of the study carried out to address research question one. Research question four was formulated after considering the outcomes of the study conducted to address research questions two and three. Research questions five, six and seven emerged based on the artefact created in response to the findings from research question four.

This emergent, phased design was purposefully employed to provide the flexibility to explore latent issues that were not evident at the beginning of the study when the research aim was set. All seven research questions are explained in the methodology chapter where a justification is provided outlining why a phased approach was appropriate. Furthermore, a description of how the findings from each research question contributed towards the creation of subsequent research questions is provided at the beginning of results chapters five, six and seven. In the discussion and conclusion chapters the findings of all research questions are restated and synthesised to form outcomes that address the research aim.

1.4 Research Justification

The justification for this research is threefold. Firstly, much privacy policy research has been conducted outside the UK with a focus on examining the privacy policies of large international organisations based in the United States (US). To date, and to the authors best knowledge, a holistic and systematic analysis of the privacy policies of UK organisations has not been carried out. Therefore, a research gap exists to investigate the privacy policies of UK organisations.

Secondly, while studies show that users either do not consult privacy policies or only rarely do so (Jensen and Potts, 2004; Williams, Agarwal and Wigand 2014; European Commission 2015; Steinfeld, 2016; Obar and Oeldorf-Hirsch, 2018), at present, they are the primary method used by organisations to communicate personal data processing practices to consumers. Therefore, these policies represent the main way that data subjects can find out how or why personal data is processed by an organisation. To that end, there is a pressing need to explore how privacy policies could be improved in consideration of today's environment of ubiquitous personal data processing.

Thirdly, the General Data Protection Regulation (European Parliament and Council, 2016; GDPR) became enforceable in 2018. The introduction of the GDPR placed renewed emphasis on the publication of information about the processing of personal data. Data controllers are now required to provide more information than was necessary under previously enforceable legislation. This legislative change provided a timely opportunity to assess UK e-commerce privacy policies.

1.5 Research Contributions

This research makes a methodological and practical contribution. From a methodological perspective, this research contributes a coding scheme that can be used in the longitudinal content analysis of UK privacy policies. Being able to measure privacy policy changes over time is important to researchers and policy makers alike and the coding scheme used in this study can be applied, in the future, to analyse policy content. This is critical to building an accurate understanding of how privacy policies change over time, particularly in light of regulatory and policy changes.

From a practical perspective, this research recommends actions that organisations should take to improve the quality of information disclosure and clarity of privacy policies. Designed to help foster compliance with the GDPR, the evidence based recommendations are shaped by the requirement for transparency. Further to that, recommendations are based on the interests of individuals and therefore underpinned by the principle under centricity. To that end, because the recommendations are user informed and driven by the beliefs of users, they help to advance understanding of how transparency and user centricity can be achieved in any programme of privacy by design. To the author’s best knowledge, this is the first study that holistically investigates the privacy policies of UK organisations. The integrated methodology used in this study revealed new findings to evidence how UK privacy policies could be improved.

1.6 Research Scope

The privacy policies of business to customer (B2C) UK e-commerce websites were the subject of this research. In the UK, people are purchasing more online than they ever have. UK e-commerce sales were worth £511 billion in 2016, up from £503 billion in 2015 (Office for National Statistics, 2017a). In contrast to bricks and mortar retail sales, the proportion of UK online retail purchases has grown sharply over the last decade, so much so that data suggests that almost 20% of all retail purchases were made online in August 2018 (Office for National Statistics, 2018). In addition, 87% of UK internet users had bought goods or services online in the twelve months prior to 2018 and this was more than any other European country (EuroStat, 2019). These factors highlighted the importance of investigating UK B2C e-commerce privacy policies and the potential breadth of any practical outcomes.

Data was collected between 2012 and 2016. Websites that were not owned by an organisation incorporated in the UK were outside of scope along with business to business (B2B) and customer to customer (C2C) e-commerce websites. In this study, the researcher worked alone to code a large sample UK B2C e-commerce privacy policies. Measures were taken to assess reliability however stronger forms of reliability, including the use of multiple coders, might have further improved reliability. Attitudes towards UK B2C e-commerce privacy policies were explored. The majority of research participants were aged 18-30. This age bracket contains the most active e-commerce users (Office for National Statistics, 2017b). Survey data shows that 95% and 96% of 16-24 and 25-34 year olds respectively made a purchase online in the twelve months before 2018 (EuroStat, 2019).

1.7 Thesis Structure

This thesis begins by reviewing the privacy literature. Chapter two provides an overview of modern data capture techniques and consequential information privacy concerns. Chapter two also critically reviews existing privacy policy research and those efforts to date that have attempted to address identified issues. Chapter three outlines the mixed method multiphase methodology used to satisfy the research aim. An account of the research findings is provided in chapters four, five, six and seven. Chapter eight discusses the findings of the research relative to previous privacy policy research. Lastly, chapter nine outlines the conclusions of this study and makes recommendations for future work.

1.8 Summary

This chapter has explored the context in which this study took place and has outlined a brief introduction to the research topic. The overarching research aim was presented along with the rationale for study and contributions this research makes.

Chapter 2 - Literature Review

2.1 Introduction

The first section of this chapter explores some of the issues associated with defining privacy. Following this, modern personal data collection techniques are described along with concerns for information privacy. In the final section of this chapter the privacy policy literature is critically reviewed.

2.2 Understanding Privacy: An Overview

Eminent law professor Daniel Solove (2008, p. 1) described privacy as a “concept in disarray”. Over the past century many legal scholars, social theorists and philosophers have attempted to define privacy. As such, multiple conceptualisations of privacy have appeared although today there is still little consensus regarding what privacy really means (Edwards, 2018b). One of the earliest recognised conceptions of privacy can be traced back to the late nineteenth century when law partners Louis Brandeis and Samuel Warren termed privacy: “the right to be let alone” (Brandeis and Warren, 1890, p. 193). At the time of writing Brandeis and Warren were concerned with the advances in photographic technology and the pervasiveness of the media press. They argued that journalists were: “overstepping in every direction the obvious bounds of propriety and decency” (Brandeis and Warren, 1890, p. 196) and in doing so were advocating scandalous gossip. They argued that this exploited an individual’s privacy. Brandies and Warren (1890, p. 196) stated:

> “The intensity and complexity of life, attendant upon advancing civilisation, have rendered it necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.”

Solove’s (2008) analysis of privacy definitions shows the complex and often overlapping nature of privacy with other concepts including security, personality, solitude and seclusion. The current research focuses on information privacy. Westin (1967) and Fried (1984) viewed privacy as matter of control over personal data. Westin (1967, p. 7) defined privacy as: “the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.” Fried (1984, p. 209) suggested privacy is: “not simply an absence of information about us in the minds of others, rather it is the control we have over information ourselves.” Tavani (2007) felt that control theories suggest that an individual could, by choice, grant or deny access to personal information about him or herself. However, Tavani (2007) is critical of such conceptualisations because they fail to identify which categories or types of personal data an individual should have control over or how much control one should expect to have over personal data.

Floridi (2005) describes an ontological view of information privacy in which information privacy is described as a function of ontological friction. Ontological friction is those forces that: “oppose the flow of information within the infosphere” (Floridi 2005, p.186). Therefore, the higher the ontological friction the greater the information privacy. Floridi (2005) feels that information about a person is part of a person. Floridi (2005, p. 195) states:

> “‘My’ in ‘my information’ is not the same ‘my’ as in ‘my car’ but rather the same ‘my’ as in ‘my body’ or ‘my feelings’: it expresses a sense of constitutive belonging, not of external ownership, a sense in which my body, my feelings and my information are part of me but are not my (legal) possessions.”

In the sense that information has a constitutive belonging to an individual, it is considered by Floridi (2005, p.194) that a breach of information privacy is an act of: “aggression towards one’s personal identity.” For that reason, Floridi argues that collecting, storing and manipulating information about an individual should be considered as cloning the identify of a person and that the right to information privacy should amount to protection against unwanted processing of information about a person’s identity.

Enumerating and agreeing on an exhaustive list of the types of personal data that *everyone* should have control over would be challenging. For Nissenbaum (2010), privacy claims are bound by contextual information norms. Information communication, sharing and dissemination all happen within a social context. Each social context has a distinctive set of rules governing the flow of information. A breach of privacy occurs when the entrenched patterns of information flow are not respected. Each flow of information is characterised by actors, types of information and transmission principles. Actors are the senders of information, the receivers of information and the information subjects. Information types are the nature of the information being communicated. Transmission principles are the rules that govern the processing of information.

Take a typical electronic-commerce (e-commerce) transaction. Person A is purchasing a book from Company Z. Person A is the sender of information and the information subject. Person A purchases a book from Company Z and as part of this transaction person A discloses his or her demographic and payment data (the information types). Person A expects the transmission of data to be unidirectional. The demographic and payment data are used to verify the purchase and send the book to Person A's address. At this stage no breach has occurred. Company Z has respected the expected unidirectional flow of information. However, Company Z decides to share the demographic details of Person A with Company Y. Person A did not consent to this sharing and the sharing of information was *not* part of the transmission principles. To that end, a breach has occurred because the flow of information has departed from the prescribed norms.

A point of contention amongst privacy scholars is the identification of when a *loss* of privacy occurs. Gavison (1984) highlighted one example. Consider person A talking to person B about his or her daily activities. Has person A lost his or her privacy in this situation? One might argue that privacy is indeed lost in this situation because person A no longer has the control to prevent person B from disseminating the information that has been discussed. If privacy has been lost, when does the loss occur? Does it occur when person A informs person B about his or her activities or does the loss occur when person B decides to share that information with person C and person D? Fried (1984) feels that the very fact that someone had knowledge about an individual did not always constitute a loss of privacy. Fried felt that privacy is not necessarily invaded when a general fact about an individual is known by others, but it may well be invaded when others know further factual details than the individual originally wished to reveal.

In the absence of an agreed upon definition of privacy it is worth pointing out the concepts of fairness, expectations and context. These concepts underpin contemporary information privacy discussions. Fairness is the degree to which personal data processing is considered acceptable. In the UK, the Information Commissioner states that personal data should be processed for purposes that individuals reasonably expect (Information Commissioner's Office, 2018a). That said, privacy expectations are not universal. Rao et al (2016) showed that privacy expectations are shaped by the type of website that a user visits. For example, users have different beliefs about how financial websites will process personal data compared to health websites. Furthermore, expectations and behaviour differ according to context. Acquisti, Brandimarte and Loewenstein (2015, p. 511) state: "the rules people follow for managing privacy vary by situation, are learned over time, and are based on cultural, motivational, and purely situational criteria."

Westin's (Westin 2001 cited in Kumaraguru and Cranor, 2005, p. 12) privacy typology revealed different attitudes towards privacy. According to Westin (2001 cited in Kumaraguru and Cranor, 2005), individuals fall into one of three categories based on their privacy beliefs. Individuals could be considered either privacy fundamentalists, privacy pragmatists or privacy unconcerned. Privacy fundamentalists are those extremely concerned about personal data processing. Typically, they do not trust organisations that ask for personal data and are in favour of stronger privacy regulation. Privacy pragmatics are those concerned about certain aspects of privacy. These individuals will consider the benefits of opportunities when buying products and services and weight these benefits against the risk of providing personal data to organisations. Pragmatists believe that organisations should provide individuals with the opportunity to opt out of personal data processing. Privacy unconcerned are those individuals that show little anxiety about privacy and are generally prepared to disclose personal data to businesses. In general these individuals will trust organisations with the processing of personal data and will likely relinquish control over personal data in order to receive customer service benefits (Westin, 2003; Kumaraguru and Cranor, 2005).

Privacy fundamentalists and privacy pragmatists show at least some degree of concern about the processing of personal data. Internet privacy concerns represent the degree to which individuals feel that the processing of personal data is fair (Campbell, 1997). Malhotra, Kim and Agarwal's (2004) Internet User Information Privacy Concern (IUIPC) scale shows that privacy concern is a multidimensional concept constituting of concerns relating to collection, control and awareness. Concerns about collection relate to the amount of personal data being processed (Smith, Milberg and Burke, 1996; Malhotra, Kim and Agarwal, 2004). Concerns about control relate to the choices that individuals have in relation to the processing of personal data. Concerns about awareness relate to the degree to which individuals are concerned about being aware of personal data processing practices (Malhotra, Kim and Agarwal, 2004).

Survey research in Europe has consistently shown that a considerable proportion of individuals are concerned about the dimensions of personal data collection, control and awareness. Findings from the Annual Track survey commissioned by the UK Information Commissioner's Office (ICO) suggest that 60% of individuals from the UK disagree that they are in control of personal data processing (Citizenme, 2016). Survey results published by the European Commission (2015) showed that four fifths of UK citizens are worried about personal data being processed for additional purposes not compatible with the original purpose of data collection. Political think tank Demos reported that almost 80% of individuals living in Great Britain were concerned about organisations using personal data without permission (Bartlett, 2012). In the same study, a similar proportion of individuals stated they were worried about personal data being sold to third parties.

2.3 Personal Data Processing: Practice, Concern and Consequence

Critics argue that modern data processing techniques erode fair processing because they allow organisations to process personal data covertly (Boerman, Kruikemeier and Zuiderveen Borgesius, 2017). One contentious personal data processing technique is profiling. Profiling is the practice of collecting and analysing information about users in order to determine or predict personality traits, behaviour and interests (Direct Marketing Association, 2017). Article 4(4) of the GDPR (European Parliament and Council, 2016, p. 14) defines profiling as:

> “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

Profiling is contentious because it involves combining personal data from different sources to predict behavioural traits. While controversial in nature, profiling is essential to the revenue models of social media companies (such as Facebook) and search organisations (such as Google) and is used more generally across e-commerce websites (Edwards, 2018a). This is the case because these organisations are dependent on generating revenue from behavioural advertising. Online behavioural advertising seeks to study behaviour over time in order to develop a profile and provide adverts to individuals based on topics that match their inferred interests (Article 29 Working Party, 2010, p. 4; Boerman, Kruikemeier and Borgesius, 2017). This practice is beneficial to organisations because decision making is completed in seconds reducing the amount of time taken to decide which user should see which advert. In addition, data used in behavioural advertising enables granular segmentation of audiences (McStay, 2016). Consulting firm Accenture (2016) found that organisations use nine distinct sources of data to segment customers. These sources include measurement companies (such as third-party data brokers), website analytics, consumer relationship management systems and social media activity.

Organisations collect data from different user interactions. The types of behavioural data collected by organisations include: browsing data, search history data, media consumption (for example videos watched, images clicked on), purchases, click-through responses to advertisements, communications content (such as Facebook posts) and social media interactions (such as Facebook Likes) (Borgesius, 2015). Data is collected by first and third parties.

2.3.1 Practice: First Party and Third-Party Data

First party data is collected and aggregated by the website the user is visiting. Most obviously this includes personal data that the user knowingly provides to the website. Examples of this practice include registering on a website, signing up to email notifications and paying for goods or services. This is obvious to users and survey research suggests that the majority of Europeans accept that disclosing personal data for the provision of services is: “part of modern life” (European Commission, 2015).

In other instances, the disclosure of personal data is not as clear. Database technology enables unique identifiers to be assigned to user devices. Unique identifiers can be used to identify and track individual behaviour. A cookie is a: "piece of information the server and client pass back on forth" (Kristol, 2001, p. 154). Cookies resolve the issue of statelessness between different web server requests and therefore allow web servers to recognise different requests originating from the same web browser. Cookies contain a unique string of characters and they are stored on a user's device to allow the web server to identify the browser that is requesting information. Additional cookie metadata, including an expiry date, can also be stored and passed between the web client and web server (Barth, 2011).

First party cookies originate from the web server of the website that the user is requesting. First party cookies can be used by e-commerce organisations to deliver customised content to consumers. The same type of cookies can be used to tailor the display preferences of users. Some e-commerce websites may use a first party cookie to enable the user's web browser to display previously chosen preferences such as the preferred language of a website, background colour and other page styling choices such as text size. Session cookies expire after the web user ends the web session. Session cookies are useful for common e-commerce activities, such as remembering the contents of a shopping cart or remembering that a user has previously logged into a website during the same browsing session. Persistent cookies do not expire after a session. Persistent cookies can have a precise expiry date or have no expiry date at all.

Research has revealed the extent of cookie setting by UK and European organisations. The Article 29 Working Party (2015) found a total of 16555 cookies were set by 478 European websites. Overall, UK e-commerce websites set 2250 cookies. UK e-commerce websites were found to set the most cookies compared to websites from other European nations. French e-commerce websites set the second highest number of cookies totalling 1286. UK websites also set the highest number of first party cookies. In total, UK websites set 1245 first party cookies while French websites set 1056 cookies of the same type.

McStay (2016) highlights that first party data is valuable to organisations because it is aggregated directly by the website the user is visiting. In turn, Edwards (2018a) notes that this data is important to organisations because it enables predictions to be made about the likelihood that a user will be interested in purchasing a particular product. Such data can be used to inform which adverts a user may see on a website. Websites can also combine data collected using first party cookies with explicit information provided by the user to build a richer picture of individual behaviour.

Third party data is collected by an entity separate to the organisation of the website that the user is visiting. Third party cookies (and other third-party content embedded within first party websites) are used to identify users and track user behaviour over multiple websites. Third party cookies originate from a web server that is different to one that the user is requesting. Kristol (2001, p. 159) notes: “a browser can receive third party cookies if it loads a page from one website, loads images (such as ads) from another website, and the latter website sends a cookie with the image.” Research from the Article 29 Working Party (2015) found that 84 UK websites set 2466 third party cookies. Only French websites were found to set more third-party cookies. Findings from the same study revealed that UK websites set twice as many third-party cookies compared to first party cookies. Results also demonstrated that UK e-commerce websites set on average 37 third party cookies. In addition, one UK e-commerce website set 148 cookies with 120 of these being third party cookies. The prevalence of third-party cookie setting was also highlighted recently by Davis (2017) who found that UK newspaper website the Daily Mail set 19,136 third party cookies.

Third party data brokers use third party cookies to collect data from users. The breadth of data points processed by data brokers is extensive. Table 2.1 shows data broker Acxiom stores data across a broad range of categories including demographic data, financial data and vehicle data. Furthermore, data broker Experian (2017) claims to hold over five hundred data points that relate to forty nine million UK adults. After personal data is collected, data brokers integrate data from other online and offline sources, synthesise the data to create a profile and then sell segmented data to organisations (Anthes, 2014). Table 2.2 shows a snapshot of the types of segmented data sold by Experian (United States Government Accountability Office, 2013). The availability of segmented marketing lists allows first party organisations to source data relevant to their product range. This can be combined with first party data and used to target advertisements at individual users. Figure 2.1 shows how data collected from a user flows through a third-party data broker ecosystem to a first party organisation.

Category	Data points
Individual	Name, address, telephone number, e-mail, gender, education, occupation, voter party, ethnic code/language preference, age, date of birth.
Household demographics	Adult age ranges, children's age ranges, gender, number of adults and number of children in the household, marital status.
Household purchase behaviour	Frequency of purchase indicator, types of purchases indicator, charitable giving indicator, community involvement indicator, average direct mail purchase amount, direct mail frequency indicator.
Household life event indicators	New parent, expectant parents, new teen driver, college graduate, empty nester, new mover, recent home buyer, recent mortgage borrower, getting married, divorced, child leaving home, buying a new car.
Household wealth indicators	Estimated household income ranges, income producing assets indicator, estimated net worth ranges.
Household vehicle data	Year, make, model, estimated vehicle value, vehicle lifestyle indicator, model and brand affinity, used vehicle preference indicator.
Household social media predictors	Social media sites likely to be used by an individual or household, heavy or light user, whether they engage in public social media activities such as signing on to fan pages or posting or viewing YouTube video.

Table 2.1 - Data points derived by data marketing organisation Acxiom adopted from United States Government Accountability Office (2013)

Location data is another category of personal data that can be collected by first or third-party websites. Edwards (2018a, p. 37) describes location data as: "an increasingly vital part of the thrust towards profiling." Location data is used to determine the longitude and latitude of a device, the altitude of a device, the direction that a device is travelling and the speed of a device. First party websites might combine location data gathered by third party services with their own data obtained using cookies or another unique identifier (Interactive Advertising Bureau, 2016). According to data obtained by consulting organisation Salesforce (2018), 74% of European advertisers use location data to deliver targeted advertisements to users.

Category	Marketing lists
Hobbies and interests	Reading, gardening, photography, volunteering
Pet owners	Cats, dogs and other pets
Reading preferences	Children's, history, mystery, romance
Collecting	Dolls, plates, sports memorabilia
Cooking and entertaining	Baking, recipes, wine appreciation
Health and fitness	Healthy living, interest in fitness, reduce fat/cholesterol
Music preference	Country, jazz, classical
Sweepstakes and gambling	Casino gambling, lotteries
Sports and recreation	Sailing, fishing, golf, tennis
Occupations	Beauty, executives, doctors, professional/technical, teacher, skilled/trade
Financial investment	Life insurance, real estate, stocks or bonds
Ailments	Angina, asthma, back pain, headaches, osteoporosis
Visual impairments	Contact lenses, eyeglasses, visual correction

Table 2.2 - Experian marketing list categories adopted from United States Government Accountability Office (2013)

One of the defining features of third-party data collection is the ability to collect data about the same user over different domains. This allows third parties to build up a profile of user behaviour across different websites. Edwards (2018a) describes this scenario using the market leading advertising network, DoubleClick. When a user visits Amazon.co.uk, Amazon deposits a first party cookie. If Amazon partners with DoubleClick, then DoubleClick would also deposit a cookie. DoubleClick may also partner with various other retailers. The next time the same user visits one of these retailers, DoubleClick would recognise that a cookie has already been set from their domain. In this scenario, DoubleClick would have the ability to collect data about user behaviour across a series of websites. This creates the opportunity to generate an in-depth profile of user activity.

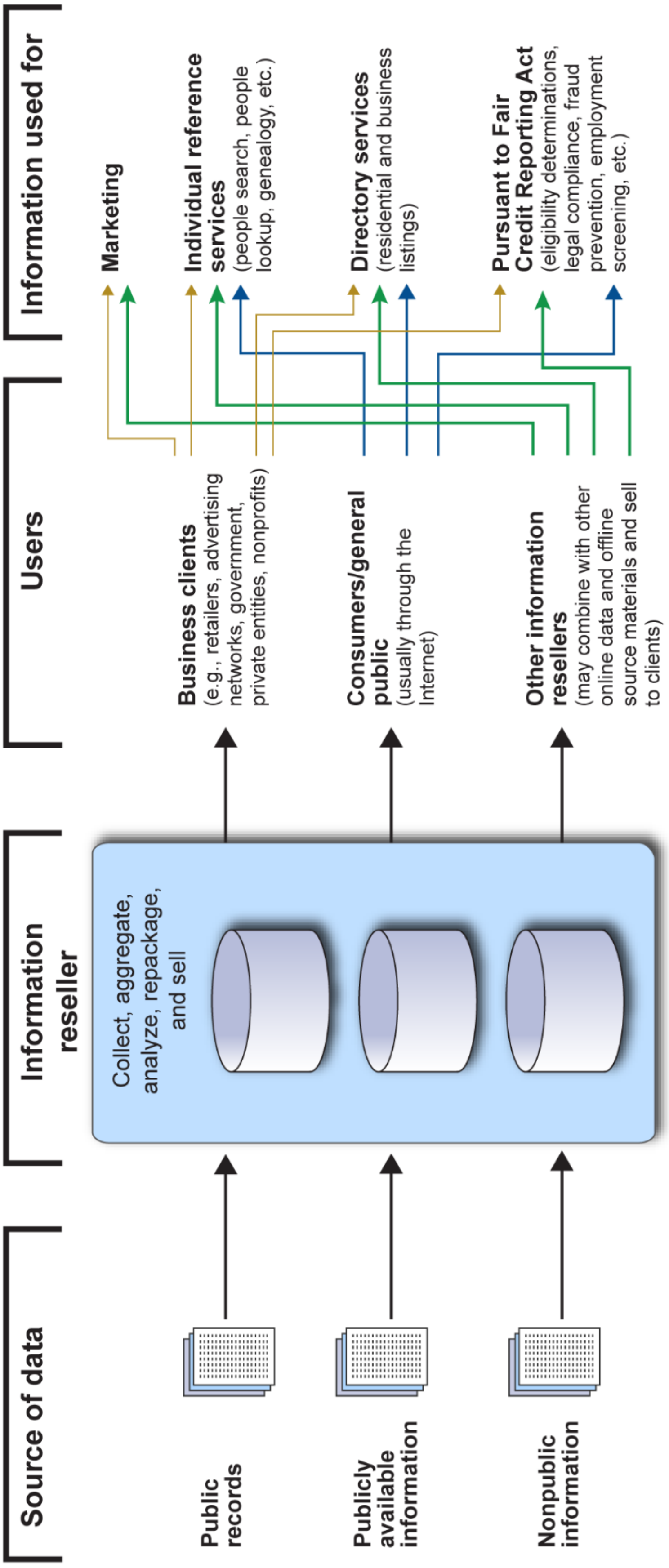

Source of data
Public records
Publicly available information
Nonpublic information
Information reseller
Collect, aggregate, analyze, repackage, and sell
Users
Business clients (e.g., retailers, advertising networks, government, private entities, nonprofits)
Consumers/general public (usually through the Internet)
Other information resellers (may combine with other online data and offline source materials and sell to clients)
Information used for
Marketing
Individual reference services (people search, people lookup, genealogy, etc.)
Directory services (residential and business listings)
Pursuant to Fair Credit Reporting Act (eligibility determinations, legal compliance, fraud prevention, employment screening, etc.)

Figure 2.1 - Consumer data flown adopted from United States Government Accountability Office (2013)

Browser fingerprinting is another method that third-party organisations use to uniquely identify users. The purpose of browser fingerprinting is to: “gather a set of attributes, which, when combined, provide a fingerprint that, for all practical purposes, is unique to a specific user’s computer” (Nikiforakis et al., 2014, p. 29). Browser fingerprinting uses attributes of the browser to generate a unique fingerprint (Upathilake, Li and Matrawy, 2015). Boda et al (2011) found that part of a machine’s IP address along with installed fonts, the time zone and the screen resolution were enough variables to accurately identify users. Version numbers of Flash or Java plugins can also be used in the generation of a browser fingerprint. Eckersley (2010) reported that Flash or Java plugins could be used to identify users where no cookies were set by a website. Findings from Eckersley’s study revealed that just one in 286,777 browsers will share the same fingerprint.

2.3.2 Concern: Creepy Marketing

Deriving an unknown characteristic about someone based on other known characteristics or behaviours is a powerful but concerning practice. Walker (2013) highlights an example where one marketing organisation used characteristics including subscribing to cable TV and purchasing a minivan to reliably infer whether an individual was obese. Creating these inferences relies on taking data collected for one purpose, such as recording that person X has purchased a minivan to administer his or her warranty on the vehicle, and use using it for a secondary purpose, such as inferring that person X is obese. Doyle (2018) states that capturing trivial information and repurposing it with a different intention without consent can result in discrimination on the basis that people are treated differently according to how they are algorithmically categorised.

Many European citizens are worried about the how personal data is being processed for online behavioural advertising purposes. Some users describe online behavioural advertising as scary and creepy (Ur *et al.*, 2012). “Creepy marketing”, as Moore at al (2015) coined it, makes users feel uncomfortable and uneasy. Typically, users feel this approach is invasive and goes beyond the principle of data minimisation by gathering more personal data than is required. Furthermore, Dolin et al (2018) found that users felt it was less fair and were less comfortable with the practice of individually targeting a single advertisement at a specific person based on their inferred interests compared to targeting a single advertisement to all users on a website. Furthermore, research carried out by The European Commission (2015) found that over half of the 27,980 European individuals surveyed were concerned about the collection of location information and purchasing habits. Findings from the same study showed that nearly half of those European citizens surveyed were concerned about organisations recording internet browsing activity. Survey findings from UK think tank Demos (Bartlett, 2012) highlighted that under 25% of over 5000 individuals living in Great Britain felt comfortable that online browsing history was collected and used to personalise offers. Martin (2015) found that on average users did not expect websites to sell personal data at an online auction or use data collected during online tracking to target advertisements towards friends or contacts. In fact, survey research conducted by the European Commission (European Commission, 2016) shows that over 80% of European citizens feel that tracking devices should only be used for monitoring online behaviour with the permission of the user. In addition, two thirds of European citizens feel that it is unacceptable for websites to monitor online behaviour in return for unrestricted access to a website (European Commission, 2016).

2.3.3 Consequence: Impact on Stated Behaviour

Privacy calculus theory postulates that consumers perform a risk benefit analysis before disclosing personal data (Culnan and Armstrong, 1999). Culnan and Bies (2003, p. 327) argued that customers: “disclose personal information as long as they perceive that they receive benefits that exceed the current or future risks of disclosure.” Privacy risk is defined as a:

> “consumer’s subjective evaluative assessment of potential losses to the privacy of confidential personally identifying information, including the assessment of potential misuse of that information that may result in identity theft” (Featherman, Miyazaki and Sprott, 2010, p. 220).

The relationship between perceived risk and concern for information privacy is bidirectional. Dinev and Hart (2006) found that a higher level of perceived risk is positively associated with the higher level of concern for information privacy. On the other hand, Gurung and Raga (2016) found that higher concerns for information privacy result in higher perceptions of risk. Where concerns for information privacy are high, consumers are more likely to refuse to provide personal data and more likely to request the removal of personal data (Dinev and Hart, 2006; Son and Kim, 2008; Schwaig *et al.*, 2013). What is more, research also suggests that consumers are more likely to complain about the processing of personal data (Schwaig *et al.*, 2013) and negatively communicate feelings about privacy threats to others where concern for information privacy is high (Son and Kim, 2008).

2.4 Privacy Policies: An Introduction

The term *privacy policy, privacy notice* and *privacy statement* are common names for the documents that communicate information about the processing of personal data (Li *et al.*, 2012; Chua *et al.*, 2017). The three terms are used interchangeably throughout this thesis. Some users state they read privacy policies when purchasing goods and services online. The European Commission (2015) found that 13% of people sampled from the UK stated that they would read, in full, a privacy policy, while 54% of people stated they would partially read a privacy statement. Evidence suggests that self-reported readership levels differ in practice. Obar and Oeldorf-Hirsch (2018) found that almost three quarters of university students ignored a website privacy policy when signing up for a fictitious service while data from Steinfeld's (2016) study showed that just one in five students clicked to view a privacy policy when asked to agree to a privacy statement under experimental conditions. Under non-experimental conditions the proportion of website users reading a privacy policy may be even less. An examination of website log files carried out by Jensen and Potts (2004) showed that in practice privacy policies were viewed only 131 times out of over 55000 website visits (0.24%). Furthermore, findings suggest that individuals that do view privacy policies spend anything from 14 seconds (Obar and Oeldorf-Hirsch, 2018) to 59 seconds (Steinfeld, 2016) reading a privacy policy.

In the absence of reading privacy policies users will draw on environmental cues to infer risk and guide decision making (Acquisti, Brandimarte and Loewenstein 2015). The availability heuristic occurs when individuals simplify the choice they make by using probability judgements (Acquisti et al, 2017). Acquisti et al (2017, p. 4) state:

> “the availability heuristic may come into play when users are heavily influenced by salient cues that may or may not be effective signals of the probability of adverse events. For instance, they may attempt to estimate the risk of disclosure by evaluating the probability of others disclosing personal information in the same or similar contexts.”

In practice, Lowry et al (2012) found that the presence of a privacy statement, brand image and website quality influence perceptions of privacy assurance.

While most users do not read privacy policies, evidence suggests that trust is influenced by readership of these documents. Trust is the:

> “willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (Mayer, Davis and Schoorman, 1995, p. 712).

Research shows that individuals place more trust in a website that displays a detailed privacy policy describing how personal data is collected and processed (Liu *et al.*, 2005). Lauer and Deng (2007) found that an organisation with a privacy policy that disclosed the fair information practices of notice, choice, access and security was perceived to be more trustworthy than a company with a privacy policy that did not mention all of the fair information practices (the fair information practices are discussed further in section 2.5). Individuals felt that an organisation with a privacy statement compliant with the fair information practices was likely to behave with more integrity, show a greater level of benevolence towards customers and show more competence than an organisation publishing a non-compliant fair information practice privacy policy. In addition, Bansal, Zahedi and Gefen (2015) showed that users report a higher level of trust where they feel that a privacy policy provided adequate assurance in relation to the fair information practices of notice, choice, access and security. Individuals with high privacy concern will rely more on the assurances provided within a privacy statement to form trusting beliefs than users with low privacy concern (Bansal, Zahedi and Gefen, 2015).

The implications of the relationship between privacy policies and perceived trust are crucial for organisations because research shows that trust is strongly associated with stated behavioural intentions (Mcknight, Choudhury and Kacmar, 2002). Recent survey research commissioned by the UK Information Commissioner shows that only a quarter of UK adults trust businesses with personal data (Citizenme, 2016). Furthermore, the same study found that internet brands are the least trusted with personal data compared to high street banks, technology brands, energy providers and government departments. Individuals that show higher levels of trust in an organisation state they are more likely to: (a) disclose personal data to the website (Dinev and Hart, 2006) and (b) disclose personal data about themselves that is accurate (Lauer & Deng, 2007). Consumers showing higher levels of trust also feel they are more likely to remain loyal to a website (Lauer & Deng, 2007). Where trust is high, individuals also state that they are more likely to recommend a website to others, make a repeat purchase, visit the website again and make positive marks about the website (Liu et al., 2005).

Tsai et al (2011) found that consumers behaved differently when presented with privacy information during the course of a transaction. In Tsai et al's study, consumers were more likely to purchase from a website that displayed salient privacy information. In addition, individuals tended to favour websites where privacy protection was strongest. Tasi et al's study (2011) investigated behaviour. Studies have shown that stated information privacy attitudes differ from actual behaviour. For example, individuals state they are concerned about the processing of personal data but tend not to seek information about how personal data is processed. Kokolakis (2017) provides an overview of theoretical explanations for this dichotomy. Immediate gratification could explain why consumers are willing to provide personal data to access services without reading privacy policies. Acquisti (2004) suggested that individuals may value the immediate benefits of personal data disclosure (for example, accessing the service that they desire), over any future risks. Information asymmetry may also contribute towards this dichotomy (Kokolakis, 2017). Information asymmetry occurs when different parties involved in a transaction have different levels of knowledge about the transaction (Acquisti, 2004). In the context of information privacy, the organisation processing personal data might have more knowledge than the user disclosing personal data because the user has not read the privacy policy. Tsai et al (2011, p. 256) stated the lack of information:

> "arguably affects individual behaviour in different ways. For one, consumers may perceive greater risk and uncertainty when dealing with merchants whose privacy policies are unknown; as a result, they may be less willing to complete transactions with those merchants. However, if the lack of information is so profound that consumers are not even aware that their personal information could be exchanged or misused, it may make them more likely to engage in such risky (from a privacy perspective) transactions."

In theory privacy policies play an important role reducing information asymmetry because they should provide individuals with a clear and comprehensive description of personal data processing. The legal requirements for organisations are outlined in the next section.

2.5 Transparency: Theory and Requirements

The Information Commissioner’s Office (2016a) states that it is of paramount importance that organisations are transparent about the processing of personal data. Article 4(1) of the GDPR (European Parliament and Council, 2016, p. 33) defines personal data as: “any information relating to an identified or identifiable natural person (‘data subject’);” Article 4(4) (European Parliament and Council, 2016, p. 33) describes an identifiable natural person as somebody that can be identified: “by reference to an identifier such as a name, an identification number, location data, an online identifier.” An individual’s name might seem an obvious identifier however the context of processing will determine whether a name identifies an individual. For example, the name Bob Smith refers to more than one individual however combining the name Bob Smith with an address could identify an individual and therefore be considered as personal data.

Recital 30 of the GDPR (European Parliament and Council, 2016, p. 6) provides more detail in relation to online identifiers:

> “Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”

Identifiers should be considered personal data where they are used to track and profile individual behaviour across websites (Information Commissioner’s Office, 2018a). This includes the alphanumeric codes that are used by cookies.

Article 5(1)(a) of the GDPR (European Parliament and Council, 2016, p. 35) states that: “personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”. Transparency is the: “perceived quality of intentionally shared information from a sender” (Schnackenberg and Tomlinson, 2016, p. 1788) The principle of transparency is a dimension of a broader concept; privacy by design. Privacy by design involves integrating data protection principles into the design decisions of digital services and business processes to ensure that data protection is a core function of systems. The aim of doing so is to safeguard data subject rights, achieve GDPR compliance and provide individuals with greater control of personal data (Cavoukian, 2011; Information Commissioner’s Office, 2019). Data controllers should ensure that systems behave in a way that is consistent with stated promises and objectives and that notice of processing is transparent and visible to data subjects (Caboukian, 2011). The concept of data protection by design is recognised in Article 25 and Recital 78 of the GDPR. Recital 78 states data controllers:

> “should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.”

Information disclosure, clarity and accuracy are dimensions of transparency (Schnackenberg and Tomlinson, 2016). Next, each dimension is explored in relation to the requirements of the GDPR.

2.5.1 Information Disclosure

Information disclosure involves openly sharing relevant information in a timely manner (Schnackenberg and Tomlinson, 2016). Relevance is the state of being appropriate (Oxford University Press, 2018). To satisfy the requirements of Article 5(1) of the GDPR organisations must provide data subjects with specific information in relation to the processing of personal data. Articles 13 and 14 of the GDPR are prescriptive about this information; this is shown in table 2.3. In addition, the conditions for lawful processing of personal data are outlined in article 7(1) of the GDPR. Consent is one of these conditions. Under article 4 of the GDPR (European Parliament and Council, 2016, p. 34) consent is defined as: “any freely given, specific, informed and unambiguous indication of the data subject's wishes.” To demonstrate that consent is an informed indication of the data subject’s wishes, article 7(2) of the GDPR stipulates that information should be provided to the data subject. The Article 29 Working Party (2018a) (now The European Data Protection Board) states that this information should enable the data subject to understand exactly what they are consenting to, in order to allow informed decision making to take place. What is more, article 6(2) of the Privacy and Electronic Communications (EC Directive) Regulations 2003

(Parliament, 2003, p. 4) requires organisations using cookies and other methods of storing identifiers on a user’s machine to provide the user with: “information about the purposes of the storage of, or access to, that information.”

The Data Protection Act 1998 (Parliament, 1998) was the enforceable UK statute governing personal data when this research started. During the current research the Data Protection Act was updated by the GDPR (European Parliament and Council, 2016). Articles 13 and 14 of the GDPR place the obligation on the data controller to provide a broader range of information compared to the requirements outlined in schedule one Data Protection Act 1998. Schedule one of the Data Protection Act 1998 stated that the data controller should provide the data subject with information about: (1) the identity of the data controller, (2) the identity of the representative (if applicable), (3) the purposes for which personal data will be processed and (4) any further information to enable fair processing to take place. The final information requirement, point four, was broad in scope. For that reason, the Information Commissioner (Information Commissioner’s Office, 2010) published best practice guidelines in 2010. In doing so the Information Commissioner recommended categories of information that should be communicated to data subjects to help satisfy the principle of fair processing. Following the introduction of the GDPR, these guidelines have been replaced. The ICO currently publishes guidance to help organisations comply with Articles 12, 13 and 14 of the GDPR (Information Commissioner’s Office, 2018c). At European level, the Article 29 Working Party has also published guidance (Article 29 Working Party, 2018b). Table 2.4 shows the differences in information requirements stipulated by Article 13 and 14 of the GDPR in comparison to the requirements of the Data Protection Act 1998 and the best practice guidelines published by the Information Commissioner in 2010 (Information Commissioner’s Office, 2010).

	Information requirement	Is the information obligatory under Article 13 of the GDPR?	Is the information obligatory under Article 14 of the GDPR?	Comments on the information requirement from the Article 29 Working Party (2018b) and the ICO (Information Commissioner's Office, 2018c)
1	The identity of the data controller	✓	✓	This information should allow the data controller to be easily identified. Multiple forms of contact information are preferable.
2	The contact details of the data controller	✓	✓	
3	Representative organisation name and contact details	If applicable	If applicable	If the data controller has a representative organisation, this should be provided to the data subject.
4	The contact details of the data protection officer	If applicable	If applicable	If the data controller has a nominated data protection officer, this should be provided to the data subject.
5	The purposes of processing	✓	✓	This information should highlight why personal data is being used.
6	The legal basis for processing	✓	✓	This information should highlight which lawful basis (under Article 6) is being used to justify the processing of personal data.
7	The legitimate interests for processing	If applicable	If applicable	The legitimate interest that the data controller is using to justify processing should be communicated to the data subject.
8	The recipients or categories of	If applicable	If applicable	This information should highlight if personal

	recipients of personal data			information is shared and who it is shared with.
9	The details of transfers to a third country or an international organisation	If applicable	If applicable	This information should state whether personal data is transferred outside the EEA.
10	The retention period	✓	✓	This information should state the retention period, or in the case of an unknown exact period, how the period will be determined.
11	The rights available to individuals	✓	✓	This information includes the right to access and rectify personal data as well as the right to erasure and the right to object to processing. The right to data portability should also be included. The information should also state how these rights can be exercised.
12	The right to withdraw consent	If applicable	If applicable	If the lawful basis for processing is based on consent, details of how the right to withdraw consent can be exercised should be provided.
13	The right to lodge a complaint with a supervisory authority	✓	✓	This information should highlight that the data subject has the right to complain to the relevant supervisory body.
14	The details of whether an individual is under	If applicable	✗	This information should highlight whether it is a contractual obligation to

	a statutory or contractual obligation to provide personal data			provide personal data and the consequences of not providing personal data.
15	The details of any automated decision making	If applicable	✓	This information should highlight the logic involved in any decisions that are made based on automated processing.
16	The source from which the personal data originated	✗	✓	This information should highlight where personal data were obtained and if applicable whether it came from a publicly accessible source.
17	The categories of personal data	✗	✓	This information should include a description of the categories of personal data that the data controller has obtained.

Table 2.3 - GDPR information requirements

	GDPR information requirements outlined in Articles 13 and 14	Explicitly required under the Data Protection Act 1998?	Recommended as part of the ICO's best practice guidelines published in 2010?
1	The identity of the data controller	✓	✓
2	The contact details of the data controller	✗	To some degree
3	Representative organisation name and contact details	If applicable	If applicable
4	Contact details of the data protection officer	✗	To some degree
5	The purposes of processing	✓	✓
6	The legal basis for processing	✗	✗
7	The legitimate interests for processing	✗	✗
8	The recipients or categories of recipients of personal data	✗	If applicable
9	The details of transfers to a third country or an international organisation	✗	If applicable
10	The retention period	✗	✓
11	The rights available to individuals	✗	✓
12	The right to withdraw consent	✗	✓
13	The right to lodge a complaint with a supervisory authority	✗	✓
14	The details of whether an individual is under a statutory or contractual obligation to provide personal data	✗	To some degree
15	The details of any automated decision making	✗	To some degree
16	The source from which the personal data originated	✗	✗
17	The categories of personal data	✗	✗

Table 2.4 - GDPR information requirements compared to the Data Protection Act 1998 and the ICO best practice guidelines

Providing information within a timely manner is: “a vital element of the transparency obligation and the obligation to process data fairly” (Article 29 Working Party, 2018b, p. 14). Article 13(1) of the GDPR (European Parliament and Council, 2016, p. 40) states that information in relation to the processing of personal data must be provided to the data subject: “at the time when personal data are obtained.” This applies when personal data are collected from the data subject. When data are not collected from the data subject, article 14(3) of the GDPR states that the data controller should provide the relevant information to data subject within a reasonable period or at the latest within one month depending on the context of processing.

2.5.2 Clarity

Clarity refers to the: “comprehensibility of information received from a sender” (Schnackenberg and Tomlinson, 2016, p. 1792). Comprehensibility is the degree to which information can be understood. Article 12 of the GDPR (European Parliament and Council, 2016, p. 39) states that the information provided to data subjects should be in a: “concise, transparent, intelligible and easily accessible form, using clear and plain language.” The information provided by data controllers should be able to be understood: “by an average member of the intended audience” (Article 29 Working Party, 2018b, p. 7). The need for clarity is repeated in article 7(2) of the GDPR. Lawful consent can only be achieved where the information provided about personal data processing is presented in: “clear and plain language” (European Parliament and Council, 2016, p. 37). Furthermore, article 6(2) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (Parliament 2003, p. 4) states that information provided to users about cookies and other similar technical storage methods should be: “clear and comprehensive.”

Legalistic terminology is not recommended (Information Commissioner’s Office, 2010, 2018c). The ICO states that such terminology would not satisfy the requirements of Article 12 (Information Commissioner’s Office, 2018c). Similarly, complex sentences and ambiguous terminology with multiple interpretations should be avoided (Article 29 Working Party, 2018b). In addition, the Article 29 Working Party recommend that personal data processing information should be communicated succinctly to prevent users becoming fatigued (Article 29 Working Party, 2018b). To help organisations produce policies that can be easily understood, the European Commission (2011) has produced guidelines on how to write clearly. The information provided to the data subject should be in writing or by electronic means. Information may be provided orally in instances where the identity of the data subject is proven.

Article 12(5) of the GDPR also states that the information should be provided to the data subject free of charge.

2.5.3 Accuracy

Accuracy is defined as: “the perception that information is correct to the extent possible given the relationship between sender and receiver” (Schnackenberg and Tomlinson, 2016, p. 1793). The information provided to the data subject should be a truthful account of personal data processing (Information Commissioner’s Office, 2010). The Information Commissioner recommends that organisations carry out an information audit to understand how personal data is processed throughout the organisation. Organisations should test, review and update policy documents to ensure accuracy at any given point in time.

2.6 Transparency: Problems in Practice

Research has highlighted several problems with website privacy policies. The following sections describe nine problems discussed within the privacy policy literature.

2.6.1 Problem One: Not all Websites Publish a Privacy Policy

In 1998, the Federal Trade Commission (1998) found that only 16% of 621 US websites that collected personal data published information about the processing of personal data. Since then, the proportion of websites publishing a privacy policy has increased. Kleen and Heinrichs’ (2007) longitudinal study found that 80% of companies listed in the Fortune 100 (a ranking of US organisations based on revenue published by Fortune (2018)) published a privacy policy in 2001 rising to 93% in 2006. More recently, Case, King and Carl (2015) found that 94% of the Fortune 500 companies published a privacy policy while Degeling et al (2018) highlighted that almost 85% of European websites published a privacy policy after the introduction of the GDPR. That said, evidence suggests publication is not ubiquitous. Zaeem and Barber (2017) found that over 30% of six hundred companies listed on New York Stock Exchange, NASDAQ and AMAX stock markets did not publish a privacy policy. Tjhin, Vos and Managanuri (2016) found that one fifth of websites from New Zealand published no privacy policy. In the public sector, Dias, Gomes and Zuquete (2016) showed that just 26% of Portuguese local government websites published a privacy policy.

2.6.2 Problem Two: The Publication of Relevant Information Is Not Consistent

Much of the evaluation of privacy policy content has involved the fair information practices. In the United States, the Federal Trade Commission (2000) recommended that organisations that collected personal data online comply with the four fair information practices (FIPs). The FIPs consist of: notice, choice, access, security. Notice involves informing individuals that personal data processing is going to take place; choice involves giving individuals some option as to how their personal data is used; access involves giving individuals the opportunity to view personal data being processed and security involves providing appropriate safeguards for personal data. These principles have been used as a framework to analyse privacy policy statements.

Recent studies report a consistently high proportion of privacy policies providing notice. Cha (2011) found that over 90% of US and Korean website privacy policies mentioned how personal data would be used. Similar results were reported by Hooper and Vos (2009); they found that 95% of websites from New Zealand based organisations identified at least one reason why personal data was being collected. In addition, most of the Fortune 500 companies either partially (98%) or fully (88%) complied with the notice requirements of the fair information practices (Schwaig, Kane, & Storey, 2006). In the UK, Mundy (2006) found that 25 out of 27 healthcare website privacy policies mentioned the purposes for processing personal data.

The principle of choice allows: *“consumers to control whether their data is collected and how it is used”* (Federal Trade Commission, 2012, p. 35). Findings published by the Federal Trade Commission (1998) in 1998 showed that just 33% of US websites that collected personal data and published information about processing provided consumers with some degree of choice about how their personal data could be used. Communication of choice has improved somewhat more recently but studies still suggest that choice is not consistently provided to data subjects. Cha (2011) reported that approximately two thirds of privacy policies from websites in the United States offered users the choice to opt in or opt out of personal data being used for direct marketing purposes. In the same study, less than 60% of privacy policies from websites in the United States provided consumers with the option to prevent personal data being used for direct marketing. Cranor et al (2015) found that a quarter of privacy policies published by online advertising organisations based in the United

States did not offer any choice to limit the merging of personal and non-personal data even though their privacy policies did suggest that such merging was a possibility.

The principle of access involves informing data subjects that they can review personal data being processed and amend or remove inaccurate personal data. The Federal Trade Commission study showed that in 1998 only 10% of websites that collected personal data and published an information disclosure provided consumers with the opportunity to access personal data. In the context of UK healthcare websites, Mundy (2006) found that only 41% of privacy policies stated that individuals have the right to access a copy of personal data being processed. Since 2006 research has shown some improvement. Cha (2011) reported that 61% of privacy policies from websites in the United States mentioned that consumers could review personal data while 68% stated that amendments to personal data was permitted. Furthermore, Tjhin, Vos and Managanuri (2016) found that 68% of privacy policies from websites in New Zealand mentioned the ability to access personal data and 63% highlighted that personal data could be corrected.

Privacy policies fall short when disclosing the security procedures and the methods used to protect personal data from unauthorised access. Just 15% of websites in the Federal Trade Commission's 1998 study that collected personal data and published an information disclosure stated the steps taken to secure personal data (Federal Trade Commission, 1998). Improvements have been made since then but there remains little evidence of consistent disclosure of security information. For example, in the Netherlands, Beldad, De Jong and Steehouder (2009) reported that only one fifth of municipal websites that collected personal data explained the technologies that would be used to keep personal data secure. In addition, Li and Zhang (2009) highlighted that less than 30% of the Fortune 100 website privacy policies discussed the use of standard secure socket layer technology used to encrypt personal data transmission. That said, more recently Tjhin, Vos and Managanuri (2016) did report that 70% of privacy policies from New Zealand based websites mentioned the steps taken to secure personal data.

Further to the fair information practices mentioned, the principle of retention has also been studied. Findings show that retention is the most poorly communicated information provision. In Beldad, De Jong and Steehouder's (2009) study, two thirds of Dutch municipal website privacy policies did not mention for how long personal data would be retained. In addition, four fifths of online advertising organisations that were not members of the National Advertising Initiative or the Digital Advertising Alliance did not mention for how long non-personal data would be stored (Cranor *et al.*, 2015). In the UK, Mundy (2006) reported that out of the 27 UK healthcare privacy policies reviewed, only six described what would happen to personal data after processing was no longer required.

2.6.3 Problem Three: There Are Mismatches Between Published Information and User Beliefs and Expectations

Earp et al (2005) compared the information disclosed within twenty four website privacy policies to user privacy attitudes. Findings from this study revealed that users were most concerned about: (a) the transfer of personal data, (b) the accessibility of personal data and (c) the storage of personal data. Earp et al’s (2005) analysis of privacy policies showed that disclosure relating to the storage of personal data and communication about accessing personal data received little attention in privacy policies. In fact, Earp et al (2005) only found evidence of two statements that related to the storage of personal data among twenty four privacy policies. Rao et al (2016) compared user expectations to data practices outlined in privacy policies. Rao et al found mismatches between expectations and practice regarding the collection of contact information. Website users felt that organisations would not collect contact information when the user did not have an account with the website, however organisations did carry out this practice. Users also felt that websites would not collect financial information without the user registering for an account, however privacy policies mentioned that this practice does occur. Finally, privacy policies mentioned that contact information would not be shared for purposes that were not part of the service the user was requesting. In this case, users typically felt that organisations would carry out this data sharing practice.

2.6.4 Problem Four: Privacy policies are Difficult to Understand

McLaughlin (1968, p. 188) defined readability as: “the degree to which a given class of people find certain reading matter compelling and, necessarily, comprehensible.” Readability formulas are a statistical measure of readability. The Flesch Readability Ease Score (FRES) and Flesch-Kincaid grade level have been frequently used to assess the readability of privacy policies. FRES (Flesch, 1948) takes into account the average number of words per sentence and the average number of syllables per word in each passage of text. FRES output is a score between 0 and 100. The higher the average number of words per sentence and syllables per word the lower the FRES. The lower the score the more difficult the passage of text is to read. Flesch grouped scores into seven categories ranging from very difficult to read to very easy to read. Flesch's categorisation of scores is shown in table 2.5. Flesch (1979) states that the minimum score for "plain English" is 60.

Research has consistently shown that privacy policies fall in the 30-49 FRES bracket. For example, Proctor, Ali and Vu (2008) found a mean score of 29.39 for a sample of pharmacy website privacy policies; retail website policies scored a mean of 37.27; financial website policies scored a mean of 35.59 and insurance website policies scored a mean of 37.84. In addition, Sumeeth, Singh and Miller (2010) reported a mean FRES of 43.5 for a sample of high traffic websites. Under the logic of Flesch, these findings suggest that privacy policies are difficult to read. To add some context to those findings a sample of academic articles from the Journal of Property Investment and Finance achieved a mean FRES of 30.4 (Lee and French, 2011) while a sample of research studies from four marketing journals scored a mean FRES of 35.3 (Sawyer, Laran and Xu, 2008).

Flesch readability ease score	Reading difficulty
0 - 29	Very difficult
30-49	Difficult
50-59	Fairly difficult
60-69	Standard
70-79	Fairly easy
80-89	Easy
90-100	Very easy

Table 2.5 - Flesch readability ease scores (Flesch 1948)

The Flesch-Kincaid grade level (Kincaid *et al.*, 1975) uses a similar methodology to the FRES to output a numeric score equivalent to a school grade level in the United States. Milne, Culnan and Greene (2006) found that a sample of high traffic websites scored a mean Flesch-Kincaid grade level of 12.3 while Sumeeth, Singh and Miller (2010) reported a mean grade level of 12.9. A study of websites from New Zealand found a mean Flesch-Kincaid grade level of 13 (Tjhin, Vos and Munaganuri, 2016). These findings suggest that individuals in the UK would need to be educated to either college or university level to be able to read and understand privacy policies.

The cloze test has also been used as a method to assess the readability of privacy policies. Singh, Sumeeth and Miller (2011) used a cloze test score of 0.6 as a threshold to determine whether a privacy policy was difficult to read. Their results showed that only 12 out of 50 participants met their 0.6 cloze test threshold while only one privacy policy from the ten they examined had a mean cloze test score greater than 0.6. In addition, the authors also found a significant positive correlation between FRES and cloze test score. This provides further validation to support those studies that have used the FRES to infer the difficulty associated with read privacy policies.

2.6.5 Problem Five: Privacy Policy Language Can Obscure the Truth

Authors have suggested that organisations deliberately use vague terminology to obscure reality. Pollach's (2005) typology of communicative strategies highlights the policy language used to blur the truth. Privacy policies tend to emphasise the qualities associated with certain practices. For example, organisations use phases such as *"carefully selected third parties"* to suggest that a degree of rigor has been placed into the process of selecting parties that personal data will or might be shared with. Furthermore, privacy policies use terms such as *"occasionally"* and *"may"* to downplay the probability that a data processing practice may occur. In addition, policies use terms that appear to reduce the commitment of the organisation processing personal data. For example, phrases akin to *"you will receive emails"* as opposed to *"we will send you information"* attempt to background the role of the organisation processing personal data.

Bhatia et al (2016) categorised vague terminology into four groups. The conditionality category contains terms such as: "depending", "necessary", "appropriate" and "as needed". These terms indicate the action to be performed is dependent upon a variable or unclear trigger. The generalisation category includes terms such as: "generally", "usually", "typically" and "mostly". The words in this category suggest that the actions to be performed have unclear conditions. The modality category contains terms such as: "may", "might", "could", "would" and "likely". These terms suggest the likelihood of an action is ambiguous. The numeric quantifier category includes terms such as: *"certain"*, *"most"* or *"some"*. These words indicate an action has a vague quantifiable element. Bhatia et al (2016) reported that almost four fifths of vague terms found in a survey of fifteen privacy policies were considered modal. Table 2.6 shows the distribution of vague terms found by Bhatia et al (2016). Pollach (2007) found 948 instances of the term "*may"* within a sample of fifty privacy policies and 123 instances of the terms *"might", "perhaps", "occasionally", "sometimes" and "from time to time"*.

Examples of statements including this terminology include: *“we may share information with carefully selected vendors”* and *“from time to time, on a limited basis, we share with trustworthy third parties contact information of registered users”* (Pollach, 2005). In practice, as Polloch (2005) notes, these terms provide little assurance about whether a practice is carried out leaving the user unsure about how personal data is really being processed.

	Vague terms			
Policy	Conditionality	Generalisation	Modality	Numeric quantifier
Barnes and Noble	12	4	98	17
Costco	6	7	50	1
JC Penny	6	0	29	5
Lowes	2	0	62	6
OverStock	1	1	19	3
AT&T	3	0	52	0
CharterComm	8	4	81	12
Comcast	20	9	91	9
Time Warner	1	6	47	18
Verizon	14	1	101	12
Career Builder	1	3	28	4
GlassDoor	5	3	42	6
Indeed	0	1	33	4
Monster	3	0	28	1
Simply Hired	1	3	55	8

Table 2.6 - Distribution of vague terms adopted from Bhatia et al (2016, p. 31)

2.6.6 Problem Six: There Are Mismatches Between Policy Meaning and User Understanding

Studies show users interpret privacy policies differently. Reidenberg et al (2015) found that expert law scholars, knowledgeable graduates and Amazon Mechanical Turk crowd workers had different interpretations of privacy policy statements. Expert law scholars showed only 50% agreement when asked whether health personal data would be shared. Furthermore, two thirds agreement was reached between experts when asked whether financial or location information would be shared. Crowd workers showed a similar trend of disagreement with each other. Overall, under two thirds of crowd workers gave the same response when asked whether contact, financial or location data would be shared.

Martin (2015) presented users with various data practice statements that described online personal data tracking scenarios. Users were asked to rate the degree to which personal data tracking scenarios conformed to a privacy policy. Unbeknown to the research participants, all the online tracking scenarios used in the study conformed to the privacy policy. Users felt that, on average, the scenarios described did not conform to the privacy policy. The findings suggested the presence of a mismatch between user perceptions of online tracking practices and the protections provided within privacy policies (Martin, 2015). In addition, McRobb (2006) found that university students also disagreed on the interpretation of privacy policies. Disagreement was strongest when students were deciding whether privacy policies provided the option to opt out of personal data collection and personal data sharing.

2.6.7 Problem Seven: Privacy Policies Take Too Long to Read

Fabian, Ermakova and Lentz’s (2017) study of almost fifty thousand privacy policies showed that the average length of a privacy policy is one thousand seven hundred words. Findings from the same study revealed that on average privacy policies contain seventy sentences. McDonald and Cranor (2008) estimated the time it would take individual American internet users and the entire American online population to read the privacy policy of each website visited annually. They suggested it would take an individual 244 hours per year to read the privacy policy of each website they visited. In addition, they also suggested it would take the entire online American population 53.8 billion hours per year to do the same.

2.6.8 Problem Eight: Privacy Policies Are Not Displayed In a Friendly Format

McRobb and Rogerson (2004) reported that two thirds of privacy policies from various industry sectors and countries were presented as a block of text with no structure. Given the potentially large amount of information to communicate within a privacy policy, websites can also insert links (HTML anchors) to allow quicker navigation to specific parts of the policy. Research carried out by Rains and Bosch (2009) showed that only a small proportion of healthcare website privacy policies utilised this format.

Websites can also break down the presentation of policy information by publishing a privacy statement over several webpages. Jensen and Potts (2004) found that 22%

of high traffic and healthcare privacy policies were split over more than one webpage. Multipage policies, as Jensen and Potts (2004) refer to it, often have one main policy page with links to additional pages with definitions and additional details. While this may be beneficial in terms of publishing less information on one single webpage there is also potential to hide or obscure important policy information away from the main privacy statement itself. Jensen and Potts (2004) present evidence to suggest this is a tactic used by a small number of websites. Recent evidence suggests that alternative policy layout formats, such as layered notices, are not being adopted in practice. Incremental presentation of policy information is the principle that underpins layered privacy policies. The idea is that organisations publish a short and full layer. The short layer should provide basic policy information; the full layer provides more policy detail. Law firm Hunton and Williams (2006) were the first organisation to develop layered privacy policy guidance. However, Kelley et al (2010) and Cranor (2013) were critical of the Hunton and Williams (2006) layered notice. They suggested that the notice was too flexible and allowed organisations to decide how much information to include in the different layers of the privacy policy. Langhorne (2014) found no evidence of layered privacy policies in her content analysis of sixteen higher education websites in the United States.

2.6.9 Problem Nine: Privacy Policies Are Not Always Truthful Accounts of Personal Data Processing

Almost three in five individuals surveyed in the ICO *Annual Track* do not feel that businesses are transparent about their use of personal data (Citizenme, 2016). In some cases, user beliefs are not unfounded. For example, sales lead generation organisation, Verso Group (UK) were fined by the Information Commissioner’s Office for not properly informing users about the disclosure of personal data. The ICO concluded that:

> “Verso failed to provide data subjects with sufficiently clear information about the companies to whom Verso intended to disclose their personal data for direct marketing purposes. Neither Verso’s telephone call scripts nor its website provided sufficiently clear information in this respect” (Information Commissioner’s Office, 2017, p. 8).

In addition, online pharmacy, Pharmacy2U, were found to be advertising the sale of consumer personal data for £130 per 1000 records. The Information Commissioner judged that the organisation had not informed consumers that personal data would be sold and therefore Pharmacy2U were considered to be processing personal data unfairly (Information Commissioner’s Office, 2015). Furthermore, Lifecycle Marketing (Mother and Baby) Ltd knowingly supplied personal data to Experian that would then be processed for political purposes by the Labour party. However, the organisation’s privacy policy made no mention that personal data would be shared with the Labour party or that personal data would be used for political purposes. The ICO concluded: *“based on the information LCMB provided, data subjects would not have foreseen that their data would be shared with a political party”* (Information Commissioner’s Office, 2018b, p. 7).

2.7 Addressing the Problems: What Has Been Done So Far?

Over the last fifteen years numerous projects have attempted to address the shortcomings of privacy policies. Perhaps the most significant of these projects was the Platform for Privacy Preferences (P3P) project led by academic Lorrie Cranor. A description of this project is outlined below. Afterwards, an overview of other notable attempts to overcome the limitations of privacy policies is provided.

2.7.1 Platform for Privacy Preferences

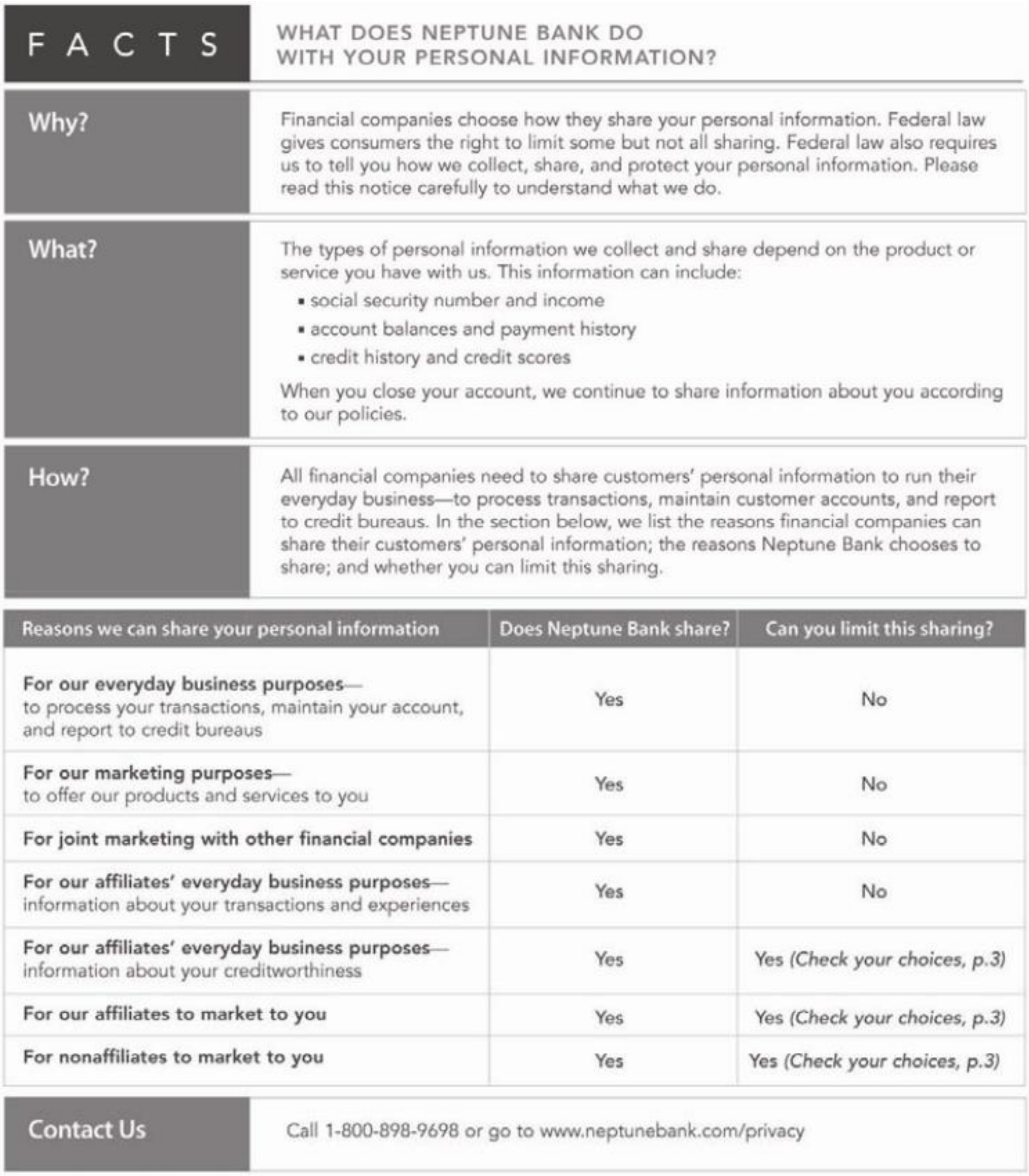
The Platform for Privacy Preferences (P3P) project was designed to allow website users to easily obtain information about personal data processing practices. Cranor et al (2008) note that the purpose of P3P was to allow users to specify their privacy preferences to a web browser prior to visiting a website. Organisations would then specify their privacy policies using the P3P XML format. When a user visits a website, the web browser would automatically compare the user’s specified preferences with the organisation’s practices. The user would then be notified if a mismatched preference was found. Data revealed the number of P3P policies increased between 2003 and 2006 (Cranor *et al.*, 2008), however full adoption of the P3P policies was never reached. Cranor (2012) notes the tension between the complexity of the P3P specification and desire for a more expressive P3P vocabulary. Some organisations argued for a more expressive vocabulary to capture every element of personal data processing while some organisations argued for a more simplistic approach to allow for practical implementation.

2.7.2 Financial Privacy Notices

In 2004 the Kleinmann Communication Group (KCG) were commissioned to develop a paper-based privacy policy that would be easy for consumers to understand and help organisations achieve compliance with the Gramm-Leach-Bliley Act (GLBA). The GLBA required U.S. financial institutions to provide consumers with an annual notice of personal data handling practices. The final KCG design is shown in figure 2.2, figure 2.3 and figure 2.4 (Kleinmann Communication Group, 2006). In 2009, eight Federal Agencies released a final version of the model privacy notice (Office of the Federal Register, 2009). It is not obligatory for organisations to adopt the standardised notice (Office of the Federal Register, 2009) although in 2013, Cranor (2013) claimed that almost 100% of U.S financial banks have adopted the standardised notice.

The KCG policy features three pages. The first page provides information on the categories of personal data that are processed and why they are processed. The first page also includes a disclosure table outlining who personal data is shared with and whether consumers can opt out of such sharing. The second page describes the protections in place to ensure any personal data processed remains secure. In addition, the second page describes the point at which personal data is collected. This page also contains a table outlining the definitions of terms used on page one. The final page is an opt out form giving consumers the opportunity to prevent their personal data being used for the purposes specified on page one.

Simplicity is a strength of the KCG policy. The KCG (2006) report highlighted that consumers found the disclosure table accessible and understandable. Furthermore, consumers also found that the disclosure table allowed for a comparison of sharing practices across different financial organisations. That said, the KCG privacy policy was designed primarily for financial institutions to achieve compliance with the GLBA in the U.S. This legislation is not applicable in the U.K and therefore the policy design would not be wholly suitable for U.K. organisations. The design does not include any provisions for describing the rights of access and rectification of personal data outlined in the GDPR (and Data Protection Act 1998). Additionally, KCG design does not mention anything about cookies or other technologies used to profile individuals.



FACTS

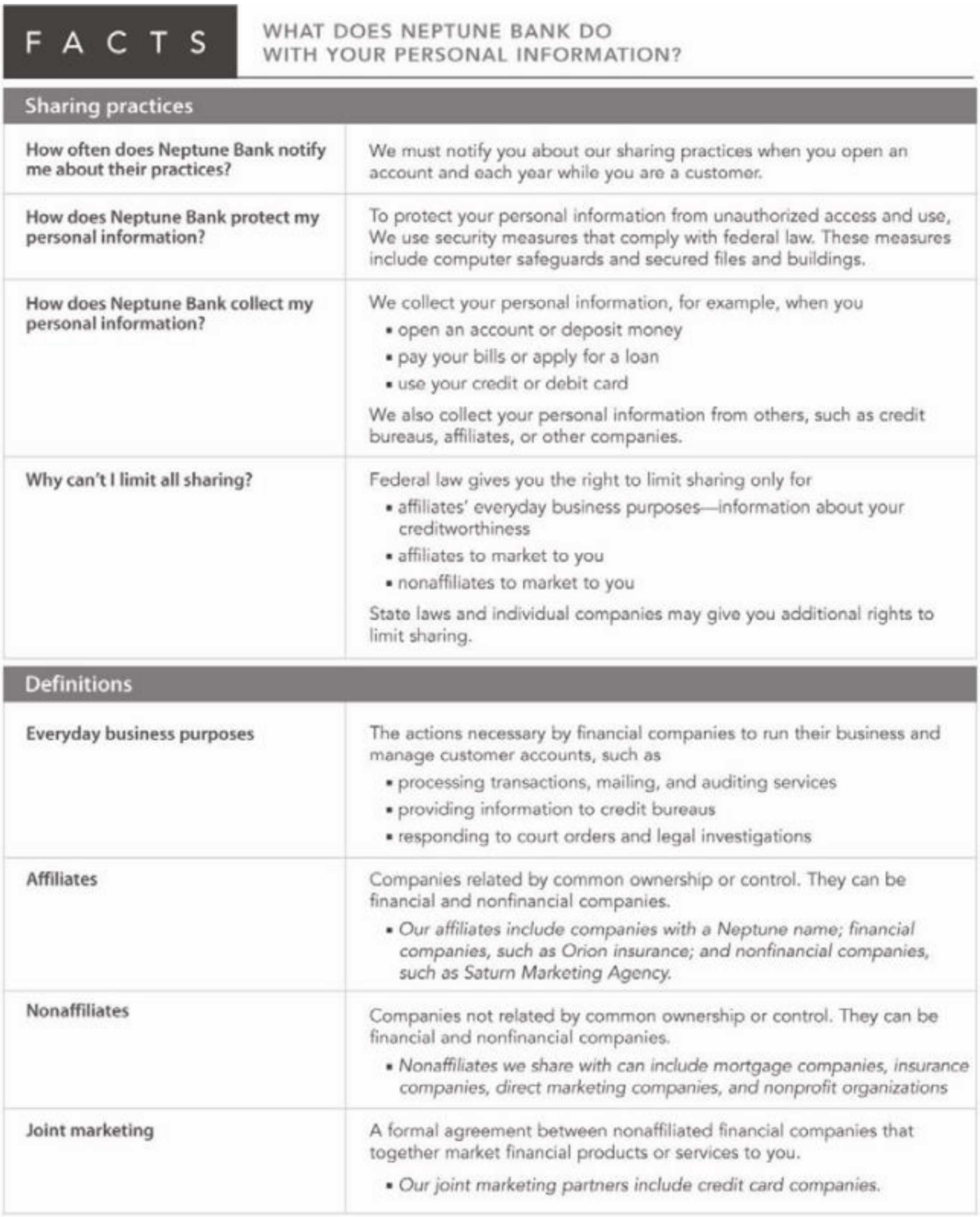
WHAT DOES NEPTUNE BANK DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ social security number and income ▪ account balances and payment history ▪ credit history and credit scores When you close your account, we continue to share information about you according to our policies.
How?	All financial companies need to share customers' personal information to run their everyday business—to process transactions, maintain customer accounts, and report to credit bureaus. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Neptune Bank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Neptune Bank share?	Can you limit this sharing?
For our everyday business purposes— to process your transactions, maintain your account, and report to credit bureaus	Yes	No
For our marketing purposes— to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes— information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes— information about your creditworthiness	Yes	Yes *(Check your choices, p.3)*
For our affiliates to market to you	Yes	Yes *(Check your choices, p.3)*
For nonaffiliates to market to you	Yes	Yes *(Check your choices, p.3)*

Contact Us	Call 1-800-898-9698 or go to www.neptunebank.com/privacy

Figure 2.2 - Kleimann Communication Group (2006) privacy policy page 1



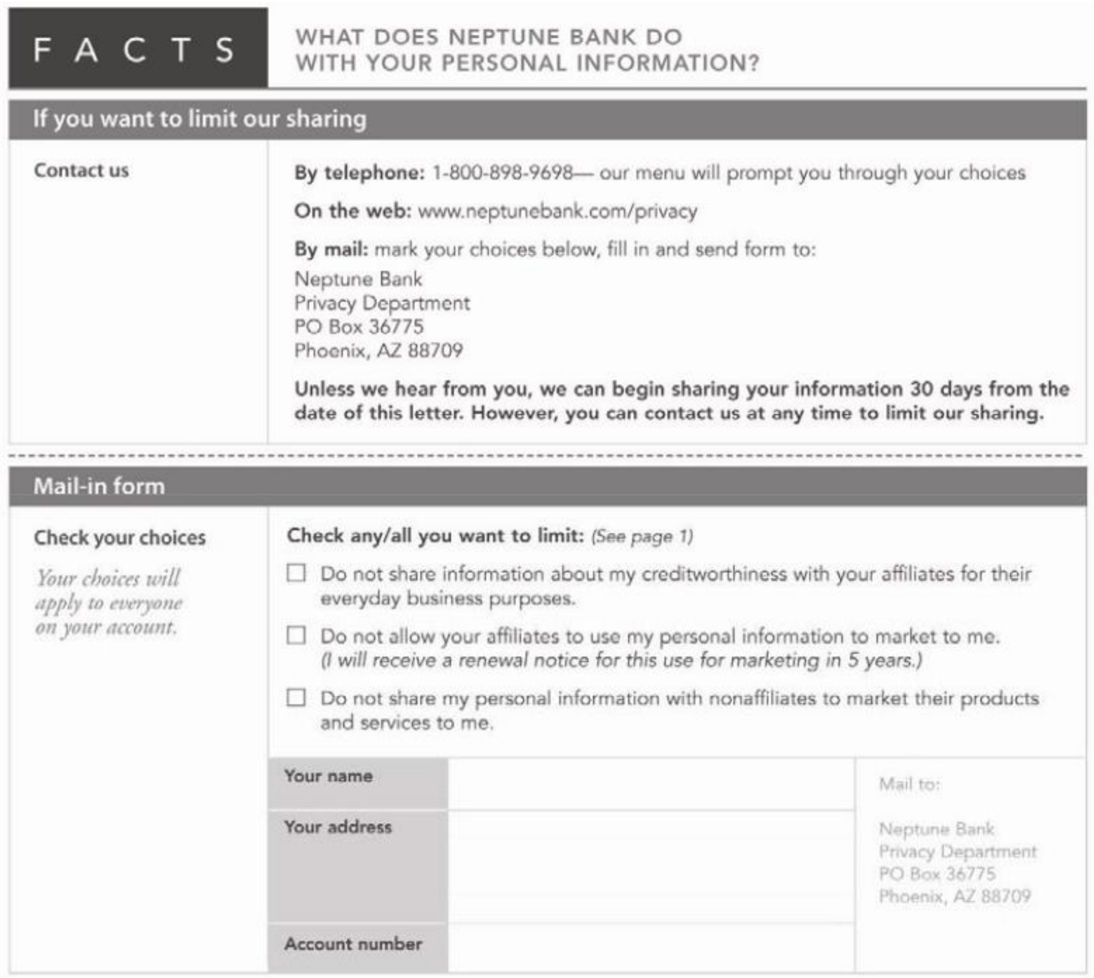
FACTS

WHAT DOES NEPTUNE BANK DO WITH YOUR PERSONAL INFORMATION?

Sharing practices	
How often does Neptune Bank notify me about their practices?	We must notify you about our sharing practices when you open an account and each year while you are a customer.
How does Neptune Bank protect my personal information?	To protect your personal information from unauthorized access and use, We use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
How does Neptune Bank collect my personal information?	We collect your personal information, for example, when you ▪ open an account or deposit money ▪ pay your bills or apply for a loan ▪ use your credit or debit card We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit sharing only for ▪ affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates to market to you ▪ nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing.

Definitions	
Everyday business purposes	The actions necessary by financial companies to run their business and manage customer accounts, such as ▪ processing transactions, mailing, and auditing services ▪ providing information to credit bureaus ▪ responding to court orders and legal investigations
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *Our affiliates include companies with a Neptune name; financial companies, such as Orion insurance; and nonfinancial companies, such as Saturn Marketing Agency.*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *Nonaffiliates we share with can include mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *Our joint marketing partners include credit card companies.*

Figure 2.3 - Kleimann Communication Group (2006) privacy policy page 2



FACTS

WHAT DOES NEPTUNE BANK DO
WITH YOUR PERSONAL INFORMATION?

If you want to limit our sharing

Contact us

By telephone: 1-800-898-9698— our menu will prompt you through your choices

On the web: www.neptunebank.com/privacy

By mail: mark your choices below, fill in and send form to:

Neptune Bank
Privacy Department
PO Box 36775
Phoenix, AZ 88709

Unless we hear from you, we can begin sharing your information 30 days from the date of this letter. However, you can contact us at any time to limit our sharing.

Mail-in form

Check your choices

Your choices will apply to everyone on your account.

Check any/all you want to limit: *(See page 1)*

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

□ Do not allow your affiliates to use my personal information to market to me.
(I will receive a renewal notice for this use for marketing in 5 years.)

□ Do not share my personal information with nonaffiliates to market their products and services to me.

Your name		Mail to: Neptune Bank Privacy Department PO Box 36775 Phoenix, AZ 88709
Your address		
Account number		

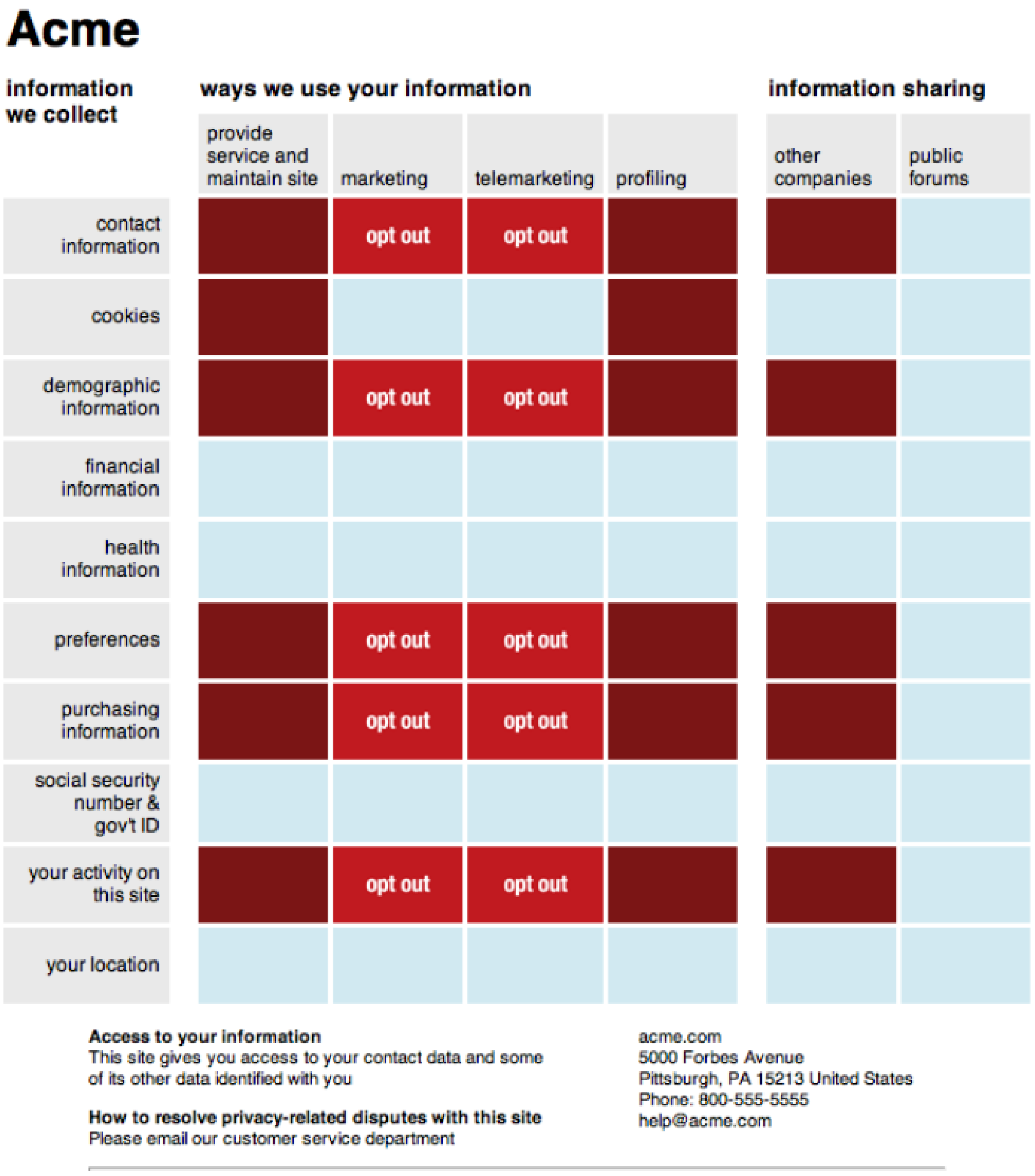
Figure 2.4 - Kleimann Communication Group (2006) privacy policy page 3

2.7.3 Privacy Label

Inspired by labelling efforts in other goods sectors, Kelley et al (2009) designed a privacy “nutrition” label. The label, shown in figure 2.5 and figure 2.6, uses a two-dimensional grid to display policy information. The grid specifies ten types of information that organisations might collect and six possible uses of personal information. Organisations then specify whether (or not) personal data is collected for each use. A unique colour and symbol is attached to each part of the grid to show whether the type of personal information is collected by means of opt out (collected by default unless the users opts in) or opt in (not collected by default unless the user opts in).

Kelley et al (2009) reported that the privacy nutrition label allowed users to find information quicker than natural language policies. Individuals also answered questions with more accuracy using the standardised table compared to natural language policies. That said, the privacy nutrition label was designed based on the

P3P specification that was not widely adopted by websites. Cranor (2012) does note that the nutrition label can be implemented manually although it is difficult to imagine that organisations would want to do this if they are unhappy with the underlying principles of P3P.



Acme

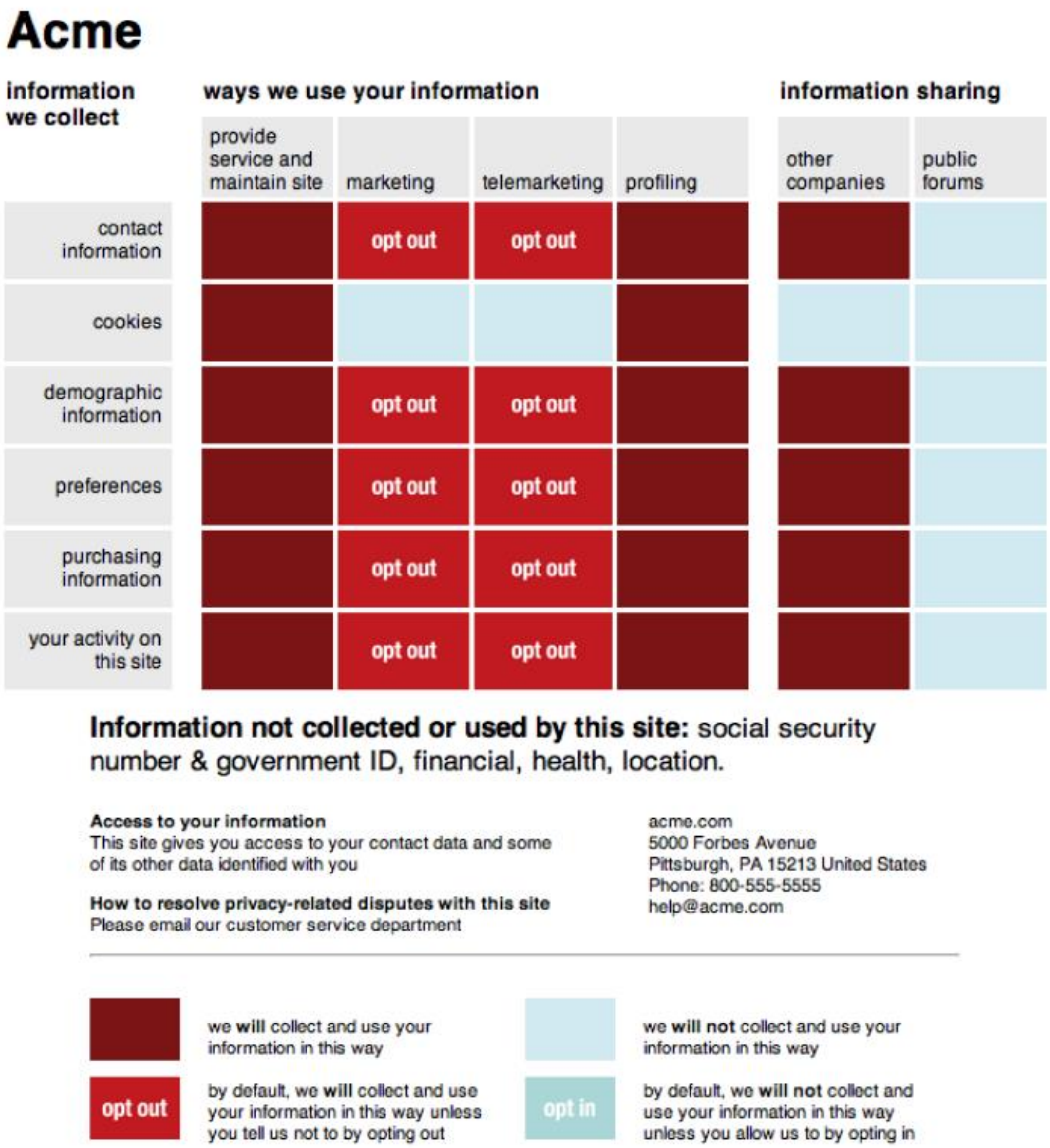
information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	■	opt out	opt out	■	■	□
cookies	■	□	□	■	□	□
demographic information	■	opt out	opt out	■	■	□
financial information	□	□	□	□	□	□
health information	□	□	□	□	□	□
preferences	■	opt out	opt out	■	■	□
purchasing information	■	opt out	opt out	■	■	□
social security number & gov't ID	□	□	□	□	□	□
your activity on this site	■	opt out	opt out	■	■	□
your location	□	□	□	□	□	□

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

Figure 2.5 - Privacy nutrition label (Kelley et al 2009)



Acme

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	■	opt out	opt out	■	■	□
cookies	■	□	□	■	□	□
demographic information	■	opt out	opt out	■	■	□
preferences	■	opt out	opt out	■	■	□
purchasing information	■	opt out	opt out	■	■	□
your activity on this site	■	opt out	opt out	■	■	□

Information not collected or used by this site: social security number & government ID, financial, health, location.

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

■	we **will** collect and use your information in this way	□	we **will not** collect and use your information in this way
opt out	by default, we **will** collect and use your information in this way unless you tell us not to by opting out	opt in	by default, we **will not** collect and use your information in this way unless you allow us to by opting in

Figure 2.6 - Privacy nutrition label (Kelley et al 2009)

2.7.4 Privacy Icons

Privacy icons are: "simplified pictures expressing privacy related statements" (Holtz, Nocun and Hansen, 2011, p. 339). Article 12 of the GDPR states that information provided to the data subject might be combined with standardised, machine readable icons. To date, several different icon sets have been proposed although the PrimeLife project is the most notable attempt in Europe to apply the principles of iconography to privacy policies. Funded by the European Union, the PrimeLife project designed a series of privacy icons (Holtz, Nocun and Hansen, 2011). The icons were not designed to replace privacy policies, but to supplement policy content. The PrimeLife icons shown in figure 2.7 were designed for use across different scenarios, including e-commerce and social networks. The icons were designed to represent the different categories of personal data that might be processed along with policy decisions such as how long personal data would be processed for. The icons were tested with Swedish and Chinese internet users. Overall, the seventeen PrimeLife Icons were considered to be too complicated (Edwards and Abel, 2014). Findings revealed that cultural interpretations of the icons varied. The PrimeLife icons were never adopted in practice. As a result, there is little data to show how effective they really are.

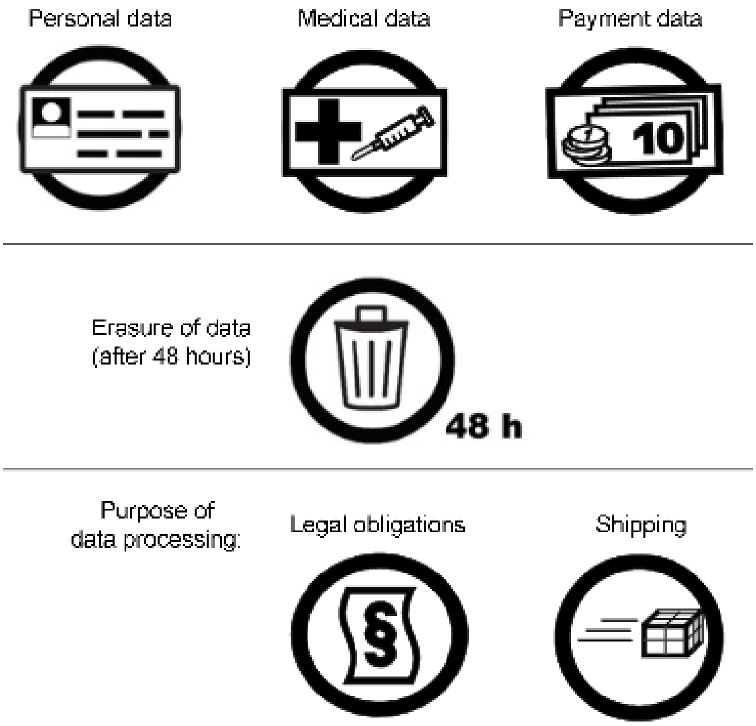


Figure 2.7 - First iteration PrimeLife Icons (Holtz, Nocun and Hansen 2011)

2.7.5 Standardisation

Standardisation is the concept that underpins the policy design efforts already mentioned. The Privacy Framework developed by the Federal Trade Commission (2012, p. 61) stated: “privacy notices should be clearer, shorter and more standardized to enable better comprehension and comparison of privacy practices.” Lorrie Cranor (2012) has long been an advocate of policy standardisation. The familiarity of standardised privacy policies is beneficial to consumers (Cranor, 2012). Kelly et al (2010) showed that time to retrieve and compare information between privacy policies were significantly better for standardised labelled formats than they were for natural language privacy policies. The principle of standardisation is also mentioned in the GDPR. Article 12(7) (European Parliament and Council, 2016, p. 40) states: “the information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give an easily visible, intelligible and clearly legible manner a meaningful overview of intended processing."

2.7.6 Privacy by Design: User Centricity and Layered Notices

The concept of privacy by design was introduced in section 2.5. Cavoukian (2011) suggests that privacy by design can achieved by following seven principles, they are: (1) proactivity not reactivity, (2) privacy as a default setting, (3) privacy embedded into the design of systems, (4) full functionality avoiding trade-offs, (5) end to end security, (6) visibility and transparency and (7) user centricity. The principle of user centricity ensures that end users are the focus of engineering efforts. Cavoukian (n.d, p.5) states that: "the best privacy by design results are usually those that are consciously designed around the interests and needs of individual users, who have the greatest vested interest in the management of their own personal data." To achieve user centricity organisations should engage with users throughout the lifecycle of systems development. Funded by the European Union, the Pirpare (PReparing Industry to Privacy-by-design by supporting its Application in Research) methodology provides guidance to help organisations embed the principles of privacy by design into systems development. Pripare (Garica, McDonnell and Troncoso et al, 2015) highlights a user centred design process that could be used to shape the development of a privacy user interface, including the creation of privacy policies. Pripare suggests that practitioners should understand and specify the context in which privacy policy is going to be used, develop interactive prototypes to demonstrate functionality and then evaluate the interface to test whether it meets the needs of users.

Further, Pripare indicates that practitioners might wish to consult guidance on layered privacy policies when considering options for privacy user interface development. The Information Commissioner (2019) and the Article 29 Working Party (2018a, 2018b) support the publication of layered privacy policies, however, there is little evidence based guidance to support organisations wishing to implement layered privacy policies. Section 2.6.9 of this thesis identified that that layered privacy policy guidance published by Hunton and Williams was considered too flexible (Kelley et al, 2010; Cranor, 2013). The ICO (Information Commissioner's Office, 2019) believes that:

> "there will always be pieces of information that are likely to need to go into the top layer, such as who you are, what information you are collecting and why you need it. What else goes into which layer will depend on the type of processing that you undertake. The ICO considers

> that data controllers have a degree of discretion as to what information they consider needs to go within each layer, based on the data controller's own knowledge of their processing."

Although, that said, in response to an ICO consultation on a privacy notices code of practice (Information Commissioner's Office, 2016b), organisations suggested that the code should: "make clear which information should go into which layer of a layered privacy notice". Evidence based advice supporting the construction of layered privacy policies including what a layered privacy policy should look like and prescriptive information about what information should be published in each layer would help organisations to construct better, more user centred privacy notices.

2.7.7 Natural Language Processing

Most recently, artificial intelligence and natural language processing techniques have been applied to privacy policies. Polisis (2017) uses an automated framework to query privacy policies and present the findings in a visual format (Harkous et al, 2018). The Usable Privacy Project (2017) is aiming to use machine learning techniques to extract privacy policy features and present these features in a user-friendly format (Sadeh et al, 2014). At the time of writing, both Polisis and the Usable Privacy Project can be used to view annotated versions of privacy policies.

2.8 Summary

This literature review has shown the complexity associated with defining privacy. Privacy is contextually dependant and rooted in individual preferences. That said, survey data shows that individuals are concerned about the processing of personal data. Only a quarter of UK adults trust businesses with their personal data and internet brands are the least trusted by people in the UK (Citizenme, 2016). One contemporary practice causing concern is profiling. European consumers are worried about the ability of organisations to monitor behaviour and combine data from several sources to build a rich behavioural profile. In addition, two thirds of UK adults feel that organisations are not transparent when processing personal data (Citizenme, 2016).

The GDPR requires UK organisations to provide information about the processing of personal data to data subjects. This information is provided in a privacy policy. However, the literature review found evidence of nine privacy policy problem areas, namely:

1. There are still organisations that do not publish information about the processing of personal data;
2. Relevant policy information is not consistently communicated in privacy policies;
3. There are mismatches between published information and user beliefs and expectations;
4. Privacy policies are difficult to read;
5. The language used in privacy policies can obscure the truth;
6. There are mismatches between policy meaning and user understanding;
7. Privacy policies take too long to read;
8. Privacy policies are not displayed in a friendly format; and
9. Privacy policies are not always a truthful account of personal data processing practices.

Efforts have been made to address the problems with privacy policies. Machine readable privacy policies, privacy labels and privacy icons have all been proposed however widescale change has not been achieved. Overall, although there has been a considerable corpus of privacy policy research carried out, to date, there has been no systematic review of UK privacy policies. The majority of privacy policy studies have been carried out in the United States with a focus on large international organisations. This, along with the introduction of the GDPR, provided an important and timely research gap that needed to be addressed.

Chapter 3 - Research Methodology

The aim of this research was **to explore how UK e-commerce privacy policies could be improved**. This chapter outlines the methodological decisions taken to address this research aim. The philosophical underpinnings of this research are described. Following that is a discussion of the research design and methods used to collect data. At the end of this chapter research quality and ethics are explained in the context of the research carried out.

3.1 The Nature of Research

Paradigms have become a fundamental concept in social science methodology. Guba and Lincoln (1994, p.116) stated that: "paradigm issues are crucial; no inquirer, we maintain, ought to go about the business of inquiry without being clear about just what paradigm informs and guides his or her approach." Kuhn (1962, p.23) defined a paradigm as an: "accepted model or pattern" that informs the beliefs and practice of a research field. In social science, ontological, epistemological and methodological positions characterise different paradigms. Ontology refers to the nature of social reality (Blaikie, 1993). Epistemology refers to: "the claims or assumptions made about the ways in which it is possible to gain knowledge about social reality" (Blaikie, 1993, p.6). Methodology is the: "strategy, plan of action, process or design" that shapes the choice and use of research methods (Crotty, 1998, p.3). Positivism and constructivism are paradigms often contrasted in social research methodology textbooks because of their different ontological, epistemological and methodological stances. The ontological, epistemological and methodological characteristics of positivism and constructivism are outlined in table 3.1.

Ontological and epistemological beliefs inform the methodology used in an inquiry (Crotty, 1998, p.4). That said, Morgan (2007) questioned the practical nature of the relationship between ontology/epistemology, and research methodology. One of Morgan's (2007, p. 52) criticisms is that although: "epistemological stances do draw attention to the deeper assumptions that researchers make, they tell us little about the more substantive decisions such as what to study and how to do so." He goes on to state that: "this combination of strong demands for self-conscious allegiance to one paradigm but less advice about how that should play out in the practices of "workaday" researchers created ongoing difficulties for the metaphysical paradigm" (Morgan, 2007, p.63).

	Positivism	Constructivism
Ontology	A single reality exists "out there" that can be predicted and controlled. Social reality consists of causal relations between variables. The causes are external to the individual.	There are multiple realities that are socially constructed. Social actors negotiate the meanings for actions and situations.
Epistemology	Knowledge is derived through observation. Concepts and generalisations are summaries of observation. The inquiry and object of inquiry are independent of each other.	Knowledge is derived through entering the social world to gather socially constructed meanings. The inquirer and the object of inquiry interact and influence each other.
Methodology	Mostly quantitative methods. Cross sectional and experimental research designs.	Mostly qualitative methods. Hermeneutics and phenomenological research design.

Table 3.1 - Characteristics of positivism and constructivism adopted from Lincoln and Guba (1985), Blaikie (1993), Gray (2009) and Onwuegbuzie, Johnson and Collins (2009).

Morgan (2007, p.65) believes that Khun's preferred meaning of a paradigm was a: "shared [set of] beliefs among a community of scholars" characterised by the nature of questions and answers in a research field. Morgan (2007, p.66) argues that a paradigm consists of a field "composed of groups of scholars who share a consensus about which questions are most important to study and which methods are most appropriate for conducting those studies". Under this logic, research questions and accepted methods underpin the decisions made at a methodological level within a research field. Morgan coined this the pragmatic approach to research.

The pragmatic approach rejects a: "top-down privileging of ontological assumptions in the metaphysical paradigm as simply too narrow an approach to issues in the philosophy of knowledge" (Morgan, 2007, p.68). Shaped by the philosophy of pragmatism, the pragmatic approach places the focus of research on societal problems and action (Creswell and Plano Clark, 2011). In this sense, the research problem informs the methodological decisions in a study. The pragmatic approach is not committed to one ontological or epistemological stance. For pragmatists, truth is characterised by what works at the time (Creswell, 2009). Ultimately the pragmatist works to provide the best understanding of the research problem at the time of inquiry. The characteristics of a pragmatic approach to research are outlined in table 3.2.

	Pragmatic approach
Communication and shared meaning	A degree of mutual understanding should be achieved between research colleagues and participants.
Transferability	The research findings of one study should be explored to understand whether they are useful in other circumstances.
Flexibility	Quantitative, qualitative and mixed methods approaches can form the basis of inquiry.
Ontology	Multiple realities exist. Current truth, meaning and knowledge are changing.
Epistemology	Knowledge is both constructed and based on the reality of the world we experience and live in. Justification of knowledge comes from warranted assertions.
Knowledge accumulation	The researcher constantly tries to improve upon past understandings in a way that fits and works in the world in which he or she operates in.

Table 3.2 - Characteristics of the pragmatic approach adopted from Morgan (2007), Onwuegbuzie, Johnson and Collins (2009) and Teddie and Tashakkori (2009).

The pragmatic approach underpinned the research methodology in this study. Adopting this approach was an acceptance that the research aim was addressed pragmatically based on the types of questions asked and methods used by those practising in the field of privacy and e-commerce research. The literature review highlighted several topical privacy research issues. Privacy policies are one of these contemporary issues. This suggested that the research aim was worthy of inquiry and likely to be of interest to privacy and e-commerce researchers. The literature review also showed a range of different methodological approaches have been used to address privacy related research questions. This suggested that a pragmatic approach to privacy policy research would be an acceptable strategy to those researchers working within this field.

3.2 Strategy of Inquiry

A strategy of inquiry refers to the types of quantitative, qualitative and mixed methods models that shape the design of procedures used in a study (Creswell, 2009). Typically, in quantitative research, there is a focus on the measurement of social concepts. Using numbers to measure phenomena offers one obvious strength; objective comparisons can be made between individuals and groups. Analysis of such data offers a structured approach to the generalisation of findings. In qualitative research social interaction is considered too complex to measure using few numerically defined variables. In this sense, qualitative research is concerned with capturing and describing an individual's construction of reality with a focus on different interpretations and meanings.

Howitt and Cramer (2011) compared quantitative and qualitative approaches to data collection and data analysis. In quantitative research, data is collected using highly structured materials (such as multiple-choice questionnaires) developed a priori. Data collection often takes place in an artificial environment designed for research (such as a laboratory). In comparison, in qualitative research, data is collected in a more naturalistic setting where the researcher aims to gather a rich picture of the topic under investigation. Less structured data collection approaches (such as observations and interviews) are used in these situations. Quantitative data analysis involves summarising data using descriptive statistics and inferring the probability that any findings can be generally applied. In qualitative research analytical approaches such as discourse analysis, conversation analysis and grounded theory are used to explore the underlying themes and patterns in the text data.

Adopting a pragmatic approach to research: "opens the door for multiple methods… as well as different forms of data collection and analysis" (Creswell, 2009, p.11). Johnson and Onwuegbuzie (2004, p.17) define mixed methods research as: "the class of research where the researcher mixes or combines quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study." Mixing quantitative and qualitative methods under one program of study provides the opportunity to address the biases inherent in either approach (Creswell, 2009). Creswell and Plano Clark (2011) describe several situations where mixed methods designs are useful; namely when there is a need to:

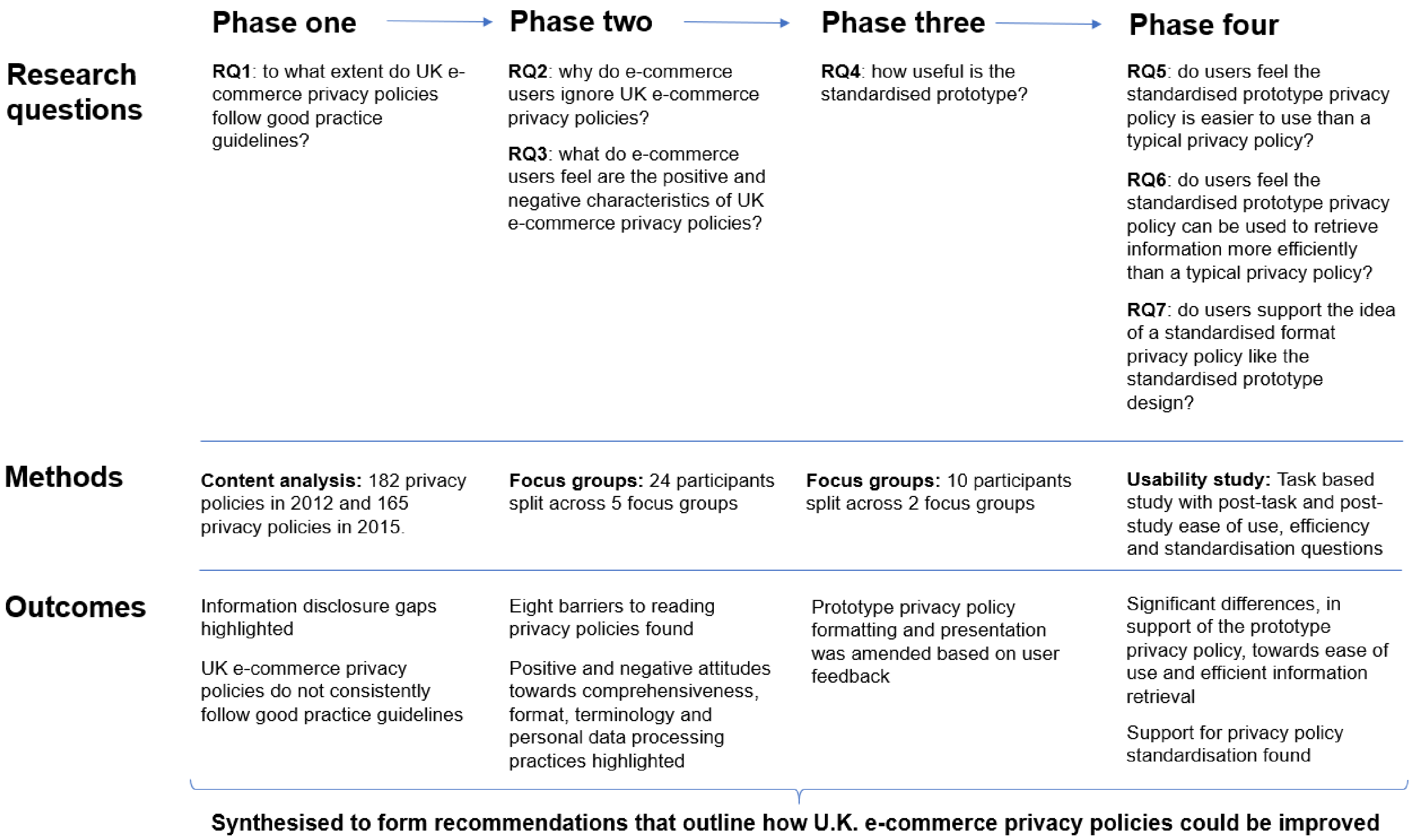
- Explain the findings of a quantitative study using a qualitative study;
- Generalise the exploratory findings of the qualitative study using a quantitative study;
- Enhance a study with a second method;
- Understand a research aim through multiple phases;
- Approach a problem using more than one data source.

A mixed methods strategy was used in this study. Creswell (2009) states that mixed methods researchers should outline a purpose and rationale for mixing research methods. The aim of this research was to explore how UK e-commerce privacy policies could be improved. This aim was deliberately broad, and the research outcome was unknown at the start of the study. Research question one (to what extent do UK e-commerce privacy policies follow good practice guidelines?) was the starting point for inquiry. After this, the direction of this study was guided by the research findings. Additional research questions emerged as further research was carried out. Mixed methods research allows questions to emerge and research to be carried out over multiple phases. In this sense, adopting a mixed methods approach offered the benefit of methodological flexibility. Selecting a quantitative or qualitative strategy at the outset of this study might have limited the scope of research. Therefore, a pragmatic, mixed methods approach was a suitable strategy to adopt to address the research aim.

3.3 Multiphase Mixed Methods Design

Timing and mixing are considerations in mixed methods research. Timing refers to the order of data collection. Sequential, concurrent and multiphase designs are used in mixed methods research (Creswell and Plano Clark, 2011). Sequential timing refers to data that is collected at two different points in time. Concurrent timing occurs when qualitative and quantitative data collection methods are executed at the same time in a study. Multiphase timing happens when data collection occurs sequentially or concurrently over three or more phases under one program of study. Creswell and Plano-Clark (2011) point out that multiphase designs can be used to address a set of interrelated research questions. This type of research design also allows the researcher to conduct iterative studies over multiple years. However, such designs can require extensive resources.

This study is best described as multiphase sequential. Four sequential phases of research were carried out. Each phase addressed different research questions that contributed to the research aim. Research question one was developed a priori; before any data collection occurred. To ensure data currency, in phase one, data was collected in 2012 and 2015. Six additional research questions were induced based on the research findings in phases one to three. The research questions that emerged (research questions two to seven) are outlined briefly in sections that follow in this chapter. The rationale behind each research question that emerged is provided at the outset of chapters five, six and seven. The multiphase sequential timing of each phase is shown in figure 3.1 along with an outline of the methods and outcomes.



	Phase one	Phase two	Phase three	Phase four
Research questions	**RQ1**: to what extent do UK e-commerce privacy policies follow good practice guidelines?	**RQ2**: why do e-commerce users ignore UK e-commerce privacy policies? **RQ3**: what do e-commerce users feel are the positive and negative characteristics of UK e-commerce privacy policies?	**RQ4**: how useful is the standardised prototype?	**RQ5**: do users feel the standardised prototype privacy policy is easier to use than a typical privacy policy? **RQ6**: do users feel the standardised prototype privacy policy can be used to retrieve information more efficiently than a typical privacy policy? **RQ7**: do users support the idea of a standardised format privacy policy like the standardised prototype design?
Methods	**Content analysis:** 182 privacy policies in 2012 and 165 privacy policies in 2015.	**Focus groups:** 24 participants split across 5 focus groups	**Focus groups:** 10 participants split across 2 focus groups	**Usability study:** Task based study with post-task and post-study ease of use, efficiency and standardisation questions
Outcomes	Information disclosure gaps highlighted UK e-commerce privacy policies do not consistently follow good practice guidelines	Eight barriers to reading privacy policies found Positive and negative attitudes towards comprehensiveness, format, terminology and personal data processing practices highlighted	Prototype privacy policy formatting and presentation was amended based on user feedback	Significant differences, in support of the prototype privacy policy, towards ease of use and efficient information retrieval Support for privacy policy standardisation found

Synthesised to form recommendations that outline how U.K. e-commerce privacy policies could be improved

Figure 3.1 – Multiphase research design overview

Mixing refers to how and where the quantitative and qualitative strands of research are integrated. A connected strategy was used in this research design. Creswell and Plano-Clark (2011, p.66) state that this type of research involves: “using the results of the first strand to shape the collection of data in the second strand by specifying research questions, selecting participants, and developing data collection protocols or instruments.” Figure 3.2 illustrates the mixing strategy used in this study.

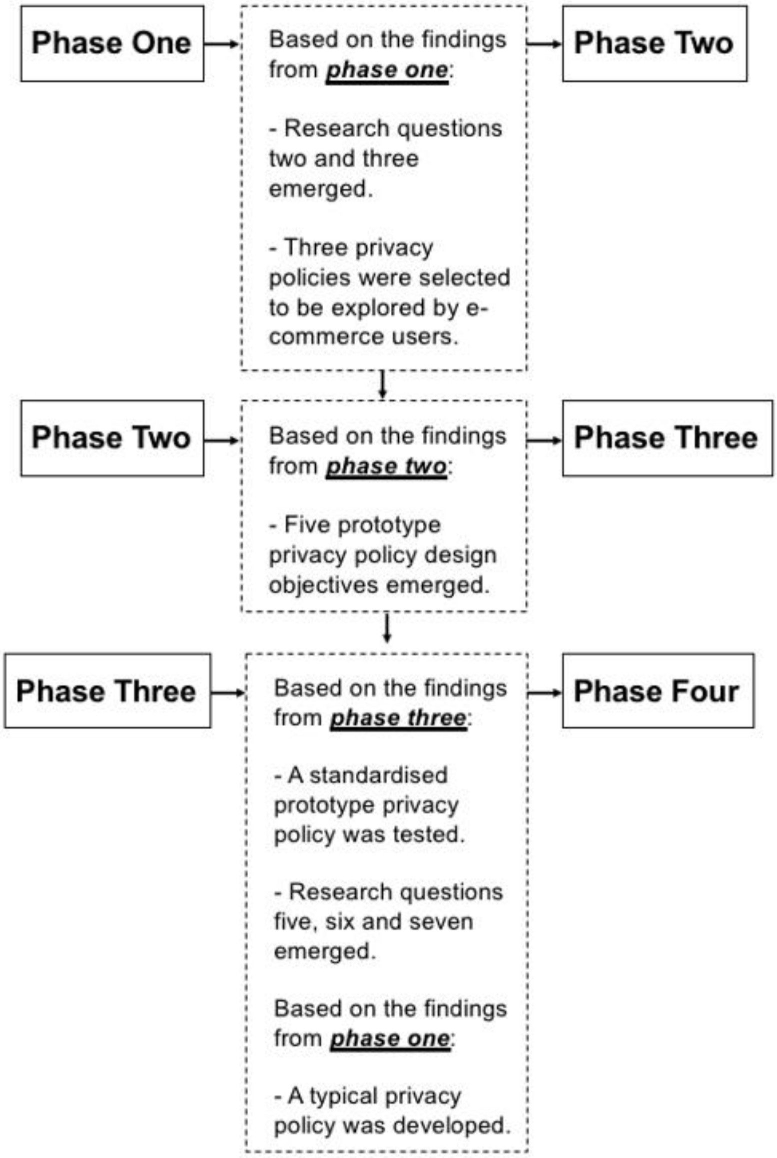

Phase One
Based on the findings from phase one:
- Research questions two and three emerged.
- Three privacy policies were selected to be explored by e-commerce users.
Phase Two
Phase Two
Based on the findings from phase two:
- Five prototype privacy policy design objectives emerged.
Phase Three
Phase Three
Based on the findings from phase three:
- A standardised prototype privacy policy was tested.
- Research questions five, six and seven emerged.
Based on the findings from phase one:
- A typical privacy policy was developed.
Phase Four

Figure 3.2 - Mixing strategy

The remainder of this chapter describes the methods used in phases one to four. For each research phase a description of the concept(s) being investigated is provided followed by a justification of the choice of research method. The decisions taken when operationalising each method is then outlined.

3.4 Phase One: Good Practice

Phase one addressed research question one. Research question one was: **to what extent do UK e-commerce privacy policies follow good practice guidelines?** Section 51(9) of the Data Protection Act 1998 (Parliament, 1998, p. 32) defines good practice as:

> "…such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of this Act."

Good practice has been operationalised through the publication of good practice guidelines by the Information Commissioner's Office (2010). In consideration of this, the method chosen to investigate good practice needed to allow for the measurement of good practice guidelines to determine the extent to which good practice is being followed.

3.4.1 Choosing a Method: Content Analysis

Content analysis was chosen as the method to measure good practice. In content analysis, texts are the starting point for research. This was relevant because privacy policies are text documents. Berelson (1952) and Neuendorf (2016) state that content analysis involves the quantitative description of texts. Berelson (1952, p.18) described content analysis as: "a research technique for the objective, systematic and quantitative description of manifest content of communication." Neuendorf (2016, p.1) suggests that content analysis is a: "systematic, objective, quantitative analysis of message characteristics." To address research question one, multiple privacy policies needed to be examined to determine whether good practice was being followed. Therefore, a count of good practice needed to be obtained for several policies and then summarised to provide answers. This approach is an established variant of content analysis (Holsti, 1969). It involves comparing the content of text to a known standard and stating whether the desired level of performance is reached. Krippendorff (2013) refers to these types of content analysis as judgements in which the standards being examined are prescribed by institutions. In this study, good practice prescribed by the Information Commissioner's Office served as the standard under measurement.

Components of Neuendorf’s (2002) and Krippendorff’s (2013) work were integrated into the design of this content analysis. Their work overlaps in many places because they focus on yielding valid and reliable findings. Each component of the content analysis in the current research is discussed next.

3.4.1.1 Operationalisation

The variables being studied in this content analysis were good practice guidelines. Twenty-seven good practice guidelines were measured. Guidelines were divided into the ten sections outlined below with each section containing one or more variables:

1. Privacy policy format
2. Effective date
3. Data controller identity and purposes for processing
4. Personal data sharing for direct marketing
5. Accessing and amending personal data
6. Direct marketing preferences
7. Accountability
8. Retention
9. Security
10. Cookies

Dichotomous categories were used to record the presence (yes) or absence (no) of a good practice guideline for twenty-five variables. These measures satisfy the criteria that categories must be mutually exclusive (Neuendorf, 2002; Krippendorff, 2013). This means that privacy policies could not be considered as including both the presence and absence of a good practice guideline. In one instance, identifying the presence or absence of good practice was difficult because of the ambiguous nature of privacy policies. For this reason, one variable was also assigned an *open to interpretation* category. This satisfied the criteria that categories must be exhaustive meaning that there was an appropriate code for each recording unit (Neuendorf, 2002; Krippendorff, 2013).

In content analysis variables can be open or closed (Krippendorff, 2013). Twenty-six of the variables in this study were classified as closed variables because their measurement values were defined prior to coding. One variable was considered open, meaning that no measurement response was provided. This variable was recorded a string of text directly from the privacy policy. A list of the variables and associated measurement categories can be found in appendix A.

3.4.1.2 Unitising

Unitising allows the researcher to define what is going to be observed. Sampling units and recording units are two types of units that are defined at the outset of a content analysis. Sampling units are naturally occurring units that can be distinguished for selective inclusion in an analysis (White and Marsh, 2006). The sampling units for this content analysis were UK e-commerce websites.

Krippendorff (2013, p.100) described recording units as: “units that are distinguished for separate description, transcription, recording or coding.” Recording units are usually contained within sampling units but should never exceed the sampling unit. Recording units should be defined so that they are large enough to contain all the necessary content needed to perform the analysis but small enough to allow content analysts to agree on their description. The recording units for this study were dependant on the good practice guideline under measurement. For most of the good practice guidelines, the recording unit was the privacy policy published by the UK e-commerce website. In some instances, the cookie policy was the recording unit. This was the case where the UK e-commerce website published a cookie policy separately to the privacy policy. The same logic applied to security policies. In this respect, the sampling unit contained each recording unit. The recording unit for each variable is reported in appendix A.

3.4.1.3 Sampling

Sampling the internet presents several challenges because websites frequently change. This makes obtaining an accurate sampling frame difficult. This study found no evidence of a comprehensive source that enumerated all UK e-commerce websites. As such, it was not possible to create a sampling frame that included the population of UK e-commerce websites. Webb and Wang (2014) outline options for researchers that face this problem. One choice includes the use of pre-existing services or companies that produce ranking lists of websites. This study used Google DoubleClick Ad Planner (discontinued in 2012 and replaced by Google Display Ad Planner) to obtain a sampling frame. Google DoubleClick Ad Planner was primarily used by organisations to plan internet advertising campaigns. The service worked by producing lists of websites based on traffic data. Lo and Sedhain (2006) referred to these services as activity-based ranking websites. These websites are beneficial to researchers because they can produce up to date lists of popular and less popular websites. However, activity-based ranks are limited to producing ranks based on the surfing patterns of individuals or organisations that use specific analytics software (Google analytics in the case of Google DoubleClick Ad Planner). Therefore, activity based ranks do not reflect the behaviour of the entirety of web users (Lo and Sedhain, 2006).

Google DoubleClick Ad Planner produced lists based on user defined criteria. The geography and placement type option were used to define the list produced for this study. The geography option specified the country the website has been accessed from. The UK was selected from this option. The placement type option specified the type of website according to Google's own categorisation mechanism. The *shopping* placement type was specified from this option. The resultant list, the sampling frame, contained one thousand shopping websites that had been accessed by individuals in the UK. This can be found in appendix B.

The sampling frame was divided into one hundred equal segments. Each segment contained ten websites. The first two websites in each segment were selected. Each website was subject to three criteria checks to ensure that the sample only contained websites that were relevant to the research question. The three criteria were:

1. Is the website owned or operated by an organisation registered in the U.K?

Company registration numbers and names were sought from each website and the Companies House website (UK Government, no date) was used to validate these.

2. Does the website correspond to the definition of a B2C e-commerce website provided by Chaffey (2011)?

The *shopping* placement type was defined by Google. Consequently, there was a risk that that the sampling frame could contain websites that were not relevant to this study (such as business to business e-commerce websites or customer to customer e-commerce websites). Each website was checked to ensure that it was consistent with the Business-to-customer e-commerce definition presented by Chaffey (2011). Chaffey (2011, p. 27) defines B2C transactions as: "a commercial transaction between an organisation and customers."

3. Has the owner or operator of the website already been included in the sample?

Sampling validity could be compromised if websites were included that were owned or operated by the same organisation. This is because their policies may be similar. Each website was checked to ensure that the owners or operators had not already been included.

Websites that failed one or more of the criteria checks were excluded from the sample. When a website did not satisfy the criteria the next website in the sampling frame was checked. This resulted in a sample of 200 websites. This is presented in appendix C.

3.4.1.4 Piloting the Coding Scheme

The coding scheme consists of the variables being measured in a content analysis and a detailed explanation of how variables should be coded (Neuendorf 2016). To understand whether each variable can be coded reliably content analysts should be familiar with the texts being examined (Krippendorff, 2013). Before the reliability of each variable was *measured*, the potential for achieving reliability was *approximated* by the researcher. The purpose of this piloting stage was twofold; (1) to explore the measures of good practice to assess the *likelihood* that each variable could be coded reliably and (2) to identify any latent practical issues that might affect the coding of recording units. A subsample consisting of the first twenty sampling units was examined. The first twenty websites were the most popular websites in the sample. They were owned by large organisations and this study assumed that they would cover a broad enough range of topics to allow each good practice measure to be explored. The privacy policies of each website were visited, and notes were made about each good practice variable. Policies were visited more than once following additions and amendments to the variables and measures. It is worth noting that policies *were not coded* at this stage. Notes were taken relative to the objectives of the pilot study. Reliability measurement, where policies were coded, was carried out after this piloting stage. The eight outcomes of the pilot study were:

1. The scope of a privacy policy was widened.

In some circumstances policy information relating to the processing of personal data was published outside of the privacy policy. In cases where this was obvious (for example a link was placed inside of the privacy policy) the other information relating to the processing of personal data was considered as part of the UK e-commerce privacy policy. This study did not search every single webpage of the UK e-commerce website to locate other information that might be related to privacy. This simply was not practical.

2. Variables were added to record the separate publication of a security policy (9.2) and cookie policy (10.2).

On some websites security and cookie policies were published separately to the privacy policy. There are no guidelines stating that this is good practice however this was considered an interesting avenue to explore given the potentially large amount of policy information to communicate. Furthermore, both security and cookie information closely relate to the processing of personal data.

3. The wording of the variable measuring data sharing for direct marketing (4.1) was amended.

The first version of variable 4.1 was: does the privacy policy mention that personal data is shared for direct marketing (with or without consent)? During the piloting stage it became clear that in some cases data sharing descriptions were ambiguous. For example, one privacy policy stated:

> "We may share your information with other carefully selected third party organisations. We or they may contact you for marketing purposes by mail, telephone, which may include automated dialling systems, electronic mail or otherwise."

In this instance, it is not possible to accurately code whether personal data is or is not shared because the policy states that personal data *may* be shared. The same logic applied to other policies as well. Another policy stated:

> "We may share your personal information across the Group so they can provide you with relevant products and services"

Considering this finding, variable 4.1 was amended to: does the privacy policy mention that personal data *is or might be* shared for direct marketing (with or without consent)? This allowed more accurate coding of the privacy policy.

4. Categories for the variable measuring data sharing for direct marketing (4.1) were amended.

Analysis of the first twenty privacy policies highlighted that the categories for measure 4.1 (does the privacy policy mention that personal data is or might be shared for direct marketing (with or without consent)?) would not be exhaustive. The categories originally assigned to this measure were dichotomous. Policies either did (yes) or did not (no) state that personal data is or might be shared for direct marketing. However, in some instances it was not possible to tell whether or not personal data is or might be shared. For example, one policy stated:

> "Updates and promotional offers: if you have consented in advance we send you updates and information on our promotional offers. This includes joint promotions with our business partners."

Does this mean that personal data is shared with these joint business partners? One might interpret this statement to mean that personal data is shared with the organisation's business partners and they may use this for direct marketing. On the contrary, it could also be argued that the organisation sends direct marketing on behalf of their business partners about products their business partners sell. In this sense, personal data would not be shared. Without further clarification, it is difficult to tell whether personal data is or might be shared. In situations like this the original categories for this variable, yes or no, did not suffice. Therefore, an *open to interpretation* category was added. The aim of this category was to record all instances where the policy was ambiguous, and it could not be ascertained whether personal data is or might be shared.

5. Four variables were excluded.

These were variables that were considered a threat to the reliability of the study because they were difficult to code objectively. These variables were about the reasons for processing personal data, helpful privacy advice, reasons for using cookies and third-party cookies.

6. The coding scheme including instructions were finalised.

The coding instructions were finalised following the additions and amendments made to the good practice variables and measures. The scope of each variable was defined and examples of how each variable should be coded were provided in the coding instructions. The coding scheme can be found in appendix D. Supporting screenshots were used to illustrate the coding instructions. They are provided in appendix E.

7. The number of recording units to be coded each day was finalised.

Coder fatigue can result in mistakes that affect the reliability of a content analysis (Neuendorf, 2002). To help reduce the risk of coder fatigue Neuendorf (2002) stated that a reasonable amount of time should be spent coding each recording unit. Based on the approximate time taken to read each recording unit during the piloting stage it was considered that five recording units was a sensible number of units to code per day.

8. General conclusions about the twenty-seven good practice variables were made.

The twenty-seven guidelines addressed a suitable range of good practice topics to allow conclusions about good practice to be made. Some guidelines, such as policy clarity, were not measured in this study. There was a deliberate attempt to avoid measuring guidelines that were not easily categorised or amendable to counting because such guidelines are difficult to record consistently and would likely affect the reliability of any findings.

3.4.1.5 Pre-Coding Reliability

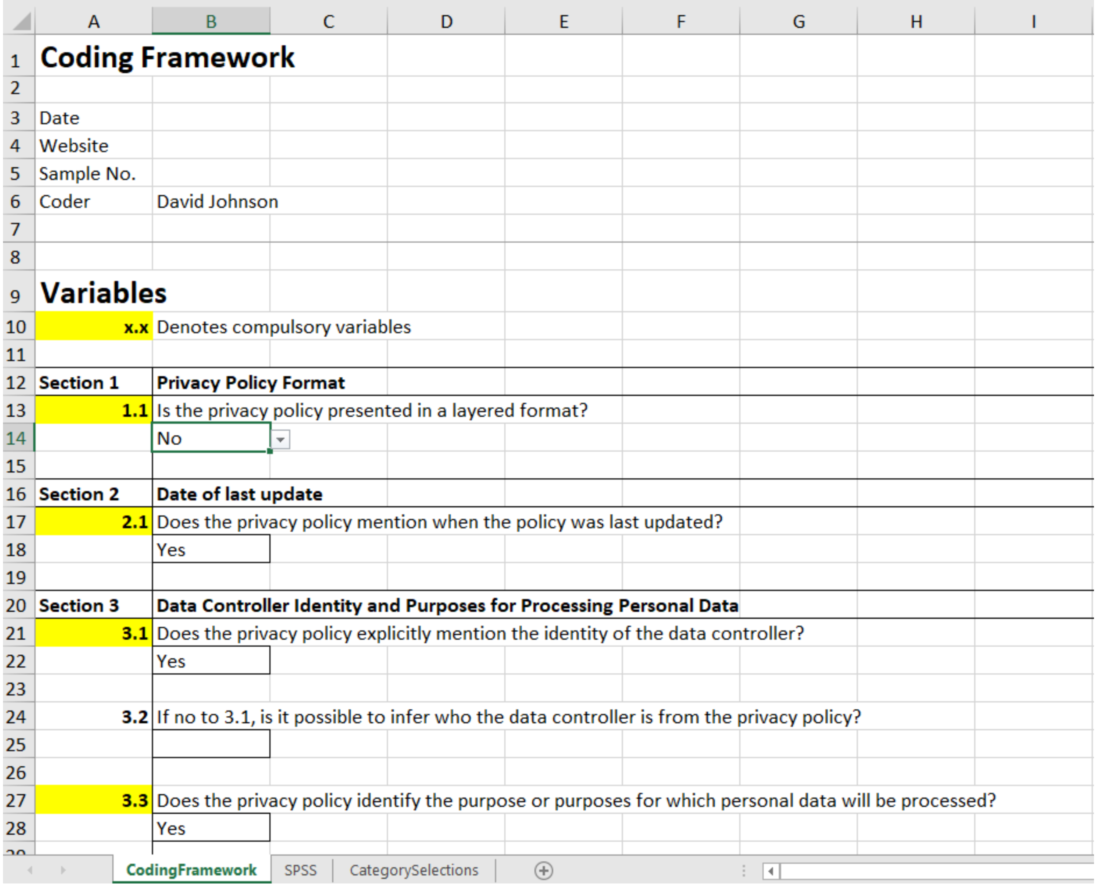
Before data collection started a sample of websites were coded at two points in time to determine whether the chosen variables could be coded reliably. A single coder (the researcher) coded the subsample. A randomly selected subsample consisting of 10% of the sample was examined based on the recommendation of Neuendorf (2002). The findings were then analysed to determine the extent of agreement.

Percentage agreement was used as a measure of reliability. Percentage agreement does not account for agreement by chance although it was the most appropriate measure of reliability for this study. Frey, Botan and Kreps (2000) stated that agreement above 70% can be considered reliable. All percentage agreement figures were above 90% and thus satisfied the 70% reliability threshold. The pre-coding percentage agreement figures for each variable in 2012 and 2015 can be found in appendix A.

Stronger forms of reliability testing exist, such as the use of two or more coders to test the same measuring procedure. However, this research was part of a PhD being undertaken by one researcher. This meant that the resources were not available to employ more than one coder. The effort invested to securitise the variables during the piloting phase and only include those that could be coded objectively went some way to addressing this limitation.

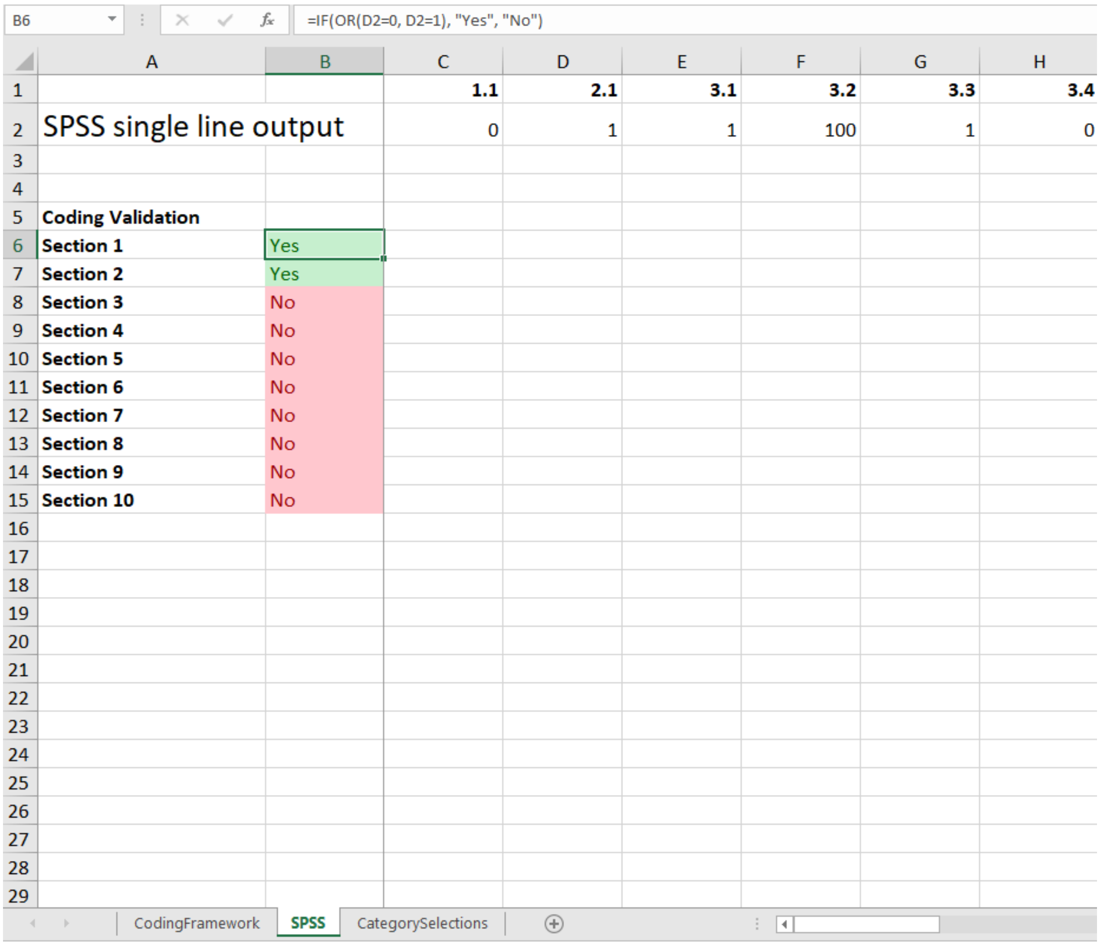
3.4.1.6 Data Collection

Coding is the process of applying codes to data (Howitt and Cramer, 2011) according to observer independent rules (Krippendorff, 2013). To start with, the privacy policy (and cookie/security policies if applicable) was copied into Microsoft Word and saved. A coding tool developed using Microsoft Excel was used to record data. The coding tool used drop down menus containing each code to allow for quick and simple recording for each variable. A numerical value was assigned to each categorical measure. The absence of a guideline was represented by the number 0 and the presence of a guideline was represented by the number 1. Once coding had finished the coding tool was programmed to produce a single line output for every variable. This consisted of a list of numerical values that corresponded to the categories chosen for each variable. Validation was used to confirm that every variable was recorded. The single line output was then copied into IBM SPSS for statistical analysis. Figure 3.3 and Figure 3.4 display the coding tool and single line output respectively. The same data collection process was carried out in 2012 and 2015.



	A	B
1	**Coding Framework**	
2		
3	Date	
4	Website	
5	Sample No.	
6	Coder	David Johnson
7		
8		
9	**Variables**	
10	**x.x**	Denotes compulsory variables
11		
12	**Section 1**	**Privacy Policy Format**
13	**1.1**	Is the privacy policy presented in a layered format?
14		No
15		
16	**Section 2**	**Date of last update**
17	**2.1**	Does the privacy policy mention when the policy was last updated?
18		Yes
19		
20	**Section 3**	**Data Controller Identity and Purposes for Processing Personal Data**
21	**3.1**	Does the privacy policy explicitly mention the identity of the data controller?
22		Yes
23		
24	**3.2**	If no to 3.1, is it possible to infer who the data controller is from the privacy policy?
25		
26		
27	**3.3**	Does the privacy policy identify the purpose or purposes for which personal data will be processed?
28		Yes

Figure 3.3 - Coding tool



B6 =IF(OR(D2=0, D2=1), "Yes", "No")

	A	B	C	D	E	F	G	H
1			**1.1**	**2.1**	**3.1**	**3.2**	**3.3**	**3.4**
2	SPSS single line output		0	1	1	100	1	0
3								
4								
5	**Coding Validation**							
6	**Section 1**	Yes						
7	**Section 2**	Yes						
8	**Section 3**	No						
9	**Section 4**	No						
10	**Section 5**	No						
11	**Section 6**	No						
12	**Section 7**	No						
13	**Section 8**	No						
14	**Section 9**	No						
15	**Section 10**	No						
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								

Figure 3.4 - Single line output for SPSS

3.4.1.7 Post-Coding Reliability

The reliability of coding was tested after coding had taken place. This followed a similar process to the pre-coding reliability phase. A subsample of 10% was randomly generated and coded two weeks after coding had finished. Twenty five of the twenty-seven variables reported a percentage agreement level above 90%. The other two variables reported a percentage agreement above 80%. All variables satisfied the 70% reliability threshold specified by Frey, Botan and Kreps (2000). The post-coding percentage agreement findings for each variable in 2012 and 2015 can be found in appendix A.

3.4.1.8 Data Analysis

Descriptive statistics were used to summarise the findings for each variable. Percentages were used to describe the presence or absence of a good practice. The percentage difference between the findings in 2012 and 2015 identify that a change has occurred in the sample of websites studied between the two timeframes measured. The percentage difference does not indicate the likelihood of observing change within the entire population of UK e-commerce privacy policies. McNemar’s test (1947) was used to test for any statistically significant changes for each good practice measure between 2012 and 2015. McNemar’s test was used to ascertain the likelihood of observing a difference in the population of UK e-commerce privacy policies. In the context of McNemar’s test, the P value refers to the probability of observing a difference between two values relative to the assumption that the null hypothesis is true. In statistics, the null hypothesis assumes that no difference exists in the population. A P value lower than a 0.05 threshold signifies that the probability of observing a difference (as large as the difference found in the sample) between the two findings is significantly small enough to be confident that the null hypothesis can be rejected. In doing so, the researcher is rejecting the assumption that there is no difference in the population.

McNemar’s test was appropriate because good practice (the dependent variable) was measured using two mutually exclusive groups (yes and no) and the sample was recorded at two points in time (2012 and 2015). McNemar-Bowker’s (Bowker, 1948) test is an extension of the McNemar’s test that is appropriate for nominal dependent variables that are not dichotomous. This test was used for variable 4.1 because three response categories (yes, no and open to interpretation) were used to measure good practice.

A compliance index was also calculated as a cumulative, single measure of good practice. The cumulative index included fifteen of the twenty-seven variables recorded. A paired samples t-test was used to determine whether there was a statistically significant mean difference in cumulative good practice compliance between 2012 and 2015. A paired samples t-test was a suitable test of statistical significance in this instance because good practice (the dependent variable) was measured along a continuum from zero to fifteen and the sample was recorded at two points in time (2012 and 2015).

Analysis also involves moving outside of the data to understand what the findings mean relative to the context of study (Krippendorff, 2013). To understand what following (or not following) good practice means for policy stakeholders, inferences need to be made that are relevant to the context of study. Krippendorff’s (2013) view is that content analysts must look outside the physicality of text to how people other than analysts use text and the feelings and behavioural changes they invoke. This involves making inferences. Holsti (1969) described two types of inferential content analysis. The first involves making inferences about the source of communication. Questions about the motives and intentions of authors are typical in these studies. The second type involves making inferences about the recipient of communication. In this type of analysis inferences about the likely effects of text are made.

In the discussion chapter, inferences are made about the source and recipient of communication to provide a best explanation of why compliance (or non-compliance) with good practice occurred and what impact this might have on e-commerce users. In content analysis inferences are usually abductive in nature because they involve a best explanation of why an observation has occurred. Inferences point out unobserved phenomena that are relevant to the context of the analysis. The two domains of content analysis, that is descriptive accounts of text (in this case compliance with good practice) and what this implies, are logically independent of each other. An analytical construct helps to bridge the gap between the two domains and justify the inferences made. Krippendorff (2013) pointed out that analytical constructs may be derived from previous research, expert knowledge or experience and existing theories and practices. The existing consumer and organisational behaviour literature was used as an analytical construct to help draw inferences.

The purpose of research phase one was to provide a starting point from which future research questions would emerge and address a gap identified in the privacy literature. The opportunity for the researcher to read and become immersed in a broad range of privacy policies was advantageous at the outset of the research. Readership of privacy policies enabled the researcher not only to partially address the research aim but also to establish a deep understanding of the privacy policies sampled. This was beneficial in uncovering themes and issues that might not necessarily have been evident from reading a small sample of privacy policies and therefore invoked thought that contributed towards devising the research questions addressed in phase two.

3.5 Phase Two: Policy Barriers and Characteristics

Research phase two addressed research questions two and three. These questions were:

2. **Why do e-commerce users ignore UK e-commerce privacy policies?**
3. **What do e-commerce users feel are the positive and negative characteristics of UK e-commerce privacy policies?**

At the start of phase two several sensitising concepts were identified. Blumer (1954, p.7) noted that sensitising concepts give the researcher: “a general sense of reference and guidance in approaching empirical instances.” More specifically, Van Den Hoonaard (1997, p.2) stated that sensitising concepts are used as a “starting point in thinking about the class of data of which the social researcher has no definitive idea and provides an initial guide to [his or] her research.” These initial ideas allow researchers to investigate how particular concepts are given meaning in a chosen context (Schwandt, 2015). For Patton (2015), sensitising concepts are a prerequisite for inductive, open ended research. They help organise the complexity of human experience. In phase two the sensitising concepts identified from the research questions were:

- Ignorance (towards privacy policies)
- Positive and Negative (characteristics of privacy policies)
- Reputation (of organisations that publish privacy policies)

These sensitising concepts provided a foundation to begin thinking about the research questions. The nature of the concepts influenced the choice of research method and shaped the nature of inquiry.

3.5.1 Choosing a Method: Focus Groups

The reasons why consumers do not read privacy policies and positive and negative characteristics of privacy policies are complex and subjective areas. Therefore, phase two required a method that would take account of the plurality of human beliefs and actions. Operationalising any variables or assigning any categories to be counted prior to inquiry would have been difficult and may well have limited the quality of data collected. For this reason, a qualitative method was chosen to address research questions two and three.

Qualitative research methods allow concepts to be understood: “through the eyes of people being studied” (Bryman, 2008, p.385). The focus group is a method that involves interviewing several people at the same time. This provides researchers with the opportunity to ask several participants questions about the topic of inquiry. Morgan (1997, p.20) writes that focus groups allow researchers to explore: “attitudes, opinions and experiences in an effort to find out not only what participants think about an issue but also how they think about it and why they think the way they do.” The main comparative advantage of focus groups over single person interviews is the ability to observe interaction. Morgan (1997) states that focus groups provide direct experience of the similarities and differences in participant opinion. Overall group interaction can elicit a wide variety of opinions leading to a rich account of the subject being investigated. In consideration of these points, the focus group was chosen as a method to address research questions two and three.

3.5.1.1 Questioning Route

To elicit perceptions and attitudes, focus group participants are asked questions about a topic of inquiry. Kruger and Casey (2009) state that effective focus group questions should have the following qualities:

- They evoke and encourage conversation to allow participants to build on and possibly critique the points they make;
- They use words that participants would use and in doing so avoid the use of jargon and technical language;
- They are clear and straightforward for participants to understand;
- They are open ended to allow the researcher to probe for explanation and description of the topic under study.

The order in which questions are asked should also be considered in focus group research. Kruger and Casey (2009) stated that a good questioning route begins with a question that every participant can answer. The opening question typically requires a short factual answer. Introductory questions follow the opening question. These questions are open ended and usually ask participants to describe their feelings towards the topic under investigation. Next, key questions are asked. These questions are focal to the purpose of the study and reflect the main motivations for the research. The final question is the ending question. The purpose of this question is to enable participants to reflect on their opinions.

Table 3.3 shows the first iteration of focus group questions. Additional prompt questions are italicised. The opening and introductory questions helped to familiarise participants with the research topic. Key question one was derived from research question two and influenced by the sensitising concept of ignorance. Key questions two, three, four and five were derived from research question three. These questions were influenced by the sensitising concepts of positive, negative and reputation. For key questions two and three participants were asked to read three privacy policies chosen purposefully based on the findings of research phase one. For key question four participants were asked to read three small personal data sharing extracts. Again, these extracts were selected based on the outcome of the content analysis. A justification of why each policy and extract was chosen is provided at the beginning of chapter five. Policy A, B and C can be found in appendix F.

	Question(s)	Estimated time
Opening	Picture the scene, you’ve just bought something online. You’ve come to pay, and the website asks you to read their privacy policy. Would you normally read it?	1 minute
Introductory	What do you think of when I say the phrase privacy policy?	2 minutes
Key	(1) What prompts you to skip reading the privacy policy?	10 minutes
	Participants asked to read policies A, B and C.	10 minutes
	(2) What was good about privacy policy A? What was good about privacy policy B? What was good about privacy policy C? (3) What were the negative aspects of privacy policy A? What were the negative aspects of privacy policy B? What were the negative aspects of privacy policy C? *(Why do you think organisations publish policies in this format or using this style or wording?)* *(What’s wrong or right about way this privacy policy is written?)* (4) What do these policies say about the organisation?	20 minutes
	Participants asked to read extracts A, B and C.	3 minutes

	(5) How did you feel about the words used in these extracts to describe whether your personal data would be shared? *What do the wording of these data sharing extracts say about the organisation?*	10 minutes
Ending	What would you say you've learned about reading the policies you have today?	3 minutes
	Total estimated time	59 minutes

Table 3.3 – First iteration focus group questions

3.5.1.2 Pilot Study

Focus group questions were piloted in November 2012. Five PhD students were recruited. Following the pilot study key questions two and three were amended. Maintaining a sequential discussion of the positive aspects of policy A, followed by policy B and then policy C was difficult. Participants tended to go off and discuss the positive and negative aspects of various policies in no set order. Key questions two and three were changed to reflect this. Table 3.4 displays the second iteration of key focus group questions.

	Question(s)	Estimated time
Key	(1) What prompts you to skip reading the privacy policy?	10 minutes
	Participants asked to read policies A, B and C.	10 minutes
	(2) What was good about these policies that you've just read? (3) What didn't you like about the three policies you've just read? (4) What do these policies say about the organisation?	20 minutes
	Participants asked to read extracts A, B and C.	3 minutes
	(5) How did you feel about the words used in these extracts to describe whether your personal data would be shared?	10 minutes

Table 3.4 - Second iteration focus group questions

3.5.1.3 Sampling

Purposeful and snowball sampling techniques were used to recruit participants. Participants must have purchased a product or service from a website in the last year to be eligible for this study. This ensured that participants would have familiarity with online purchasing and would therefore be able to address the questions being asked. Overall twenty-four participants were recruited through research and personal contacts. Fourteen were students; nine of which were undergraduate finalist students and five were PhD students. The remaining ten participants were friends of the researcher.

Five focus groups were carried out. Morgan (1998) and Krueger and Casey (2009) suggest that between three and five focus groups is a suitable point to assess for data saturation. Data saturation occurs when the main analytic themes continue to occur in each focus group. The main themes and points of interest were beginning to be repeated after the fourth focus group and therefore it was considered appropriate to stop collecting data after the fifth focus group.

Homogeneous focus groups help stimulate free flowing discussion. Morgan (1998) stated that: “when participants perceive each other as fundamentally similar, they spend less time explaining themselves to each other and more time discussing the issues at hand.” Krueger and Casey (2009) and Morgan (1998) describe common criteria for defining group characteristics. These include age, occupation, gender, location, education, income, family status and use of a program or service. Participants in three of the focus groups were at the same point in higher education. Participants in the remaining two focus groups were similar ages. In each focus group, participants had a pre-existing relationship. They were friends or knew each other before data was collected. However, this can manifest as a limitation in some circumstances. Morgan (1998) points out that participants may be less willing to share perceptions knowing opinions may be the subject of further discussion after the focus group.

The exact size of a focus group is dependent on nature of the research topic. Krueger and Casey (2009) state that ten to twelve participants are required for commercial marketing research. For non-commercial topics, five to eight participants should be able to generate sufficient insight into the research topic. Morgan (1998) feels that between six and ten participants works well for a focus group. Smaller groups are preferable where the researcher requires in-depth insight (Krueger and Casey, 2009).

In this study, four focus groups consisted of five participants. In the remaining focus group there were four participants because one participant did not attend. Smaller numbers of participants were appropriate in this study because of the practical requirement to allow participants sufficient room to read, comment and organise the printed privacy policies. The demographic characteristics of each focus group is summarised below in table 3.5.

	Number of participants	Age ranges	Gender
Group One	Five	18-20: one participant; 21-30: four participants	Three males; Two females
Group Two	Five	21-30: all participants.	All males.
Group Three	Five	21-30: all participants.	All males.
Group Four	Five	21-30: all participants.	All females.
Group Five	Four	21-30: all participants.	One male; Three females.

Table 3.5 – Phase two focus group demographics

3.5.1.4 Data Collection

Focus groups took place in December 2012 and January 2013. Creating an environment where participants feel comfortable to discuss the research topic is an important consideration when planning focus groups (Morgan, 1998). Morgan (1997) writes that the location used to collect data must balance the needs of the researcher and the participants. The room used for data collection needed to be quiet and have a large enough table to allow participants to take notes. Suggested places to carry out focus groups are a community centre, library, school, researcher's office or the participants' home (Morgan, 1997). Three of the five focus groups took place at Loughborough University. The remaining two focus groups took place at homes of participants.

The three privacy policies that participants were asked to review were printed on A4 paper. No amendments were made to the format of each policy. To provide context to the reading of privacy policies, participants were asked to think about which website they would prefer to purchase from based on reading each privacy policy. Participants were provided with highlighters and pens and were asked to write down anything they felt was positive or negative about each privacy policy.

The researcher was the moderator for each focus group in this study. Krueger and Casey (2009) highlight the skills required to moderate a focus group. They mention that the moderator should respect participants and show sensitivity when trying to understand their perspective. Moderators should refrain from discussing their personal opinions and should be able to communicate questions clearly. Bryman (2008) also discussed the degree to which the moderator should be involved in the discussion with participants. Bryman states that the moderator should take a balanced approach to guide the direction of the discussion. This involves intervening when the direction of the discussion moves sufficiently away from the research questions. However, the moderator should also promote a free-flowing discussion.

3.5.1.5 Data Analysis

The purpose of thematic analysis is to identify the major themes that occur in textual data (Howitt and Cramer, 2011). Thematic analysis can be applied across a range of theoretical positions (Braun and Clarke, 2006) suggesting its application was suited to the pragmatic nature of this research. This analytical process in this research followed that described by Braun and Clarke (2006). The process is recursive. Movement occurs back and forth between the following stages:

Stage one: Focus group data were transcribed.

Focus group data were transcribed verbatim. Focus group transcripts were printed and read several times (Miles and Huberman, 1994). Initial notes were made highlighting immediate points of interest. This initial stage is immersive in nature. Howitt and Cramer (2011) note that a researcher who is well immersed in data will have more informed ideas about the later stages of analysis.

Stage Two: Initial codes were generated

Codes are: “tags or labels for assigning units of meaning to descriptive or inferential information compiled during a study” (Miles and Huberman, 1994, p.56). Extracts or chunks of the data that were important or interesting in relation to the research questions were identified. Codes were attached to various sized chunks of text, ranging from a phrase to a paragraph of text. Transcripts were read on multiple occasions with codes assigned on each reading of the transcript. Initial codes were descriptive. As the researcher became more familiar with the codes, more interpretive codes were developed.

Stage Three: Themes were identified

A theme represents a patterned response within the data being analysed. It identifies something important in relation to the research question (Braun and Clarke, 2006). A theme pulls together data to form an intelligible and meaningful representation of codes (Miles and Huberman, 1994). Codes were organised into a list and themes were derived from the codes. Each theme consisted of coded extracts. Mind mapping software was used to help organise and visualise the themes that were developed.

Braun and Clarke (2006, p.82) mention the issue of prevalence when developing themes. They write that: “ideally, there will be a number of instances of the theme across the data set, but more instances do not necessarily mean the theme itself is more crucial.” It was important to ensure that the themes reflected the nature of the research question rather than giving weight to the prevalence of each theme as a determinant of its importance.

Stage Four: Themes were reviewed

Some themes were discarded. Some “movement” of codes and refinement of themes occurred at this stage. Data extracts were checked to ensure they were appropriate for each theme. All five transcripts were read again to ascertain how well the derived themes “fitted” the data set. Braun and Clarke (2006) state that at the end of this stage the researcher should have a good idea of the themes, the relationship between the themes and story that the themes tell about the data set.

Stage Five: Themes were finalised

Themes were refined, and the essence of each theme was outlined. Braun and Clarke (2006) note that theme names should be short and concise. Theme descriptions should also be concise; the researcher should be able to define the theme in a small number of sentences.

3.6 Phase Three: Policy Design

In phase three a prototype privacy policy was designed based on the findings of phases one and two. A user evaluation was carried out as part of phase three. The user evaluation addressed research question four. This was: **how useful is the standardised prototype?** To address research question four several sensitising topics were derived when developing the standardised prototype. These topics were important considerations relating to the design of the prototype privacy policy. These concepts were:

- Layout (of the summary and full layers)
- Categories of information (presented within the summary layer)
- Improvements (to the standardised prototype)

These concepts guided the research question, design of the research instrument and analysis in much the same respect as the sensitising concepts outlined at the start of phase two underpinned the study design.

3.6.1 Choosing a Method: Focus Groups

The sensitising concepts identified are subjective and open ended. Therefore, a qualitative research method was used to address research question four. Focus groups were used to explore user attitudes and perceptions towards the standardised prototype privacy policy. A fuller explanation of the benefits of carrying out focus groups can be found in section 3.5.1.

3.6.1.1 Questioning Route

The questioning route was developed using the strategy outlined by Krueger and Casey (2009) (this is the same strategy adopted in research phase two). The key questions were based on obtaining participant attitudes towards the layout and information provided in the standardised prototype. Prompt questions are italicised below in table 3.6.

	Question(s)	Estimated time
Opening	Has anyone ever read a website privacy policy before?	1 minute
Introductory	**Participants review the standardised prototype privacy policy.**	10 minutes
	Can you note down two or three things that you did not know about before reading the policy? What points did you note down?	5 minutes
Key	Thinking about the topics you wrote down earlier (that's the topics that you didn't know about before reading the privacy policy), how useful is the information presented in the summary layer? *(Would you change any of the information?)*	10 minutes

	(What information would you add or take out?)	
	Participants review three existing privacy policies.	5 minutes
	What do you think about the layout of the summary page? *(How helpful is the table?)* *(Could the layout be changed in any way?)*	10 minutes
	What do you think about the layout of the privacy and cookie policy? *(Would you change anything about the layout of the privacy and cookie policies?)*	10 minutes
Ending	On reflection, is there anything else that that you think might improve the new privacy policy?	5 minutes
	Total estimated time	56 minutes

Table 3.6 - Phase three focus group questions

3.6.1.2 Sampling

Elements of purposeful, snowball and convenience sampling were used to recruit participants. Initial contacts of the researcher (friends and relatives) helped to recruit ten participants. To take part in the study participants were required to have purchased a product from an e-commerce website within the last twelve months. Two focus groups were carried out. Each focus group comprised of five participants. Table 3.7 shows the demographic characteristics of each group.

	Number of participants	Age ranges	Gender
Group One	Five	21-30: Four participants; 31-40: One participant.	One male; Four female
Group Two	Five	21-30: Four participants; 41-50: One participant.	Five males.

Table 3.7 - Phase three focus group demographics

3.6.1.3 Data Collection

Focus groups took place at the researcher’s house. Five laptops were loaned from the School of Business and Economics at Loughborough University. Participants used a laptop to view the standardised prototype privacy policy. Participants were also shown three other current privacy policies. Each policy was open within a separate tab of the same browser window. These policies were selected based on their different formats. The characteristics of the three additional policies are outlined in chapter six.

3.6.1.4 Data Analysis

Data were analysed thematically using the process described in section 3.5.1.5. Miles and Huberman (1994) state that codes can be identified prior to fieldwork. These codes can be derived from a conceptual framework, research questions, hypotheses or key variables being examined. The sensitising topics identified before data collection were used as broad codes to guide the analysis of data. Codes were further identified within each topic.

3.7 Phase Four: Policy Usability

The effectiveness of the standardised prototype privacy policy was the focus of research phase four. This phase addressed research questions five, six and seven. These questions were:

5. **Do users feel the standardised prototype privacy policy is easier to use than a typical privacy policy?**
6. **Do users feel the standardised prototype privacy policy can be used to retrieve information more efficiently than a typical privacy policy?**
7. **Do users support the idea of a standardised format privacy policy like the standardised prototype design?**

The concepts under measurement in phase four were perceived ease of use, perceived efficiency and policy standardisation. Perceived ease of use is a measure of the degree to which a user feels that using a technology will be free from effort (Davis, 1989). Perceived efficiency is a measure of the extent to which a user feels that the product or service allows him or her to work quickly and efficiently (Capellini, Tassistro, & Actis-Grosso, 2015). A justification of the rationale to study these concepts is provided at the beginning of chapter seven.

In a broader sense, perceived ease of use and perceived efficiency form part of user experience and usability. In ISO 9241 (International Organisation for Standardization, 2010) user experience is defined as a: “person’s perceptions and responses resulting from the use and/or anticipated use of a product, system or service.” Tullis and Albert

(2008) stated that user experience takes into consideration the hedonistic qualities of a product as well as the emotions that are associated with product interaction. Usability refers to: “the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” (International Organisation for Standardization, 2010). Tullis and Albert (2008, p. 8) describe satisfaction as: “the degree to which the user was happy with his or her experience.” Satisfaction involves having positive attitudes towards a product while being free from discomfort (International Organisation for Standardization, 2010).

3.7.1 Choosing a Method: Usability Study

Perceived ease of use and perceived efficiency are established usability concepts (Tullis and Albert, 2008). Both concepts (although more so perceived ease of use) have been operationalised and examined theoretically (Venkatesh and Davis, 2000; Gefen, Karahanna and Sttraub, 2003) and practically in usability studies (Lewis, 1995; Bangor, Kortum and Miller, 2008). The purpose of a usability study is to investigate how a product or service is perceived by users, how well the product or service meets its stated objectives and where users have difficulties using a product or service (Chowdhury and Chowdhury, 2011). A usability study is a broad term that encompasses several different methods. To illustrate, table 3.8 outlines a selection of usability methods. The choice of usability method is dependent on whether performance or satisfaction is being measured (Tullis and Albert, 2008). Performance measures behaviour. This involves recording what the user does while interacting with the product. Satisfaction measures attitudes. This involves measuring what the user thinks about his or her interaction with the product.

A usability study was a suitable method to adopt in this phase because the purpose of the study was to measure attitudes towards a prototype privacy policy. This phase is best described as adopting elements of A/B testing and concept testing. User attitudes were assessed after interaction with two different privacy policies. One policy was a *typical privacy policy* developed using data gathered from phases one and two. The second policy was the *standardised prototype* design developed in phase three. The characteristics and choice of policies is discussed at the beginning of chapter seven.

Method	Description
Clickstream (log) analysis	Records where a user clicks on a webpage as they interact with different parts of a website.
Card sorting	Items of information are organised into groups and categories are assigned to each group. Used to help structure information.
A/B testing	Testing two different designs. Users are assigned to each design and interaction data is gathered to assess the effectiveness of each design.
Concept testing	An approximation of a product is presented to a user to determine if the product meets the needs of the user.
Ethnographic (camera) studies	A camera is used to record user interaction with a product. Users may be asked to describe what they're thinking "aloud" as they perform different tasks.
Eye tracking	An eye tracking device records where the user looks on a screen as they perform different tasks.

Table 3.8 - Usability research methods adopted from Rohrer (2014) and Chowdhury and Chowdhury (2011)

3.7.1.1 Task Design

Participants interact with a product or system by performing tasks in a usability study. Tasks help to familiarise the user with the functionality of the new product. Kuniavsky, Goodman and Moed (2012) state that tasks should be clearly defined and should focus on certain elements of the product that the researcher is aiming to examine. Tasks should take no longer than ten minutes to complete, although this depends on the complexity of the topic being investigated. In this study, participants were asked to complete five tasks. Each task contained one question. Participants were asked to answer the question for the typical privacy policy (policy A) and for the standardised prototype privacy policy (policy B). The five questions participants were required to respond to were:

1. Based on the policies, can you prevent your personal data being used to send you information about products or services?
[Yes; No; Policy does not say]

2. Do the policies provide any links to external websites about cookies?
[Yes; No; Policy does not say]

3. Based on the policies, might your personal data be shared with another organisation that may use it to send you information about products or services? [Yes; Yes with consent; No; Policy does not say]

4. Based on the policies, might your personal data be sent outside the European Economic Area (EEA)?
[Yes; No; Policy does not say]

5. Based on the policies, can you contact an independent organisation and complain about the processing of your personal data?
[Yes; No; Policy does not say]

Participants were provided with possible answers to each question. These are outlined in square brackets above. The questions covered a range of personal data processing topics. The questions were not designed to be overly challenging.

After completing each question participants were asked to respond to two post-task statements. These statements were designed to measure perceived ease of use and perceived efficiency. After completing all five tasks participants were asked to respond to eleven post-study statements. These statements were designed to measure perceived ease of use, perceived efficiency and attitudes towards privacy policy standardisation. Figure 3.5 shows the ordering of tasks and response statements.

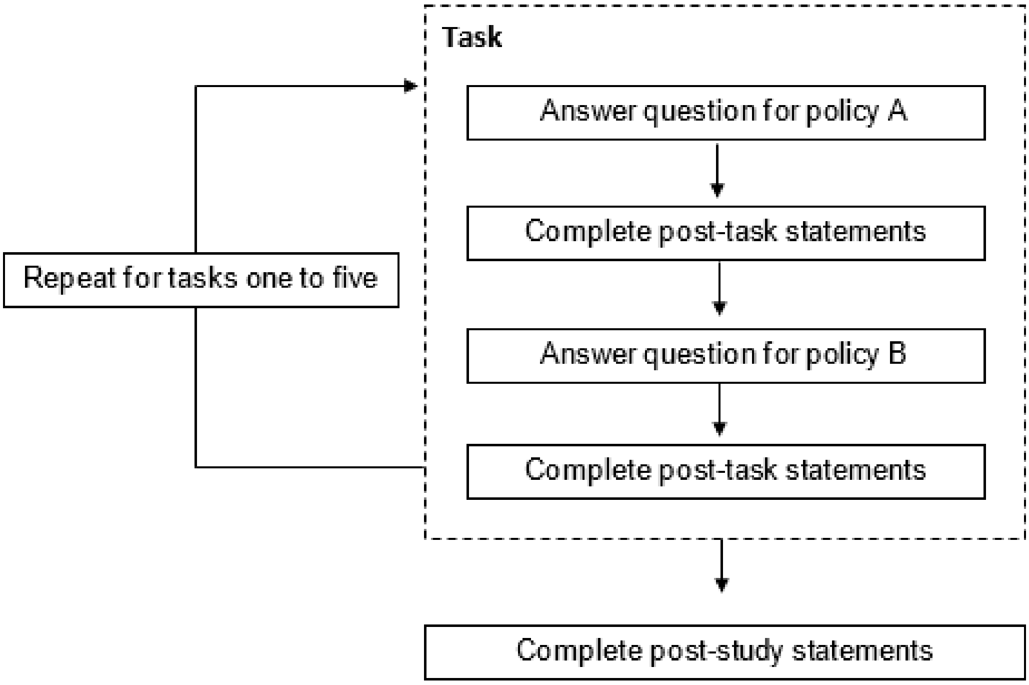

Task
Answer question for policy A
Complete post-task statements
Answer question for policy B
Complete post-task statements
Repeat for tasks one to five
Complete post-study statements

Figure 3.5 - Usability task and statement order

3.7.1.2 Operationalisation

Inspired by the After-Scenario Questionnaire (Lewis, 1995), the post-task statements were designed to take little time to answer. These statements were:

1. I could locate the information required to answer question [insert question number] with ease.
2. I could locate the information required to answer question [insert question number] quickly.

The post-study statements are presented in table 3.9. Four of the post-study statements were used to measure perceived ease of use. These statements were inspired by the *Usefulness, Satisfaction and Ease of Use Questionnaire* (Lund, 2001). Three of the post-study statements measured perceived efficiency. These statements were developed based on the definition of perceived efficiency provided by Capellini, Tassistro, & Actis-Grosso (2015). The final four post-study statements measured attitudes towards the standardisation of privacy policies.

Other self-reported metrics were consulted when developing the post-study statements. These included the *System Usability Scale (SUS)* and the *Website Analysis and Measurement Inventory (WAMMI)*. The SUS measures usability and learnability (Brooke, 2013). WAMMI measures website attractiveness, controllability, efficiency, helpfulness and learnability (Kirakowski and Cierlik, 1998). Using either measure would have involved collecting data that was not entirely relevant to research questions six and seven. Moreover, these scales are often used for website evaluation. This study was only concerned with a privacy policy and not an entire website. As such, they were discounted for use in this research.

Post-task and post-study responses were measured using five-point Likert type items (Likert, 1932) ranging from strongly disagree to strongly agree. Likert type items measure the strength of a feeling towards a concept. Participants respond to the Likert type item by indicating the extent to which they agree with a statement.

3.7.1.3 Pilot Study

Piloting was carried out over two stages. The first stage examined whether questions one to five were understandable. Participants were asked to answer questions one to five using the standardised prototype design at the end of the focus groups in phase three. Participants reported that the questions were clear and logical therefore no amendments were made to the wording of questions.

In the second stage of piloting, four participants were recruited using a convenience sample to assess the adequacy of the post-task and post-study statements and the time taken to complete the study. The length of time to complete the study varied from twelve minutes to twenty-two minutes. This was considered satisfactory. No changes were made to the wording of the statements however the ordering of the post-study statements was changed. The statements measuring perceived ease of use and perceived efficiency were ordered randomly instead of being ordered as two consecutive blocks of statements. This meant that participants were not responding to similarly worded statements consecutively.

Research question	Post-task/post-study	Statement number	Statement
5	Post-task	1a, 1c, 2a, 2c, 3a, 3c, 4a, 4c, 5a, 5c	I could locate the information required to answer question [insert question number] with ease.
	Post-study	6	The privacy policy was easy to use.
		8	The privacy policy layout was straightforward.
		10	The privacy policy headings were signposted clearly.
		12	The privacy policy was simple to use.
6	Post-task	1b, 1d, 2b, 2d, 3b, 3d, 4b, 4d, 5b, 5d	I could locate the information required to answer question [insert question number] quickly.
	Post-study	7	The privacy policy could be used to find information quickly.
		9	I understood where I needed to look to find information when answering questions 1 to 5.
		11	I could use the privacy policy efficiently to answer questions 1 to 5.
7	Post-study	13	It would be a good idea to have a summary policy page on all websites.
		14	It would be a good idea to have a summary policy page that has a consistent look and feel across all websites.
		15	It would be a good idea to have privacy policies that have a consistent look and feel across all websites.
		16	I would like websites to offer variety in the way in which they present their privacy policies.

Table 3.9 – Post-task and post-study statements

3.7.1.4 Sampling

Drawing a random sample from a definitive, enumerated list of e-commerce users in the UK was not possible. No such list exists. For this reason, participants were drawn from a non-probability, convenience sample. Undergraduate students were selected for participation. Internet use among students is ubiquitous (Office for National Statistics, 2017c). Fieldwork published by the European Commission (2017) suggests that 79% of students purchased a product or service online in the three months running up to data collected in 2016. This suggested that undergraduate students would have purchased a product or service from a website recently and therefore they would be a suitable demographic to participate in this study.

Thirty-five undergraduate students were recruited from a research methods module. The researcher contacted the responsible examiner for the module. The examiner agreed that undergraduate students could take part in the study during scheduled contact time. While the sample is unlikely to be representative of all UK e-commerce shoppers, students were the most appropriate choice of research participants given the time and budget constraints of this study.

3.7.1.5 Data Collection

A computer laboratory at Loughborough University was used to collect data in April 2016. Participants were provided with a paper-based set of instructions describing how to access each policy. Research participants used the same computers, operating system and web browser to access the standardised prototype and typical privacy policies. Separate tabs were used to display each policy within the same browser window. A practice question was completed at the beginning of the study. Following this, students then worked through the questions, post-task statements and post-study statements. Responses were recorded on paper. This allowed participants to view the privacy policy and questions/statements at the same time rather than alternating between browser tabs. The format of questions, post-task and post-study questions provided to participants is presented in appendix G.

Policy designs were counterbalanced. Participants were randomly assigned to one of two groups. Group one completed the task for the typical policy first followed by the standardised prototype policy. Group two completed the task for the standardised prototype policy first followed by the typical policy. Counterbalancing helps to reduce possible learning effects based on the ordering of tasks. Any differences between policies could then be attributed, with more confidence, to design of the policy and not the order in which participants viewed the policies.

3.7.1.6 Data Analysis

Paper based responses were entered into IBM SPSS. Descriptive statistics were used to summarise the responses to individual questions and statements. Likert items were treated as interval data therefore the mean was calculated as a measure of central tendency. Experts have long debated whether Likert data should be treated as ordinal or interval data for the purposes of analysis. Norman (2010) highlights that it is reasonable to treat Likert items as interval data. Norman shows that parametric statistics are highly robust to violations of normal distribution meaning that there is a small chance of drawing erroneous conclusions based on data that is skewed. Box (1979) also shows that the t-test is approximately robust when using a highly skewed distribution with a sample size of ten. Paired t-tests were used to test for statistically significant differences between policies. A paired samples t-test was an appropriate test in this instance because two policies were examined using the same participants.

3.8 Research Quality

In a mixed methods study, quality checks should be carried out for quantitative and qualitative research phases (Creswell and Plano Clark, 2011). Reliability and validity are the concepts used to evaluate quantitative research. Broadly speaking, reliability refers to the consistency of a measure and seeks to understand whether the findings of a study are repeatable. Validity refers to the extent to which the research measures what it purports to measure. Bryman (2008, p.32) notes that: “validity is concerned with the integrity of the conclusions that are generated from a piece of research.” Howitt and Cramer (2011) describe different types of reliability and validity. Stability, content validity and external validity are relevant to this research. A description of how these criteria were addressed in phases one and four is provided in table 3.11.

Qualitative research is evaluated differently. Lincoln and Guba (1985, p.290) speak of trustworthiness. They state that: “the basic issue in relation to trustworthiness is simple. How can an inquirer persuade his or her audiences that the findings of an inquiry are worth paying attention to, worth taking account of?” Lincoln and Guba operationalise trustworthiness using four criteria: credibility, transferability, dependability and confirmability. Miles and Huberman (1994) also point out the criteria of action orientation in qualitative research. These criteria and the steps taken to address them for phases two and three are presented in table 3.11.

Creswell and Plano Clark (2011, p.239) point out that research quality should also be addressed when mixing research methods. They state that mixed methods validity involves addressing issues that: “might compromise the merging or connecting of quantitative and qualitative strands of the study and the conclusions drawn from the combination.” Creswell and Plano Clark outline strategies to address issues associated with mixing methods in sequential and concurrent study designs. Those relevant to this research are identified in table 3.10.

Quantitative phases		
	Phase One	Phase Four
Stability – to what degree are the findings consistent over time?	Pre-test reliability and post-test reliability were calculated in 2012 and 2015. *(Sections 3.1.4.5 and 3.1.4.7).*	Not applicable.
Content validity – to what degree do the items measure the concept being examined?	A broad range of variables were adopted from the organisation responsible for operationalising the concept under study. *(Section 3.4.1.1 and appendix A)*	Variables were adopted from established instruments where findings showed high levels of internal consistency. *(Section 3.7.1.2)*
External validity – to what degree are the findings generalisable?	Potential for the findings to be applied generally. The use of one coder was a limiting factor therefore claims were only made about the sample analysed. *(Section 3.1.4.5)*	Non-random sampling meant that claims were only made about students and not the entire population of UK e-commerce users. *(Section 3.7.1.3)*
Qualitative phases		
	Phase Two and Phase Three	
Credibility – do the findings ring true,	- Purposeful sampling was used. A relationship was established with participants prior to inquiry helping to	

seem convincing and plausible?	build trust. It was important to demonstrate that responses would not be used against participants. - Peer debriefing. Findings were reviewed by experienced academics at various stages during investigation for the purpose of clarifying meanings, biases and interpretations. *(Sections 3.5.1.3 and 3.6.1.2)*
Transferability – to what degree are the findings applicable in other contexts?	- A thick description of the context, settings and protocol for study are provided to support judgements about the transferability of findings to other settings. - The sampling strategy is described and justified. *(Sections 3.5 and 3.6)*
Auditability – Is the research process consistent?	- A philosophical research stance is provided. - Research methods are justified considering the nature of the questions begin asked. - Coding checks were made to ensure consistency with participant responses. *(Sections 3.1, 3.5.1.5 and 3.6.1.4)*
Confirmability – is the research free from bias? Or is bias explicitly described?	- Materials were kept ensuring that bias can be judged. - Materials include electronic recordings of focus groups, transcriptions, field notes, revisions of categories and themes and notes about methodological decisions made. *(Sections 3.5.1.5 and 3.6.1.4)*
Action orientation – What does the study do for researchers and participants?	- Findings supported the development of a policy that could be used in practice. - Findings contributed towards solving policy problems discussed in the literature review.
Mixed method study	
	All phases
Research questions	A justification of why the research aim is best approached using mixed methods is provided. *(Section 3.2)*
Mixing strategy	The connections between phases are described broadly in the methodology chapter and more explicitly before

	the findings of each phase are presented. *(Sections 3.3, 5.2, 6.2 and 7.2)*

Table 3.10 - Research quality criteria

3.9 Ethical Considerations

Research involving human participants requires justification on the grounds that it is ethical to undertake. Researchers have a duty of care to participants. Research should not cause harm or deceive participants. At Loughborough University an ethical approval checklist is completed for every study involving human participants. If the study involves working with particularly vulnerable participants (or any other ethical concern of considerable nature) then a secondary, more in depth ethical justification is required.

For this research, an ethical checklist was approved. The checklist covers the principles of informed consent, investigator safety, vulnerable participants and data protection. The Code of Practice for Investigations involving Human Participants published by Loughborough University (2017) provides guidance on ethical considerations in research projects.

Prior to each investigation involving human participants in this study, participants were required to provide informed consent. Informed consent was provided on the basis that participants were aware of the context of research. Participants were provided with a research information sheet prior to study disclosing the nature of the research and other information about data protection along with the option to withdraw consent. A financial incentive in the form of an Amazon voucher worth ten pounds was provided to participants in phase two. This was approved by the ethics committee at Loughborough University.

3.10 Summary

In this chapter the philosophical underpinnings and methodology used to address the research aim were described. Based on the pragmatic approach outlined by Morgan (2007), a multiphase, mixed methods research strategy was used explore how UK e-commerce privacy policies could be improved. Four sequential research phases that were carried out. Phase one addressed research question one. Phases two, three and four addressed research questions two to six. Research questions two to six emerged based on the findings of each phase. Data collection and analysis methods used in each phase were outlined. Criteria for evaluating the quality of this research was also presented along with an outline of the ethical considerations relevant to this study.

Chapter 4 - Phase One: Good Practice

4.1 Introduction

Phase one addressed research question one. Research question one was: **to what extent do UK e-commerce privacy policies follow good practice guidelines?** To address this question a content analysis of privacy policies was carried out in 2012 and 2015. This chapter presents a statistical analysis of these two studies. The sample (presented in appendix C) consisted of 200 websites. In 2012, 18 websites were removed from the sample. In 2015, 17 websites were excluded from the sample. The reasons for exclusion are tabulated in appendix C. The most common reasons for removal were: the privacy policy could not be found; the website had ceased trading and the website was owned by a group that were already included within the sample. After exclusion, data were collected from 182 privacy policies in 2012 and 165 privacy policies in 2015.

Findings for each good practice variable are presented individually. The findings from the 2012 sample (182 privacy policies) and the 2015 sample (165 privacy policies) are tabulated for each good practice variable. In addition, a third data point is also presented, named 2012a. This data point shows the 2012 findings with the removal of the 17 privacy policies that were not analysed in 2015. This enabled a like for like comparison of differences between 2012 and 2015. At the end of this chapter a cumulative account of privacy policy good practice compliance is provided. Figure 4.1 provides an overview of the different research phases in this study showing how phase one fits in with the overall research design.

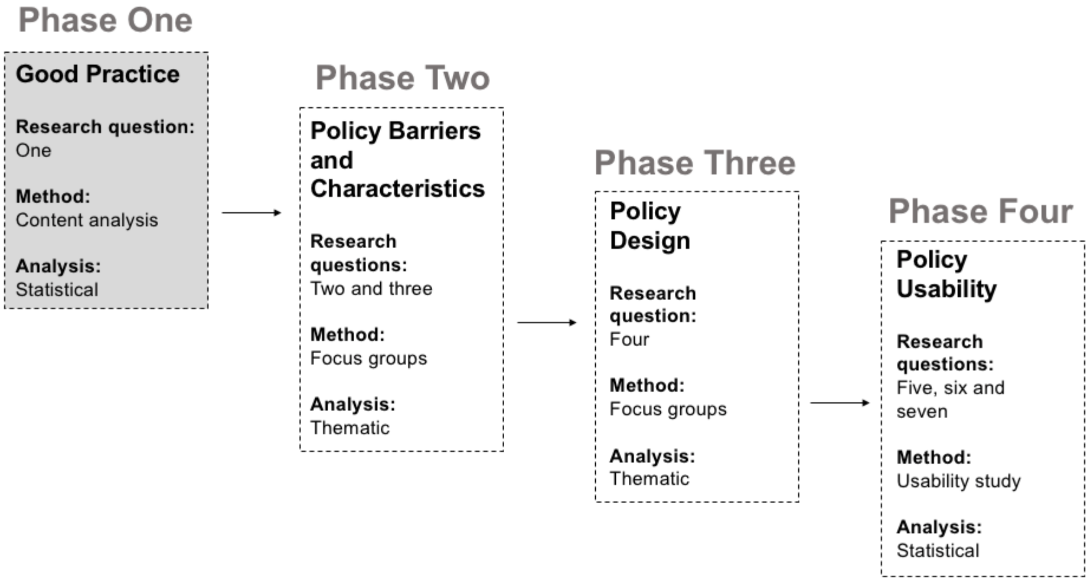


Figure 4.1 – Research design

4.2 Format

Variable 1.1 examined privacy policy format. Table 4.1 shows that this study found no evidence of websites publishing a layered privacy policy in 2012 or 2015. McNemar's test was not performed because it was clear no change occurred between 2012 and 2015.

1.1. Is the privacy policy presented in a layered format?			
	2012 (%)	2012a (%)	2015 (%)
No	182 (100.0)	165 (100.0)	165 (100.0)
Yes	0 (0.0)	0 (0.0)	0 (0.0)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.1 - Frequency of privacy policies presented in a layered format

4.3 Effective Date

Variable 2.1 examined whether each privacy policy included a date of last update. In 2012, only 17% privacy policies included a date of last update. Table 4.2 shows that this increased slightly to just under 21% in 2015. An exact McNemar's test determined that the change in proportion between 2012 and 2015 was not statistically significant (n= 165; p=0.263). This is shown in table 4.3.

2.1 Does the privacy policy state when the policy was last updated?			
	2012 (%)	2012a (%)	2015 (%)
No	151 (83.0)	137 (83.0)	131 (79.4)
Yes	31 (17.0)	28 (17.0)	34 (20.6)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.2 - Frequency of privacy policies that included a date of last update

2.1 Does the privacy policy state when the policy was last updated?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	124 (75.2)	13 (7.9)	137 (83.0)
	Yes	7 (4.2)	21 (12.7)	28 (17.0)
	Total	131 (79.4)	34 (20.6)	165 (100.0)
				Exact McNemar's test: p=0.263

Table 4.3 - Cross tabulation of privacy policies that included a date of last update

4.4 Data Controller Identity and Purposes for Processing

Variable 3.1 measured whether each privacy policy *explicitly* mentioned the identity of the data controller. For example, the privacy policy from Sainsbury's (2012):

> Sainsbury's Supermarkets Ltd is a registered Data Controller under the terms of the Data Protection Act 1998, Details of the Sainsbury's Supermarkets Ltd notification to the Regulator for data protection, may be found in the Information Commissioner's Office Public Register of Data Controllers at www.ico.gov.uk under registration number Z4722394.

In this instance, the privacy policy had used the term *data controller* to reference the identity of the organisation responsible for the processing of personal data. Table 4.4 shows that 22% of privacy policies explicitly mentioned the identity of the data controller in 2012. This proportion increased to just under 29% in 2015. An exact McNemar's test determined that the change in the proportion between 2012 and 2015 was statistically significant (n=165; p=0.035). This is as shown in table 4.5.

3.1. Does the privacy policy explicitly mention the identity of the data controller?			
	2012 (%)	2012a (%)	2015 (%)
No	142 (78.0)	129 (78.2)	118 (71.5)
Yes	40 (22.0)	36 (21.8)	47 (28.5)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.4 - Frequency of privacy policies explicitly mentioning the identity of the data controller

3.1 Does the privacy policy explicitly mention the identity of the data controller?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	112 (67.9)	17 (10.3)	129 (78.2)
	Yes	6 (3.6)	30 (18.2)	36 (21.8)
	Total	118 (71.5)	47 (28.5)	165 (100.0)
Exact McNemar’s test: p=0.035				

Table 4.5 - Cross tabulation of privacy policies explicitly mentioning the identity of the data controller

Those privacy policies that did not explicitly identify the data controller were examined to determine whether it was possible to *infer* the identity of the data controller. This study considered it possible to infer identity where the privacy policy included the name of an organisation. Some privacy policies included a statement discussing privacy at the start of the policy and the name of an organisation was mentioned. For example, the privacy policy from Tesco (2015) stated:

> Tesco is committed to protecting your privacy. This Privacy Policy explains our data processing practices and your options regarding the ways in which your personal data is used.

In this instance, it could be inferred that the data controller is Tesco. Other privacy policies did not include any statement about privacy but did include a written address or email address with an organisational name. For example, the privacy policy from The Office (2012) stated:

> In this Privacy Policy, we, us and our, refer to OFFICE Limited,
> registered in England & Wales.
>
> Our registered office is:
> OFFICE Ltd
> 9-10 Great Sutton Street
> London
> EC1V 0BX

In this instance, it could be inferred that the address refers to the identity of the data controller. Table 4.6 shows that it was possible to infer identity of the data controller in just over 93% of privacy policies that did not explicitly state the identity of the data controller in 2012 and 2015. An exact McNemar's test determined that the change in the proportion between 2012 and 2015 was not statistically significant, (n=112; p=1.000). This is shown in table 4.7.

3.2 If no to 3.1, is it possible to infer who the data controller is from the privacy policy?			
	2012 (%)	2012a (%)	2015 (%)
No	9 (6.3)	8 (6.2)	8 (6.8)
Yes	133 (93.7)	121 (93.8)	110 (93.2)
Total	142 (100.0)	129 (100.0)	118 (100.0)

Table 4.6 - Frequency of privacy policies where it was possible to infer the identity of the data controller

3.2 If no to 3.1, is it possible to infer who the data controller is from the privacy policy?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	2 (1.8)	6 (5.4)	8 (7.1)
	Yes	5 (4.5)	99 (88.4)	104 (92.9)
	Total	7 (6.3)	105 (93.8)	112 (100.0)
				Exact McNemar's test: p=1.000

Table 4.7 - Cross tabulation of privacy policies where it was possible to infer the identity of the data controller

Variable 3.3 measured whether each privacy policy mentioned one or more purposes for which personal data would be processed. Table 4.8 shows that approximately 98% of privacy policies in 2012 and 2015 identified a purpose or purposes for which personal data is processed. An exact McNemar's test determined that the difference in the proportion between 2012 and 2015 was not statistically significant (n=165; p=1.000). This is shown in table 4.9.

3.3 Does the privacy policy identify the purpose or purposes for which personal data will be processed?			
	2012 (%)	2012a (%)	2015 (%)
No	4 (2.2)	2 (1.2)	3 (1.8)
Yes	178 (97.8)	163 (98.8)	162 (98.2)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.8 - Frequency of privacy policies mentioning the purpose or purposes for which personal data will be processed

3.3 Does the privacy policy identify the purpose or purposes for which personal data will be processed?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	0 (0.0)	2 (1.2)	2 (1.2)
	Yes	3 (1.8)	160 (97.0)	163 (98.8)
	Total	3 (1.8)	162 (98.2)	165 (100.0)
				Exact McNemar's test: p=1.000

Table 4.9 - Cross tabulation of privacy policies mentioning the purpose or purposes for which personal data will be processed

Variable 3.4 assessed whether each privacy policy mentioned a named contact. The findings in table 4.10 show that only four (2.2%) out of one hundred and eighty-two privacy policies provided a named contact in 2012 with this decreasing to two (1.2%) from one hundred and sixty-five in 2015. An exact McNemar's test determined that the change in proportion between 2012 and 2015 was not statistically significant (n=165; p=1.000). This is shown in table 4.11.

3.4 Does the privacy policy identify a named individual to contact regarding personal data processing?			
	2012 (%)	2012a (%)	2015 (%)
No	178 (97.8)	162 (98.2)	163 (98.8)
Yes	4 (2.2)	3 (1.8)	2 (1.2)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.10 - Frequency of privacy policies mentioning a named individual to contact regarding personal data processing

3.4 Does the privacy policy identify a named individual to contact regarding personal data processing?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	162 (98.2)	0 (0.0)	162 (98.2)
	Yes	1 (0.6)	2 (1.2)	3 (1.8)
	Total	163 (98.8)	2 (1.2)	165 (100.0)
				Exact McNemar's test: p=1.000

Table 4.11 - Cross tabulation of privacy policies mentioning a named individual to contact regarding personal data processing

4.5 Personal Data Sharing for Direct Marketing Purposes

To understand whether UK B2C e-commerce websites followed best practice personal data sharing guidelines it was necessary to determine whether the website shared or might share personal data for direct marketing purposes. For variable 4.1 each privacy policy was coded to one of three responses. Policies were coded as *no* if they did not mention that personal data would or might be shared for direct marketing purposes. Policies were coded as *yes* if they did mention that personal data would or might be shared for direct marketing purposes. Alternatively, policies were coded as *open to interpretation* (OTI) if the policy mentioned something to suggest that personal data could be shared for direct marketing although the wording of the policy made it difficult to accurately gauge whether or not personal data would or might be shared for direct marketing. This study defined direct marketing as the communication of marketing material aimed at an individual. This is the definition used in section 14 of the DPA. For example, the privacy policy from Marisota (2015) stated:

> Unless you have previously stated otherwise, we may share your information with other carefully selected third party organisations. We or they may contact you for marketing purposes by mail, telephone, which may include automated calling systems, electronic mail or otherwise.

In this instance, the privacy policy has stated that personal information may be disclosed to carefully selected third party organisations and they may contact the individual for marketing reasons. Therefore, this privacy policy has also mentioned that personal data is or might be shared for direct marketing. Marisota's (2015) privacy policy is one example where it was straightforward to decide whether personal data would or might be shared for direct marketing. A minority of privacy policies used similar terminology although a small proportion of privacy policies required more interpretation. For example, the privacy policy from Argos (2012) mentioned:

> If you do not wish to receive information of products and services which may be of interest to you from us or carefully chosen third parties, please select the opt-out option where appropriate.

This privacy policy did not *directly state* that personal data is shared with third party organisations however this policy does state that the user should opt out of receiving information about products and services from carefully chosen third parties should they not wish to receive any correspondence. Therefore, it is reasonable to assume that if the user does not opt out the website may well share their personal data with a carefully chosen third party. This policy would then be coded as yes in response to variable 4.1.

The examples above highlight policies where personal data is or might be shared for direct marketing however there were also some policies where it was much more difficult to interpret whether or not personal data would be shared. For example, the privacy policy from Hobbs (2012):

> Updates and Promotional offers: if you have consented in advance we send you updates and information on our promotional offers. These may include joint promotions with our business partners.

In this example, the privacy policy mentions that if the user has consented they will be sent promotional offers and this may include joint promotions with business partners. Does this mean that personal data is shared with these business partners? The policy does not directly state that personal data is shared and therefore it is open to interpretation as to whether personal data is actually shared. It could be interpreted that personal data is shared with the organisation's business partners and used to send consumers information about promotional offers. Alternatively, it could be argued that the organisation may send users promotional offers on behalf of their business partners meaning no personal data is shared. Without further clarification on this point it is difficult to tell what this statement really means. However, because there is the possibility that personal data may be shared with business partners this policy would be coded as open to interpretation in response to variable 4.1.

The results in table 4.12 show that sixty-two (34.1%) privacy policies mentioned that personal data is or might be shared for direct marketing purposes in 2012 while sixty-five (39.4%) policies were considered as mentioning the same in 2015. A small proportion of privacy policies in both years included a statement where it was open to interpretation as to whether or not personal data would be shared for direct marketing. This amounted to seven (3.8%) privacy policies in 2012 and three (1.8%) privacy policies in 2015. A McNemar-Bowker's (Bowker, 1948) test determined that the change in proportion between 2012 and 2015 was not statistically significant (n=165; p=0.121). This is shown in table 4.13.

4.1 Does the privacy policy mention that personal data is or might be shared for direct marketing purposes (with or without the consent of the user)?			
	2012 (%)	2012a (%)	2015 (%)
No	113 (62.1)	101 (61.2)	97 (58.8)
Yes	62 (34.1)	57 (34.5)	65 (39.4)
Open to interpretation	7 (3.8)	7 (4.2)	3 (1.8)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.12 - Frequency of privacy policies mentioning personal data is or might be shared for direct marketing purposes

4.1 Does the privacy policy mention that personal data is or might be shared for direct marketing purposes (with or without the consent of the user)?					
			2015 (%)		
		No	Yes	OTI*	Total
2012 (%)	No	84 (50.9)	17 (10.3)	0 (0.0)	101 (61.2)
	Yes	10 (6.1)	47 (28.5)	0 (0.0)	57 (34.5)
	OTI*	3 (1.8)	1 (0.6)	3 (1.8)	7 (4.2)
	Total	97 (58.8)	65 (39.4)	3 (1.8)	165 (100.0)
					McNemar-Bowker's test: p=0.121

Table 4.13 - Cross tabulation of privacy policies mentioning personal data is or might be shared for direct marketing purposes

Variable 4.2 determined whether those privacy policies that mentioned personal data is or might be shared stated with whom personal data is shared. Variable 4.3 investigated the terms used to describe the sharing of personal data for marketing purposes. Table 4.14 shows that this study found that every privacy policy that mentioned that personal data is or might be shared stated with whom personal data would be shared. A statistical test was not performed for this variable because it was clear that there was no change between 2012 and 2015.

4.2 If yes to 4.1, does the privacy policy mention with whom personal data will be shared?			
	2012 (%)	2012a (%)	2015 (%)
No	0 (0.0)	0 (0.0)	0 (0.0)
Yes	62 (100.0)	57 (100.0)	65 (100.0)
Total	62 (100.0)	57 (100.0)	65 (100.0)

Table 4.14 - Frequency of privacy policies stating who personal data would be shared with

Table 4.15 and table 4.16 show the descriptions used to describe with whom personal data would be shared in 2012 and 2015 respectively. Some privacy policies included more than one name when describing with whom personal data would be shared for direct marketing meaning that the total number of terms recorded in both years was greater than the number of policies mentioning that personal data is or might be shared for direct marketing purposes. The results from variable 4.3 showed that the term *selected third parties* was recorded most frequently in both 2012 and 2015. In 2012 the term *selected third parties* accounted for nearly 25% of those terms recorded while in 2015 the same term accounted for just under 15% of terms recorded. The terms *third parties, carefully selected companies and carefully selected third parties* were also frequently recorded in 2012 and 2015. There was slightly more variability in the frequency of terms recorded in 2015 with 53 different terms recorded compared to 49 in 2012.

	Who personal data is or might be shared with for direct marketing purposes in 2012	Frequency (%)
1	Selected third parties	22 (24.4)
2	Third parties	7 (7.8)
3	Carefully selected companies	4 (4.4)
4	Carefully selected third parties	4 (4.4)
5	Other carefully selected companies	2 (2.2)
6	Other organisations	2 (2.2)
7	Business partners	2 (2.2)
8	Third party business partners	2 (2.2)
9	Our group companies	2 (2.2)
10	Other companies	2 (2.2)
11	Our partners	2 (2.2)
12	Other virgin group companies	2 (2.2)
13	Offspring	1 (1.1)
14	Associated companies within the group	1 (1.1)
15	Mutual commercial partners	1 (1.1)
16	Third parties we work with	1 (1.1)
17	Trusted third parties	1 (1.1)
18	Third party	1 (1.1)
19	Companies within the park group	1 (1.1)
20	Carefully selected organisations	1 (1.1)
21	Carefully chosen third parties	1 (1.1)
22	Other Arcadia Group Companies	1 (1.1)
23	Joint marketing partners	1 (1.1)
24	Other carefully selected third party organisations outside the group	1 (1.1)
25	Deckers Consumer Direct Corporation	1 (1.1)
26	Relevant third parties	1 (1.1)
27	Any company outside of Snow+Rock	1 (1.1)
28	Other selected third parties	1 (1.1)

29	Related third parties	1 (1.1)
30	Other carefully screened companies	1 (1.1)
31	Other carefully selected companies or organisations	1 (1.1)
32	Other companies in our group	1 (1.1)
33	Other companies within the universal music group	1 (1.1)
34	An artist or its management company	1 (1.1)
35	Partners	1 (1.1)
36	Other Prescription Eyewear Ltd brands	1 (1.1)
37	A third party	1 (1.1)
38	Carefully selected and trustworthy third parties	1 (1.1)
39	Reputable suppliers of goods or services	1 (1.1)
40	Carefully screened companies	1 (1.1)
41	Other companies or individuals	1 (1.1)
42	Subsidiaries or subsidary companies	1 (1.1)
43	Another trader	1 (1.1)
44	Other reputable companies	1 (1.1)
45	Trustworthy and reputable companies	1 (1.1)
46	Other companies or organisations	1 (1.1)
47	Cox & Cox Wholesale Limited	1 (1.1)
48	Cake Designs UK Limited	1 (1.1)
49	Plantstuff Limited	1 (1.1)
	Total	90 (100.0)

Table 4.15 - Terms recorded to describe the sharing of personal data for direct marketing purposes in 2012

	Who personal data is or might be shared with for direct marketing purposes in 2015	Frequency (%)
1	Selected third parties	12 (13.5)
2	Carefully selected third parties	9 (10.1)
3	Third parties	8 (9.0)
4	Carefully selected companies	4 (4.5)
5	Partners	3 (3.4)
6	Subsidiaries	2 (2.2)
7	Our group of companies	2 (2.2)
8	Our group companies	2 (2.2)
9	Our partners	2 (2.2)

10	Another trader	2 (2.2)
11	Other companies within the JD Sports Fashion Group	1 (1.1)
12	Affiliates	1 (1.1)
13	Other carefully selected companies	1 (1.1)
14	Vertbaudet	1 (1.1)
15	Daxon	1 (1.1)
16	Across the Tesco Group	1 (1.1)
17	Other members of the La Redoute Group	1 (1.1)
18	Companies within the Park group	1 (1.1)
19	Offspring	1 (1.1)
20	Carefully selected third party organisations	1 (1.1)
21	Mutual commercial partners	1 (1.1)
22	Our group	1 (1.1)
23	Affiliated companies	1 (1.1)
24	Related third parties	1 (1.1)
25	Carefully selected companies or organisations	1 (1.1)
26	Other reputable companies	1 (1.1)
27	Any other MyOptique Group Ltd brands	1 (1.1)
28	Carefully selected and trustworthy third parties	1 (1.1)
29	Reputable suppliers of goods or services	1 (1.1)
30	Other third parties	1 (1.1)
31	Carefully screened companies	1 (1.1)
32	Carefully selected retail partners	1 (1.1)
33	Subsidiary companies	1 (1.1)
34	Companies within the same group as MGN Ltd	1 (1.1)
35	Trustworthy and reputable companies	1 (1.1)
36	Other companies or organisations	1 (1.1)
37	Virgin group companies	1 (1.1)
38	Other organisations	1 (1.1)
39	Carefully chosen third parties	1 (1.1)
40	Other Arcadia group companies or other third parties	1 (1.1)
41	Joint marketing partners	1 (1.1)
42	Outside company	1 (1.1)
43	Third party business partners	1 (1.1)
44	Non-affiliated third parties	1 (1.1)

45	Trusted third parties	1 (1.1)
46	Third party companies	1 (1.1)
47	Relevant third parties	1 (1.1)
48	Carefully selected organisations	1 (1.1)
49	Any company outside of Snow and Rock	1 (1.1)
50	Specially selected third parties	1 (1.1)
51	Cox & Cox wholesale Limited	1 (1.1)
52	Cake Designs UK Limited	1 (1.1)
53	Plantstuff Limited	1 (1.1)
	Total	89 (100.0)

Table 4.16 – Terms recorded to describe the sharing of personal data for direct marketing purposes in 2015

The findings from variable 4.4 revealed that only three privacy policies in both 2012 and 2015 provided the *actual name* of the organisation they were going to share personal data with for direct marketing. This is shown in table 4.17. This equates to under 5% of privacy policies in both years. Table 4.18 shows that an exact McNemar's test determined that the change in proportion between 2012 and 2015 was not statistically significant (n=47; p=1.000).

4.4 If yes to 4.2, are any names of organisations mentioned?			
	2012 (%)	2012a (%)	2015 (%)
No	59 (95.2)	54 (94.7)	62 (95.4)
Yes	3 (4.8)	3 (5.3)	3 (4.6)
Total	62 (100.0)	57 (100.0)	65 (100.0)

Table 4.17 - Frequency of privacy policies mentioning the names of the organisation that personal data is shared with for direct marketing

4.4 If yes to 4.2, are any names of organisations mentioned?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	43 (91.5)	1 (2.1)	44 (93.6)
	Yes	1 (2.1)	2 (4.3)	3 (6.4)
	Total	44 (93.6)	3 96.4)	47 (100.0)
Exact McNemar's test: p=1.000				

Table 4.18 - Cross tabulation of privacy policies mentioning the names of the organisation that personal data is shared with for direct marketing

4.6 Accessing and Amending

Variable 5.1 measured whether each privacy policy provided users with the choice to access or amend personal data. Following this variable 5.2 examined whether each privacy policy explained how to access or amend personal data. For the purposes of variable 5.1 the privacy policy did not necessarily have to mention that it is the right of the user to access or amend personal data neither did it have to mention how to access or amend personal data. However, the policy did have to mention that it was possible to access or amend personal data. For example, the privacy policy from Fred Perry (2015) stated:

> The information we hold about you needs to be accurate and up to date. You can check and amend the information we hold about you. The personal information that we hold about you will be held in accordance with our internal security policies.

In this instance, the privacy policy does mention that it is possible to view and amend personal data however it does not mention anything about user rights or how to access or amend personal data. In contrast, the privacy policy from Vision Express (2015) stated:

> You are entitled by law to request from us whether we hold any of your personal information and, if so, to request a copy of it. If you wish to exercise your data subject access rights, please contact us in writing with sufficient information to verify your identity and the personal information you require to: the Data Compliance Officer, Vision Express (UK) Limited, Ruddington Fields Business Park, Mere Way, Ruddington, Nottingham NG11 6NZ.

In this instance, the privacy policy mentioned that it is the right of the user to access personal data being processed and also stated how that right can be exercised. Table 4.19 shows that in 2012 approximately 65% of privacy policies mentioned that it is possible to view or amend personal data with this proportion rising to just over 72% in 2015. An exact McNemar’s test determined that the change in the proportion between 2012 and 2015 was statistically significant (n=165; p=0.027). This is shown in table 4.20.

Further to this, not all those privacy policies that mentioned it was possible to access or amend personal data described how to access or amend personal data. In 2012, 55.5% of privacy policies mentioned how to access or amend personal data while 62.4% of policies were recorded as doing the same in 2015. An exact McNemar's test determined that the change in proportion between 2012 and 2015 was not statistically significant (n=165; p=0.108). This is shown in table 4.21.

5.1 Does the privacy policy mention that it is possible to view or amend personal data?			
	2012 (%)	2012a (%)	2015 (%)
No	64 (35.2)	57 (34.5)	46 (27.9)
Yes	118 (64.8)	108 (65.5)	119 (72.1)
Total	182 (100.0)	165 (100.0)	165 (100.0)
5.2 Does the privacy policy mention anything about how personal data being processed by the organisation can be viewed or amended?			
No	81 (44.5)	71 (43.0)	62 (37.6)
Yes	101 (55.5)	94 (57.0)	103 (62.4)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.19 - Frequency of privacy policies mentioning it was possible/how to access or amend personal data

5.1 Does the privacy policy mention that it is possible to view or amend personal data?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	41 (24.8)	16 (9.7)	57 (34.5)
	Yes	5 (3.0)	103 (62.4)	108 (65.5)
	Total	46 (27.9)	119 (72.1)	165 (100.0)
				Exact McNemar's test: p=0.027

Table 4.20 - Cross tabulation of privacy policies mentioning it was possible to access or amend personal data

5.2 Does the privacy policy mention anything about how personal data being processed by the organisation can be viewed or amended?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	54 (32.7)	17 (10.3)	71 (43.0)
	Yes	8 (4.3)	86 (52.1)	94 (57.0)
	Total	62 (37.6)	103 (62.4)	165 (100.0)
				Exact McNemar's test: p=0.108

Table 4.21 - Cross tabulation of privacy policies mentioning how to access of amend personal data

Variables 5.3 to 5.5 examined subject access rights outlined in part 2 of the DPA. Variable 5.3 measured whether each privacy policy mentioned that the data subject has the right to request a copy of personal data while variables 5.4 and 5.5 determined whether each privacy policy mentioned that the data subject has the right to amend and remove inaccurate personal data respectively. Privacy policies were coded as either yes or no in response to variables 5.3 to 5.5. For example, the privacy policy from Interflora (2015) stated:

> We have a legal obligation to ensure that the personal information is kept accurate and up to date. Please assist us to comply with this obligation by informing us of any changes to the personal information. You have the right to request details of the information we hold about you and to delete or rectify any inaccurate information about you by sending us a written request to:
>
> Customer Liaison
> Interflora British Unit
> Interflora House
> Sleaford
> Lincolnshire NG34 7TB

In this instance, the privacy policy had explicitly mentioned that users have the right to request a copy of personal data and correct or delete any inaccurate personal data and were therefore be coded as a yes in response to variables 5.3, 5.4 and 5.5. However, a privacy policy did not necessarily have to explicitly mention that users have the right to access, amend or delete inaccurate personal data to be coded as a yes for variables 5.3 to 5.5. Those policies that included information about user rights under the heading of *legal information* or something similar were also considered as mentioning the existence of subject access rights. Findings in table 4.22 show that sixty-five (37.5%) privacy policies mentioned the user had the right to access personal data in 2012 whereas seventy (42.4%) privacy policies were considered as doing the same in 2015. Fewer privacy policies mentioned that users have the right to amend or delete inaccurate personal data. In total only nineteen (10.4%) privacy policies mentioned that users have the right do rectify inaccurate personal data in 2012 with twenty-six (15.8%) privacy policies recorded as doing the same in 2015. Additionally, only five (2.7%) policies mentioned users have the right to remove inaccurate personal data in 2012 while twelve (7.3%) privacy policies did the same in 2015.

5.3 Does the privacy policy mention that it is the right of the user to request a copy of the personal data being processed?			
	2012 (%)	2012a (%)	2015 (%)
No	117 (64.3)	106 (64.2)	95 (57.6)
Yes	65 (35.7)	59 (35.8)	70 (42.4)
Total	182 (100.0)	165 (100.0)	165 (100.0)
5.4 Does the privacy policy mention that it is the right of the user to amend inaccurate personal data being processed?			
No	163 (89.6)	149 (90.3)	139 (84.2)
Yes	19 (10.4)	16 (9.7)	26 (15.8)
Total	182 (100.0)	165 (100.0)	165 (100.0)
5.5 Does the privacy policy mention that it is the right of the user to remove inaccurate personal data being processed?			
No	177 (97.3)	160 (90.3)	153 (92.7)
Yes	5 (2.7)	5 (3.0)	12 (7.3)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.22 - Frequency of privacy policies mentioning subject access rights

There was an overall increase in the proportion of privacy policies mentioning each right in 2015 compared to 2012. A McNemar's test with continuity correction (Edwards, 1948) determined that the change in proportion of privacy policies mentioning that it is the right of the individual to access personal data between 2012 and 2015 was not statistically significant (n=165; $\chi^2(1)=3.448$; p=0.063). This is shown in table 4.23. Further to this, an exact McNemar's test determined that the change in proportion of privacy policies mentioning that it is the right of the user to amend inaccurate personal data between 2012 and 2015 was statistically significant (n=165;

p=0.006). This is shown in table 4.24. Finally, an exact McNemar’s test determined that the change in proportion of privacy policies mentioning that it is the right of an individual to remove inaccurate personal data between 2012 and 2015 was statistically significant (n=165; p=0.016). This is shown in table 4.25.

5.3 Does the privacy policy mention that it is the right of the user to request a copy of the personal data being processed?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	86 (52.1)	20 (12.1)	106 (64.2)
	Yes	9 (5.5)	50 (30.3)	59 (35.8)
	Total	95 (57.6)	70 (42.4)	165 (100.0)
McNemar’s test with continuity correction: p=0.063				

Table 4.23 - Cross tabulation of privacy policies mentioning the right to access personal data

5.4 Does the privacy policy mention that it is the right of the user to amend inaccurate personal data being processed?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	138 (83.6)	11 (6.7)	149 (90.3)
	Yes	1 (0.6)	15 (9.1)	16 (9.7)
	Total	139 (84.2)	26 (15.8)	165 (100.0)
Exact McNemar’s test: p=0.006				

Table 4.24 - Cross tabulation of privacy policies mentioning the right to amend inaccurate personal data

5.5 Does the privacy policy mention that it is the right of the user to remove inaccurate personal data being processed?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	153 (92.7)	7 (4.2)	160 (97.0)
	Yes	0 (0.0)	5 (3.0)	5 (3.0)
	Total	153 (92.7)	12 (7.3)	165 (100)
Exact McNemar’s test: p=0.016				

Table 4.25 - Cross tabulation of privacy policies mentioning the right to remove inaccurate personal data

4.7 Direct Marketing Preferences

Variable 6.1 measured whether each policy provided a user with the choice to prevent personal data being used for direct marketing. Further to this, variable 6.2 examined whether each policy mentioned *how* to prevent personal data being used for direct marketing. In much the same respect as variable 5.1 the privacy policy did not necessarily have to mention *how* to amend direct marketing preferences to be considered as mentioning that is possible to change direct marketing preferences. For example, the privacy policy from Forbidden Planet (2015) stated:

> We will not e-mail you in the future unless you have given us your consent. We will give you the chance to refuse any marketing email from us or from another trader in the future.

In this instance, the privacy policy did not state how to prevent personal data being used for direct marketing purposes but it did mention that users will be given the opportunity to refuse direct marketing. Therefore, the privacy policy has mentioned that it is possible to prevent personal data being used for direct marketing.

Table 4.26 shows that a large proportion of privacy policies mentioned that it is possible to prevent personal data being used for direct marketing. In 2012, one hundred and thirty-two (72.5%) privacy policies mentioned that it is possible to prevent personal data being used for direct marketing while in 2015, four more (82.4%) privacy policies were recorded as doing the same. However, not all of those privacy policies that stated it was possible to prevent personal data being used for direct marketing described how a user would go about doing so. In 2012, 68.7% of privacy policies stated how an individual would go about preventing personal data being used for direct marketing while in 2015, 77.6% of privacy policies mentioned the same. An exact McNemar’s test determined that the change in proportion of privacy policies mentioning that it is possible to prevent personal data being used for direct marketing between 2012 and 2015 was statistically significant (n=165; p=0.002). This is shown in table 4.27. In addition, an exact McNemar’s test determined that the change in proportion of privacy policies mentioning how to prevent personal data being used for direct marketing between 2012 and 2015 was statistically significant (n=165; p=0.004). This is shown in table 4.28.

6.1 Does the privacy policy mention that it is possible to prevent personal data being used for direct marketing?			
	2012 (%)	2012a (%)	2015 (%)
No	50 (27.5)	45 (27.3)	29 (17.6)
Yes	132 (72.5)	120 (72.7)	136 (82.4)
Total	182 (100.0)	165 (100.0)	165 (100.0)
6.2 Does the privacy policy mention how to prevent personal data being used for direct marketing purposes?			
No	57 (31.3)	51 (30.9)	37 (22.4)
Yes	125 (68.7)	114 (69.1)	128 (77.6)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.26 - Frequency of privacy policies mentioning it is possible/how to prevent personal data being used for direct marketing

6.1 Does the privacy policy mention that it is possible to prevent personal data being used for direct marketing?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	25 (15.2)	20 (12.1)	45 (27.3)
	Yes	4 (2.4)	116 (70.3)	120 (72.7)
	Total	29 (17.6)	136 (82.4)	165 (100.0)
Exact McNemar's test: p=0.002				

Table 4.27 – Cross tabulation of privacy policies mentioning it is possible to prevent personal data being used for direct marketing

6.2 Does the privacy policy mention how to prevent personal data being used for direct marketing purposes?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	33 (20.0)	18 (10.9)	51 (30.9)
	Yes	4 (2.4)	110 (66.7)	114 (69.1)
	Total	37 (22.4)	128 (77.6)	165 (100.0)
Exact McNemar's test: p=0.004				

Table 4.28 - Cross tabulation of privacy policies mentioning how to prevent personal data being used for direct marketing

Variable 6.3 measured whether each privacy policy disclosed that it is the right of the user to prevent personal data being used for direct marketing. This variable followed the same rules of coding applied to variables 5.3 to 5.5. Table 4.29 demonstrates that in 2012 only nineteen (10.4%) privacy policies mentioned something about the existence of the right to prevent personal data being used for direct marketing while in 2015 only twenty-one (12.7%) privacy policies mentioned the same. An exact McNemar's test determined that the change in proportion between 2012 and 2015 was not statistically significant (n=165, p=0.302). This is shown in table 4.30.

6.3 Does the privacy policy mention that it is the right of the user to prevent personal data being processed for direct marketing purposes?			
	2012 (%)	2012a (%)	2015 (%)
No	163 (89.6)	149 (90.3)	144 (87.3)
Yes	19 (10.4)	16 (9.7)	21 (12.7)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.29 - Frequency of privacy policies mentioning the right to prevent personal data being used for direct marketing

6.3 Does the privacy policy mention that it is the right of the user to prevent personal data being processed for direct marketing purposes?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	139 (84.2)	10 (6.1)	149 (90.3)
	Yes	5 (3.0)	11 (6.7)	16 (9.7)
	Total	144 (87.3)	21 (12.7)	165 (100.0)
Exact McNemar's test: p=0.302				

Table 4.30 - Cross tabulation of privacy policies mentioning the right to prevent personal data being used for direct marketing

4.8 Accountability

Variable 7.1 determined whether each privacy policy mentioned that a user can complain to the Information Commissioner about any aspect of personal data processing should they wish so to do. The results in table 4.31 show that in 2012 just one (0.5%) privacy policy mentioned that the user has that option to contact the ICO should they wish to. In 2015 this study found no evidence of privacy policies stating that users could contact the ICO. A statistical test was not performed for this variable because there were no changes in the proportion of privacy policies mentioning individuals can contact the ICO between 2012 and 2015.

7.1 Does the privacy policy mention that the user has the option to contact the Information Commissioner's Office should a dispute arise?			
	2012 (%)	2012a (%)	2015 (%)
No	181 (99.5)	165 (100)	165 (100)
Yes	1 (0.5)	0 (0)	0 (0)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.31 - Frequency of privacy policies mentioning that users have the option to contact the ICO

Variable 7.2 assessed whether each privacy policy included any recognised contact details. Findings in table 4.32 show that in 2012 and 2015 approximately four fifths of privacy policies included some form of contact details. A McNemar's test with continuity correction (Edwards, 1948) determined that the change in proportion between 2012 and 2015 was not statistically significant (n=165; $\chi^2(1)=0.552$; p=0.458). This is shown in table 4.33.

7.2 Does the privacy policy mention any contact details for the organisation?			
	2012 (%)	2012a (%)	2015 (%)
No	39 (21.4)	36 (21.8)	31 (18.8)
Yes	143 (78.6)	129 (78.2)	134 (81.2)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.32 - Frequency of privacy policies mentioning some form of contact details

7.2 Does the privacy policy mention any contact details for the organisation?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	19 (11.5)	17 (10.3)	36 (21.8)
	Yes	12 (7.3)	117 (70.9)	129 (78.2)
	Total	31 (18.8)	134 (81.2)	165 (100.0)
McNemar's test with continuity correction: p=0.458				

Table 4.33 - Cross tabulation of privacy policies mentioning some form of contact details

4.9 Retention

Variable 8.1 measured whether each privacy policy mentioned a specific length of time for which personal data will be retained. The results show that a very small proportion of privacy policies mentioned a specific data retention period in both years. Table 4.34 shows that in 2012 only four (2.2%) privacy policies mentioned a specific length of time for which personal data would be retained while in 2015 only six (3.6%) privacy policies were recorded as doing the same. An exact McNemar's test determined that the change in proportion between 2012 and 2015 was not statistically significant (n=165; p=0.500). This is shown in table 4.35.

8.1 Does the privacy policy mention a specific length of time personal data will be retained for?			
	2012 (%)	2012a (%)	2015 (%)
No	178 (97.8)	161 (97.6)	159 (96.4)
Yes	4 (2.2)	4 (2.4)	6 (3.6)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.34 - Frequency of privacy policies mentioning a specific personal data retention period

8.1 Does the privacy policy mention a specific length of time personal data will be retained for?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	159 (96.4)	2 (1.2)	161 (97.6)
	Yes	0 (0.0)	4 (2.4)	4 (2.4)
	Total	159 (96.4)	6 (3.6)	165 (100.0)
Exact McNemar's test: p=0.500				

Table 4.35 - Cross tabulation of privacy policies mentioning a specific personal data retention period

4.10 Security

Variable 9.1 determined whether each privacy policy mentioned anything about the technology or technologies used to keep personal data secure. For example, the 2012 M and Co (2012) privacy policy stated:

> We take the security of your transaction very, very seriously. All online purchases take place in a safe environment using the latest security technology to protect all of our customers. We encrypt your credit card

> information to ensure your transactions with us are private and protected whilst online. We accept orders only from Web browsers that permit communication through Secure Socket Layer (SSL) technology - this means you cannot inadvertently place an order through an unsecured connection.
>
> In technical terms this means:
>
> We use a state of the art payment platform; Customer credit card data is protected with the industry-standard Secure Sockets Layer (SSL) encryption when transferred over the Internet. SSL provides for a variety of encryption technologies including RSA, 3-DES and AES. Credit card details are encrypted with AES before being stored. The production network is partitioned into a proxy server tier, an application server tier, and a database server tier. Servers running at each tier are protected using ipchains/iptables firewalling, which is set to only permit the necessary network traffic and deny and log everything else. The front end of the entire infrastructure is protected with a virtual firewall rack from a company called Inkra (http://www.inkra.com/) which provides additional firewalling and DoS protection.

In this instance, the privacy policy has provided a detailed account of the various technologies used to help keep personal data secure. For example, the policy has mentioned that it uses secure socket layer (SSL) encryption to help prevent unauthorised access to stored information. The findings in table 4.36 show that around half of the privacy policies in 2012 (52.2%) and 2015 (47.3%) mentioned something about the technology or technologies used to keep personal data secure. A McNemar’s test with continuity correction determined that the change in the proportion between 2012 and 2015 was not statistically significant (n=165; $\chi^2(1)=1.750$; p=0.186). This is shown in table 4.37.

9.1 Does the privacy policy mention anything about the technology or technologies used to keep personal data secure?			
	2012 (%)	2012a (%)	2015 (%)
No	87 (47.8)	79 (47.9)	87 (52.7)
Yes	95 (52.2)	86 (52.1)	78 (47.3)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.36 - Frequency of privacy policies mentioning something about the technology or technologies used to keep personal data secure

9.1 Does the privacy policy mention anything about the technology or technologies used to keep personal data secure?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	69 (41.8)	10 (6.1)	79 (47.9)
	Yes	18 (10.9)	68 (41.2)	86 (52.1)
	Total	87 (52.7)	78 (47.3)	165 (100.0)
McNemar’s test with continuity correction: p=0.186				

Table 4.37 - Cross tabulation of privacy policies mentioning something about the technology or technologies used to keep personal data secure

Variable 9.2 examined whether each website published information on the security of personal data separately to the privacy policy, for example, in a security policy. This study defined separately as on another webpage or on a page that is different to the privacy policy where the website has used a web technology (such as CSS or JavaScript) meaning that a request for a new webpage is not required. A common example of the latter display is the use of tabs where a new webpage is not requested when the user clicks on another tab however information is presented on another page. The results shown in table 4.38 highlight that approximately a quarter of websites published security information separately to the privacy policy in 2012 and 2015. A McNemar’s test with continuity correction determined that the change in proportion between 2012 and 2015 was not statistically significant (n=165; $\chi^2(1)=0.593$; p=0.441). This is shown in table 4.39.

9.2 Does the website publish information on the security of personal data separately to the privacy policy?			
	2012 (%)	2012a (%)	2015 (%)
No	138 (75.8)	126 (76.4)	121 (73.3)
Yes	44 (24.2)	39 (23.6)	44 (26.7)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.38 - Frequency of websites publishing a cookie policy separately to the privacy policy

9.2 Does the website publish information on the security of personal data separately to the privacy policy?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	110 (66.7)	16 (9.7)	126 (76.4)
	Yes	11 (6.7)	28 (17.0)	39 (23.6)
	Total	121 (73.3)	44 (26.7)	165 (100.0)
				Exact McNemar's test: p=0.442

Table 4.39 - Cross tabulation of websites publishing a cookie policy separately to the privacy policy

Variable 9.3 analysed each website that published information on security separately to the privacy policy to determine whether the statement mentioned anything about the technology used to keep personal data secure. shows that approximately 85% of websites in 2012 and 2015 that published separate security information mentioned the technology used to keep personal data secure. An exact McNemar's test determined that the change in proportion between 2012 and 2015 was not statistically significant (n=28; p=0.250). This is shown in table 4.41.

9.3 If yes to 9.2, does the separate security information mention anything about the technology or technologies used to keep personal data secure?			
	2012 (%)	2012a (%)	2015 (%)
No	6 (13.6)	5 (12.8)	7 (15.9)
Yes	38 (86.4)	34 (87.2)	37 (84.1)
Total	44 (100.0)	39 (100.0)	44 (100.0)

Table 4.40 - Frequency of security policies mentioning something about the technology or technologies used to keep personal data secure

9.3 If yes to 9.2, does the separate security information mention anything about the technology or technologies used to keep personal data secure?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	2 (7.1)	3 (10.7)	5 (17.9)
	Yes	0 (0.0)	23 (82.1)	23 (82.1)
	Total	2 (7.1)	26 (92.9)	28 (100.0)
				Exact McNemar's test: p=0.250

Table 4.41 - Cross tabulation of security policies mentioning something about the technology or technologies used to keep personal data secure

4.11 Cookies

Variable 10.1 measured how many websites published a cookie policy. Findings in table 4.42 show that 85.2% of websites published a cookie policy in 2012 while almost 97.6% of websites did so in 2015. An exact McNemar's test determined that the change in proportion between 2012 and 2015 was statistically significant (n=165; p<0.001). This is shown in table 4.43.

10.1 Does the website publish a cookie policy?			
	2012 (%)	2012a (%)	2015 (%)
No	27 (14.8)	25 (15.2)	4 (2.4)
Yes	155 (85.2)	140 (84.8)	161 (97.6)
Total	182 (100.0)	165 (100.0)	165 (100.0)

Table 4.42 - Frequency of websites publishing a cookie policy

10.1 Does the website publish a cookie policy?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	3 (1.8)	22 (13.3)	25 (15.2)
	Yes	1 (0.6)	139 (84.2)	140 (84.8)
	Total	4 (2.4)	161 (97.6)	165 (100.0)
				Exact McNemar's test: p<0.001

Table 4.43 - Cross tabulation of websites publishing a cookie policy

Variable 10.2 determined how many UK B2C e-commerce cookie policies were published separately to the privacy policy. This study used the same definition as variable 9.2 to operationalise the term *separately*. The results show that eleven (7.1%) websites published a cookie policy separately to the privacy policy in 2012 with eighty-four (52.2%) of websites doing so 2015. This is shown in table 4.44. A McNemar's test with continuity correction determined that the change in proportion between 2012 and 2015 was statistically significant (n=139; $\chi^2(1)=54.391$; p<0.001). This is shown in table 4.45.

10.2 If yes to 10.1, does the website publish a cookie policy separately to the privacy policy?			
	2012 (%)	2012a (%)	2015 (%)
No	144 (92.9)	131 (93.6)	77 (47.8)
Yes	11 (7.1)	9 (6.4)	84 (52.2)
Total	155 (100.0)	140 (100.0)	161 (100.0)

Table 4.44 Frequency of websites publishing a cookie policy separately to the privacy policy

10.2 If yes to 10.1, does the website publish a cookie policy separately to the privacy policy?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	68 (48.9)	62 (44.6)	130 (93.5)
	Yes	2 (1.4)	7 (5.0)	9 (6.5)
	Total	70 (50.4)	69 (49.6)	139 (100.0)
McNemar's test with continuity correction: p<0.001				

Table 4.45 - Cross tabulation of websites publishing a cookie policy separately to the privacy policy

Variable 10.3 assessed whether privacy or cookie policies included a statement about why cookies are used. The content analyses found that the majority of privacy or cookie policies included a purpose or some purposes for which cookies will be used by the website. Table 4.46 shows that in 2012 almost 97% of those websites that published a cookie policy mentioned why cookies would be used while in 2015 close to 99% of those websites that published a cookie policy did the same. An exact McNemar's test determined that the change in proportion between 2012 and 2015 was not statistically significant (n=139; p=0.375). This is shown in table 4.47.

10.3 If yes to 10.1, does the cookie policy describe the purpose of purposes for which cookies are used?			
	2012 (%)	2012a (%)	2015 (%)
No	5 (3.2)	5 (3.6)	2 (1.2)
Yes	150 (96.8)	135 (96.4)	159 (98.8)
Total	155 (100.0)	140 (100.0)	161 (100.0)

Table 4.46 - Frequency of cookie policies mentioning the purpose or purposes for which cookies are used

10.3 If yes to 10.1, does the cookie policy describe the purpose of purposes for which cookies are used?				
		2015 (%)		
		No	Yes	Total
2012 (%)	No	1 (0.7)	4 (2.9)	5 (3.6)
	Yes	1 (0.7)	133 (95.7)	134 (96.4)
	Total	2 (1.04)	137 (98.6)	139 (100.0)
Exact McNemar's test: p=0.375				

Table 4.47 - Cross tabulation of cookie policies mentioning the purpose or purposes for which cookies are used

4.12 Cumulative Best Practice Count

A cumulative count of best practice was calculated to show how many best practice guidelines each privacy policy followed. The fifteen variables listed in table 4.48 were included in the cumulative count. These were best practice guidelines that all privacy policies should follow regardless of how personal information is processed. Third party sharing guidelines were not included in the cumulative count because organisations would only have to follow these guidelines if personal data was shared with a third party.

Variables		Followed good practice guidelines			
		2012 (%)	2012a (%)	2015 (%)	P < 0.05 (✓) P < 0.01 (✓✓)
1.1	Is the privacy policy presented in a layered format?	0 (0.0)	0 (0.0)	0 (0.0)	N/A
2.1	Does the privacy policy mention when the policy was last updated?	31 (17.0)	28 (17.0)	34 (20.6)	✘
3.1 or 3.2	Does the privacy policy explicitly mention the identity of the data controller? OR Is it possible to infer who the data controller is from the privacy policy?	173 (95.1)	157 (95.2)	157 (95.2)	✘
3.3	Does the privacy policy identify the purpose or purposes for which personal data will be processed?	178 (97.8)	163 (98.8)	162 (98.2)	✘
5.1	Does the privacy policy mention that it is possible to view or amend personal data?	118 (64.8)	108 (65.5)	119 (72.1)	✓
5.3	Does the privacy policy mention that it is the right of the user to request a copy of the personal data being processed?	65 (35.7)	59 (35.8)	70 (42.4)	✘
5.4	Does the privacy policy mention that it is the right of the user to amend inaccurate personal data being processed?	19 (10.4)	16 (9.7)	26 (15.8)	✓
5.5	Does the privacy policy mention that it is the right of the user to remove inaccurate personal data being processed?	5 (2.7)	5 (3.0)	12 (7.3)	✓
6.1	Does the privacy policy mention that it is possible to prevent personal data being used for direct marketing?	132 (72.5)	120 (72.7)	136 (82.4)	✓
6.3	Does the privacy policy mention that it is the right of the user to prevent personal data being processed for direct marketing purposes?	19 (10.4)	16 (9.7)	21 (12.7)	✘
7.1	Does the privacy policy mention that the user has the option to contact the	1 (0.5)	0 (0)	0 (0)	✘

	Information Commissioner’s Office should a dispute arise?				
7.2	Does the privacy policy mention any contact details for the organisation?	143 (78.6)	129 (78.2)	134 (81.2)	✗
8.1	Does the privacy policy mention a specific length of time personal data will be retained for?	4 (2.2)	4 (2.4)	6 (3.6)	✗
9.1 or 9.2	Does the privacy policy mention anything about the technology or technologies used to keep personal data secure? OR Does the separate security information mention anything about the technology or technologies used to keep personal data secure?	116 (63.7)	104 (63.0)	104 (63.0)	✗
10.3	Does the cookie policy describe the purpose or purposes for which cookies are used?	150 (96.8)	135 (96.4)	159 (98.8)	✗

Table 4.48 – Cumulative good practice variables

Table 4.49 shows the distribution of good practice scores. In 2012 each privacy policy followed a mean of 6.34 guidelines. This increased slightly in 2015 to a mean of 6.91 guidelines. One privacy policy followed zero guidelines in 2012 while the lowest score achieved in 2015 was two good practice guidelines. The highest score achieved in 2012 and 2015 was eleven and twelve good practice guidelines respectively. A paired samples t-test was used to determine the statistical significance of the findings. Three outliers were considered extreme. The paired t-test was run with and without extreme outliers. The outcome was almost identical therefore the extreme outliers were retained in the analysis. The test continued even though there was evidence of a non-normal distribution as assessed using Shapiro-Wilk’s test because the t-test is approximately robust even for highly skewed distributions (Launer & Wilkinson, 1979). Privacy policies achieved a higher mean good practice score in 2015 (6.91) compared to 2012 (6.33). The change between 2012 and 2015 (0.58; 95% CI 0.29 to 0.87) was statistically significant (t=3.97; df=164; p<0.001).

Number of good practice guidelines	Year		
	2012 (%)	2012a (%)	2015 (%)
0	1 (0.5)	0 (0.0)	0 (0.0)
1	3 (1.6)	3 (1.8)	0 (0.0)
2	4 (2.2)	4 (2.4)	3 (1.1)
3	12 (6.6)	10 (6.1)	2 (1.2)
4	17 (9.3)	16 (9.7)	11 (6.7)
5	18 (9.9)	17 (10.3)	19 (11.5)
6	35 (19.2)	33 (20.0)	35 (21.2)
7	40 (22.0)	37 (22.4)	37 (22.4)
8	24 (13.2)	21 (12.7)	25 (15.2)
9	17 (9.3)	14 (8.5)	16 (9.7)
10	7 (3.8)	7 (4.2)	12 (7.3)
11	4 (2.2)	3 (1.8)	4 (2.4)
12	0 (0.0)	0 (0.0)	1 (0.6)
13	0 (0.0)	0 (0.0)	0 (0.0)
14	0 (0.0)	0 (0.0)	0 (0.0)
15	0 (0.0)	0 (0.0)	0 (0.0)
Total	182 (100.0)	165 (100.0)	165 (100.0)
Mean	6.34	6.33	6.91
SD	2.17	2.10	1.92

Table 4.49 – Cumulative good practice distribution

4.13 Summary

This chapter presented the findings of two content analysis studies. One study was carried out in 2012. This was replicated and carried out again in 2015. The purpose of the content analyses was to address research question one. Research question one was: **to what extent do UK e-commerce privacy policies follow good practice guidelines?** Findings showed that privacy policies do not consistently follow good practice guidelines. Results also show there has been little change between 2012 and 2015. On average, privacy policies followed under half of the fifteen good practice guidelines measured in this study in both 2012 and 2015. No evidence of layered privacy policy adoption was found and only around a fifth of privacy policies contained a date of publication. A limited number of privacy policies mentioned a specific personal data retention period and only one privacy policy mentioned that users could contact that ICO to raise processing concerns. Many privacy policies did mention that it was possible for users to access personal data and prevent direct marketing however policies did not consistently mention that users had the right to do this. A high proportion of policies followed the most basic requirements of the law, that is to communicate the identity of the data controller, purposes for processing and reasons for using cookies.

Chapter 5 - Phase Two: Policy Barriers and Characteristics

5.1 Introduction

Phase two of this study addressed research question two and three. Research questions two and three were conceived based on the findings from phase one. Phase one showed UK e-commerce privacy policies do not consistently follow good practice guidelines. While phase one identified those privacy policies that do and do not follow good practice, it was felt that an investigation involving the subjects of privacy policies would help to unravel some of the more subjective elements of these statements. For example, the content analysis highlighted the terminology used to describe the sharing of personal data. While most organisations did not follow good practice in this area, the nature of the terminology used provoked additional questions such as: how do users perceive organisations that use such vague descriptions? For this reason, the researcher felt that it was worth exploring user attitudes towards privacy policies. It was felt that studying user perception towards privacy policies in detail might identify factors that contribute towards (non) readership of privacy policies. In consideration of these points, two broader research questions emerged:

2. **Why do e-commerce users ignore UK e-commerce privacy policies?**
3. **What do e-commerce users feel are the positive and negative characteristics of UK e-commerce privacy policies?**

To address research questions two and three questions five focus groups were carried out at the end of 2012 and start of 2013. This chapter presents the findings of these focus groups. Figure 5.1 provides an overview of the different research phases in this study showing how phase two fits in with the overall research design.

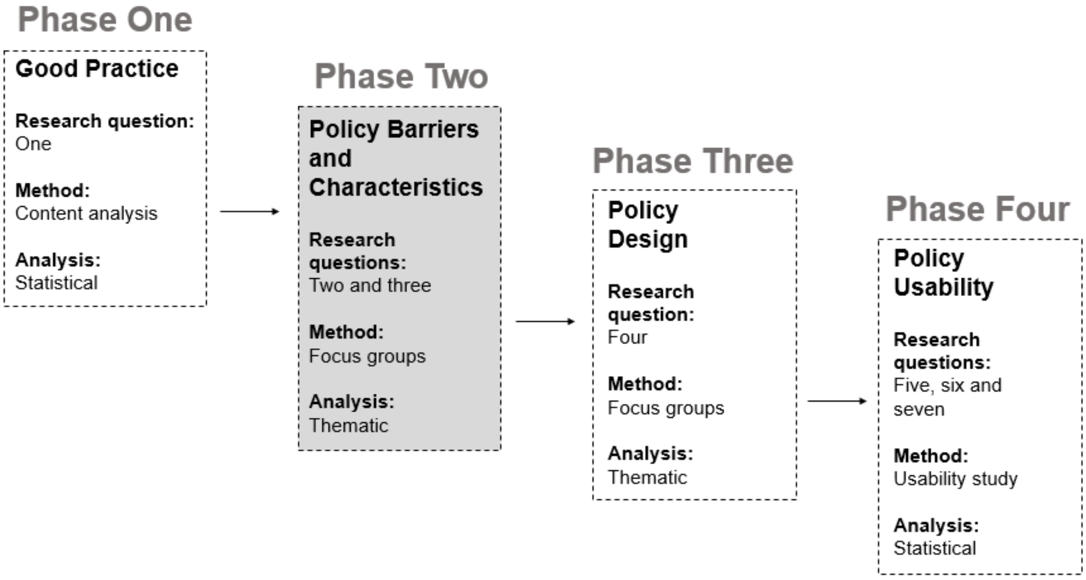


Figure 5.1 - Research design

5.2 Integration of Findings from Research Phase One and the Literature

Phase one findings showed that UK e-commerce privacy policies do not consistently follow good practice guidelines. Results also showed that policies use terms such as “carefully selected third parties”, “partners” and “members of the same group” to describe who personal data will or might be shared with for direct marketing. The literature showed that privacy policy length has received significant criticism. Selecting privacy policies that incorporated a blend of these issues ensured that important themes were reflected in this research and that new insightful data would be generated that would contribute towards the research aim.

In each focus group users were asked to read and take notes on positive and negative characteristics of privacy policies and personal data sharing extracts. The findings from phase one and the research literature guided the selection of privacy policies that users were asked to review in each focus group. Three privacy policies and three personal data sharing extracts were selected from the sample analysed in phase one. Policy A contained 1612 words, policy B contained 516 words and policy C contained 982 words. Phase one found that privacy policies do not consistently follow good practice guidelines. Policy A included thirteen good practice guidelines, policy B included ten and policy C included nine. The presence and absence of good practice guidelines for each privacy policy are summarised in table 5.1. Policy A published information on seven other personal data processing topics, policy B published information on three and policy C on six. The other personal data processing topics included in each policy are summarised in table 5.2. Summing good practice and other personal data processing topics together meant that overall policy A contained information on twenty personal data processing topics, policy B on thirteen and policy C on fifteen. The privacy policies reviewed in phase two can be found in appendix F.

Good practice guidelines from phase one	Policy		
	A	B	C
Is the privacy policy presented in a layered format?	✘	✘	✘
Does the privacy policy mention when the policy was last updated?	✘	✘	✘
Does the privacy policy explicitly mention the identity of the data controller?	✓	✘	✓
Is it possible to infer who the data controller is from the privacy policy?	N/A	✓	N/A
Does the privacy policy identify the purpose or purposes for which personal data will be processed?	✓	✓	✓
Does the privacy policy identify a named individual to contact regarding personal data processing?	✓	✘	✘
Does the privacy policy mention that personal data is or might be shared for direct marketing purposes (with or without the consent of the user)?	✓	✓	✓
Does the privacy policy mention with whom personal data will be shared?	✓	✓	✓
Are any names of organisations mentioned?	✘	✘	✘
Does the privacy policy mention that it is possible to view or amend personal data?	✓	✓	✓
Does the privacy policy mention that it is the right of the user to request a copy of the personal data being processed?	✓	✓	✓
Does the privacy policy mention that it is the right of the user to amend inaccurate personal data being processed?	✘	✓	✘
Does the privacy policy mention that it is the right of the user to remove inaccurate personal data being processed?	✘	✘	✘
Does the privacy policy mention that it is possible to prevent personal data being used for direct marketing?	✓	✓	✓

Does the privacy policy mention that it is the right of the user to prevent personal data being processed for direct marketing purposes?	✓	✗	✗
Does the privacy policy mention that the user has the option to contact the Information Commissioner’s Office should a dispute arise?	✓	✗	✗
Does the privacy policy mention any contact details for the organisation?	✓	✓	✓
Does the privacy policy mention a specific length of time personal data will be retained for?	✗	✗	✗
Does the privacy policy mention anything about the technology or technologies used to keep personal data secure?	✓	✗	✗
Does the cookie policy describe the purpose or purposes for which cookies are used?	✓	✓	✓
Total	13	10	9

Table 5.1 - Good practice guidelines for policies A to C

Other personal data processing topics	Policy		
	A	B	C
Categories of personal data collected	✓	✓	✓
Transfer of personal data outside the European Economic Area	✓	✗	✓
Mentioning of legislation	✓	✗	✓
Storage location	✓	✗	✓
Sharing personal data for purposes other than direct marketing	✓	✗	✓
Links to helpful privacy information	✓	✓	✗
Future changes	✓	✓	✓
Total	7	3	6

Table 5.2 - Other personal data processing topics for policies A to C

Data sharing extracts were selected based on findings from phase one. The extracts contain some of the common terms used to describe the sharing of personal data for direct marketing found in phase one (a full account of the terms recorded can be found in table 4.15 and table 4.16 in chapter four). The extracts are presented below. The characteristics of each extract are summarised in table 5.3.

Extract A

"Nu Books and Gifts may, from time to time, share your personal information with its affiliated company, Offspring. Offspring may contact you by post or by electronic mail services about new products, special offers or other information which we think you may find interesting using the delivery or email address which you have provided."

Extract B

"Unless you have previously stated otherwise, we may share your information with our associated companies within the Group and other carefully selected third party organisations outside the Group. We or they may contact you for marketing purposes by mail, telephone, electronic mail or otherwise."

Extract C

"If you give us consent then we may share your information with our partners, subsidiaries or subsidiary companies in order that they can contact you with information, promotions, products, services, and offers that may be interesting to you

Characteristics	Extract A	Extract B	Extract C
Described who personal data is shared with	✓	✓	✓
Names mentioned	Offspring	Associated companies within the group; other carefully selected third party organisations outside the group	Our partners, subsidiaries or subsidiary companies
Mentioned the name of an organisation	✓	✗	✗
Stated consent would be obtained prior to processing	✗	✓	✓
Stated method of contact	✓	✓	✗

Table 5.3 - Personal data sharing extract characteristics

The themes that emerged from the focus group discussions are presented below. The findings are split into three themes. Section 5.3 highlights reasons why users do not read privacy policies. Section 5.4 describes alternative mechanisms (apart from a privacy policy) that e-commerce consumers use to determine whether personal data is used fairly by a website. Finally, section 5.5 outlines the positive and negative aspects of the three policies reviewed. Focus groups are referred to throughout by the designation FG followed by a number. The terms users and consumers are used interchangeably to refer to focus group participants.

5.3 Barriers to Reading

Unsurprisingly all focus group participants except for one individual stated that they did not read privacy policies when buying products and services online. Some users expressed that they had seen a privacy policy before while others expressed the contrary. In FG5 one user said she “would never” search for a privacy policy and an individual in FG3 stated that he had “never read a privacy policy until today.” Interestingly, there was a collective opinion that other people do not read privacy policies as well. When asked if they read privacy policies participants replied with statements like “people don’t read privacy policies do they?” (FG1), “No one reads them” (FG2) and “People don’t want to read them.” (FG5). One user said, “you don’t really give it a second thought do you” (FG2) when asked about personal data usage by organisations. As well as this, one individual felt that the way an organisation handled his personal data was not a factor he considered when buying something online. He mentioned “you wouldn’t go online and be like: well I’m not buying that, it’s got a terrible privacy policy.”

Privacy policies are synonymous with “that tick box”, typically at the bottom of the page. One user pointed out that instead of reading a privacy policy he would scroll to the bottom of the page and “just tick the box” (FG4). A person in FG1 said she always ticks yes without reading the privacy policy while someone in FG2 described a privacy policy as “just like data protection. You have to click this box to continue.” For e-commerce consumers in FG1, FG3 and FG5 a privacy policy was described as that “small print.” Overall the findings showed several reasons why users do not read privacy policies. This section discusses these reasons beginning with the finding that some users do not expect to understand privacy policies.

5.3.1 Won't Understand

There is an expectation among some e-commerce users that they are unlikely to be able to understand policy content. During FG5 one individual felt that a privacy policy would "include words you don't understand, like legal terms." Additionally, in FG4, one user described a privacy policy as "a bunch of mumbo jumbo." Furthermore, one participant in FG2 pointed out:

> "You don't understand what they are saying anyway so what's the point in reading them if I have no idea what they are talking about?"

Policy language was an issue in FG5. One individual described the terminology as "very specific to the law" and she felt that this meant that "people would just not read them [privacy policies] or understand what they mean." This opinion was shared in FG4. One user noted that he was not willing to sit for fifteen to twenty minutes to read a privacy policy that was going to confuse him. One participant in FG3 felt that privacy policies deliberately try and confuse people. In addition, an individual in FG1 stated that "99% of people would read it [the privacy *policy] and still not understand what they're reading."*

5.3.2 Don't Understand

For some users the expectation not to understand a privacy policy was realised after reading policies A, B and C. There was a debate between two participants in FG3 about the use of security technology. Both participants acknowledged that they did not understand what SSL was or meant although one user viewed this term positively and felt that it provided a degree of "reassurance". The other user felt that the inclusion of the term within the policy was pointless because she was not aware of the meaning of SSL technology. Separately, but in the same focus group, another individual made the point that the term SSL could have been made up because she was unaware of its meaning. More generally, one user in FG4 expressed some frustration at not being able to understand policy A:

> "I mean, my lack of knowledge of what's in policy A. I could read it three times over but if I don't understand it, it's pointless!"

For an individual in FG2 the inability to understand a privacy policy was viewed in a more positive light. She felt that "the more I don't understand it, the more I think it's probably legit." For her, the use of legalistic terms was a sign of legitimacy and trust.

Participants also described their perceptions towards consent tick boxes. In FG4 one user felt that it was confusing that some check boxes were pre-ticked, and some were not. He felt that "you have to be careful with things like this [the tick boxes] because each website is worded differently." A similar opinion was expressed in FG3 where one user suggested that "those check boxes at the end are worded in a way which confuses people. They are there to *try and confuse you."*

5.3.3 Desire for Convenience

The desire for a quick transaction outweighed the desire to read a privacy policy for some individuals. During FG4 one person stated:

> "Online shopping is meant to be easy, isn't it? You want to buy your thing; have it sent to your house and get on with your life. You don't want to be sat there for 15 to 20 minutes reading a pile of paper that will confuse you."

A user in FG1 pointed out that reading a privacy policy would slow down the process of buying something online. This opinion was repeated in FG5 by one participant that stated the main reason for e-commerce is convenience and "you don't want to have to spend even more time looking through policies." That said, there was evidence that some users understood the limitations of not reading a privacy policy. One person openly acknowledged the pitfalls of not reading privacy policies when discussing the convenient nature of e-commerce:

> "And that is bad because they could exploit that and put stuff in their terms and conditions that they would give it [personal data] to their partners and so you could be in trouble. But that is what online shopping is about. Speed." (FG5)

This opinion was shared in FG1. A person in this focus group said that she always ticked yes to agreeing to the privacy policy even though she had not read it. Afterwards she admitted that the privacy policy "could mean anything and you've not actually read *it."*

5.3.4 Length

Before reading policies A, B and C some participants were critical of privacy policy length. An individual in FG2 pointed out that “a lot of them are like ten pages long and they are all in small text.” One user in FG5 stated that he felt that “…people won’t read them all the time because they are pages long…” while a person in FG1 described her expectation of a privacy policy as “lots and lots of words and paragraphs.” In addition, an e-commerce consumer described his opinion in the context of an online transaction:

> “It’s just the case that it is such a long document and you kind of put in your details and you have to sit there and read through all the small print” (FG4)

Users feel that longer policies take too long to read. One user from FG5 commented that it would “take hours to read all the policies” while one individual in FG2 simply said “it takes too much time to sit there and re*ad.”*

Policy length was also discussed after reading policies A, B and C. Some participants were critical of the length of policy A. The most common term used to describe policy A was “long winded” (FG1, FG2 and FG5). One participant in FG4 stated that he disliked policy A because it was “so long” while an individual in FG3 pointed out that policy A was “less attractive” compared to policy C because it was longer. Furthermore, one person in FG2 pointed out that policy A:

> “…was the one that was most long winded which is what I hate about these privacy policy things because they just go on for about 5 days…”

One participant in FG1 described the effect that policy A had on her. She felt this policy was daunting because it was considerably longer than policy B and she felt bored half way through reading policy A. Along with this, one person in FG2 stated that policy A “looks really detailed but would take ages to read.”

5.3.5 Format

Policy format was an issue for some e-commerce users. One individual felt that privacy policies are not “displayed or presented in any way where it makes you want to read it.” He described privacy policies as being formatted in “very small text.” This was a recurring theme across the focus groups. In FG1 policy text was described as “always being really small.” In FG2 one user referred to privacy policies as “all being in small text.” Similar findings materialised from FG4 where policies were labelled as “effectively being the small print at the end of the contract.” One person in FG4 succinctly pointed out that small text “means you don’t bother reading it [the privacy policy].”

5.3.6 You Haven’t Got a Choice

Some participants felt that they had to accept the personal data handling procedures of e-commerce organisations to purchase a product. During FG4 one participant stated:

> “The other thing about privacy is there is no alternative. You either agree with their privacy policy or you do not buy the product.”

This opinion was shared in FG3. One individual felt that it was “pointless to go through and read a privacy policy because regardless of what it says you’ve got to accept it.” Another user agreed. He stated that “you’ve just kind of got to go along with it really, especially if you are buying something. You haven’t got a choice.” In FG2 one person described the use of tick boxes. He felt that companies “make you tick anyway” and for this reason he felt no real desire to read the privacy policy.

5.3.7 They’re Not for Us

Findings revealed mixed evidence about the perceived purpose of a privacy policy. Many users felt that privacy policies exist to help organisations comply with legal obligations. Two individuals in FG1 felt that the purpose of a privacy policy is to help organisations “cover their arses”. Similar opinions were evident in FG2 and FG5. In these focus groups users felt organisations use privacy policies “to cover their own backs in case you complain” and “to protect themselves and say you have already agreed to this.” Notably, one person stated “they’re not for us, are they? They’re for big companies. Any company that takes your information has to have one” (FG3). In FG4 one individual referred to a privacy policy as a “type of legal protection for companies”. For one person in FG1, privacy policies are “worded in such a way that they’re not meant for people to really truly understand what they’re for.” She felt that privacy policies are “there just for companies to say they’ve done it” and not for the benefit of e-commerce users.

5.3.8 People Think They Are Just All the Same

Some individuals held the opinion that all privacy policies are already standardised. A user in FG5 described a privacy policy as *"just a standard thing at the bottom of the page."* Furthermore, one person thought that users do not read privacy policies because they think they're all the same:

> "I think now people actually think they are actually standardised so people think they are all the same anyway so they just sort of skip them." (FG2)

In response to being asked if all privacy policies are the same, one person in FG2 honestly admitted:

> "Errm, no. Now you have said that. But before, I would have been like, yeah!"

5.4 Privacy Proxies Not Privacy Policies

Participants were asked how they would determine whether a website uses their personal data fairly if they did not read privacy policies. Individuals infer website legitimacy and trust from other website components and external sources. Company size and familiarity was a source of trust for one individual in FG1. He stated that he would place more trust in a "big high street name like Next or River Island" compared to "if you were buying from Joeblogs.com". This participant felt that he could "automatically trust" large familiar websites and this meant that he would not need to read the website privacy policy. For some individuals company size was associated with perceived safety. One person in FG3 stated that "if it is *a* big company you kind of assume it [your personal data] will be alright". An individual in FG4 felt that larger organisations would invest more money into protecting customer personal data. This participant stated:

> "…I subconsciously think that a bigger company would probably be safer to put my bank details into because they would invest more money into security."

In FG5 one person described her experience of using the clothing retailer ASOS. She stated that she would never look or read the ASOS privacy policy and assumed that because "millions of people use them why would they not have a secure policy."

It is possible to determine whether a website complies with the law by consulting a privacy policy however the focus group findings suggested that users prefer to infer legitimacy in other ways. For some users, there is an expectation that they will learn about privacy breaches via the media. During FG5 one user stated:

> “It’s a really powerful tool, if there is something wrong with people’s rights you would hear about it in the news or somewhere online.”

Similar feelings were evident in FG4. One individual felt that if an organisation was misusing personal data “they would get a reputation for it quickly and you would hear about it”. Bearing this in mind, he felt “no news was good news.” For one person in FG3, website reviews were a source of legitimacy. This individual stated that he would check reviews left by other shoppers on comparison websites to determine whether an online store was “legit.” The look and feel of a website was a source of legitimacy for one user in FG5. She described her opinion in the context of a ticketing website:

> “It’s how professional the website looks, for me. Like, if you have a ticket website where they are trying to sell festival tickets and things look dodgy, it is quite obvious to spot if it is not legitimate.”

This opinion was shared by one individual in FG3. He openly acknowledged that he “makes a lot of assumptions that things are legit” by using the look and feel of a website as a source of legitimacy.

5.5 Positive and Negative Attributes

Attitudes towards policies A, B and C and extracts A, B and C were explored in each focus group. Findings are discussed in the following sections, beginning with the user perceptions of the comprehensiveness of policies A, B and C.

5.5.1 Comprehensiveness

Policy A published information on twenty-three personal data processing topics and this was the most out of the three policies that participants reviewed. Individuals felt that policy A was the most comprehensive of the three policies. Two individuals in FG1 felt that policy A provided the most information while a participant in FG2 stated that policy A would be “better for people who just sort of want to get the gist of it [data protection issues].” Individuals in FG3 and FG4 described policy A as “covering everything” and “telling you all the information you want” respectively. Some participants pointed out specific data protection topic areas that policy A mentioned that other statements had failed to discuss. An individual from FG4 pointed out:

> “Yeah but the others don’t say that they are not going to send it [personal data] to Europe. They don’t discuss it. That’s why policy A is full disclosure and it tells you exactly what is going to happen.”

Additionally, a person in FG2 commented:

> “I think it’s [policy A] good though where it says about payment transactions encrypted using that SSL technology. I don’t think the others stated that.”

Furthermore, a participant in FG3 felt that policy A described exactly what information would be collected and how it would be processed while an individual in FG5 pointed out that policy A included the contact details of somebody at the organisation should anyone wish to complain about personal data handling. Policy B published information on thirteen personal data processing topics and this was the least of the three policies reviewed. One individual in FG1 felt that “there were things missing from [policy] B” while a participant in FG4 stated that policy B “doesn’t really give full disclosure”. Similar points were also raised in FG5 with one participant noting:

> “It doesn’t really give you a lot of substance. It’s just kind of general statements that don’t really tell you a lot.”

Another individual in FG5 agreed and pointed out that “there is not really a lot there.” Additionally, a participant in FG2 said that policy B “left stuff out” while an individual from FG3 felt policy B was not very comprehensive. Focus group participants also picked out specific personal data handling practices areas that policy B did not mention. One individual from FG3 stated:

> “I mean it doesn’t say about security of your data. What they actually do. Like policy A states what they actually do about it. Doesn’t really say anything here.”

A participant in FG2 made a point about policy B not mentioning the transfer of personal data outside the EEA:

> “There is nothing about outsourcing it to places where the others have talked about the European economic area. There is nothing covered in this [policy] about that. I mean, you understand for things like shipping but why doesn’t this [policy] have that?”

Policy B stated that individuals have the right to obtain a copy of any personal data being processed by the organisation and to amend any inaccurate personal data however the policy made no reference as to how this could be done. One user in FG1 highlighted this point and felt that the policy should have provided some form of contact details to allow such a process to take place. This individual acknowledged that the policy did provide some form of contact details at the bottom of the page although he felt this would have been better placed immediately after the policy mentioned accessing and amending personal data. In addition, one individual in FG2 highlighted that policy B did not refer to personal data retention whereas policy C did.

In each focus group participants were asked how they perceived the organisation publishing each policy. Some individuals felt that the organisation publishing policy A had placed considerable resource in publishing a comprehensive privacy policy. One person in FG4 stated:

> “This [policy A] looks like it has been properly thought about and they have all the procedures in place. Yeah and it feels like it has covered all the bases. It looks like it has been a significant issue for them [the organisation] and they have covered it properly.”

The comprehensive nature of policy A led a participant in FG3 to believe that the organisation publishing the disclosure “knew what they were talking about” while an individual from FG2 thought that he could trust the company producing policy A more so than the business providing policy B. In comparison, one individual in FG5 felt that policy B gave the impression that the organisation publishing the policy were not particularly worried about personal data or privacy and therefore consumers need not to be concerned either. Additionally, participants in FG2 also stated:

> "They [the organisation publishing policy B] don't sound like a very legit company"

> "Do they [the organisation publishing policy B] really know what they are talking about?"

> "I wouldn't trust them [the organisation publishing policy B] because they don't sound like they know what they're doing."

Furthermore, a user in FG3 felt that he did not really have "much faith" in the company publishing policy B and this gave the impression that they "might not hold your data very securely."

5.5.2 Format

Individuals in FG2 and FG5 felt that policy A had a more professional look and feel compared to policy B and policy C. One user in FG2 described policy A as "more inviting" because it used bullet points while a participant in FG3 stated the that use of headings in policy A gave the disclosure "more structure." In contrast one individual in FG5 stated that the use of numbered statements in policy B "didn't really provide much structure" to the statement. This person subsequently described the organisation publishing policy B as unprofessional. In FG4 a participant also commented that it looked as if policy B had been "put together by someone on work experience".

One individual in FG1 felt that the use of headings and separate paragraphs in policy A allowed him to locate the information he wished to find with more ease compared to policy B and policy C. This participant stated:

> "If I wanted to know a certain thing in policy A about cookies I know exactly where I'm looking because it's got a big heading and it says, "IP addresses and cookies" and I can find the relevant information. It's easier to find the information on that one [policy A] than it is on B and C. Because looking at B, if I wanted to know information about cookies I have to read the entire policy to find the small bit there is on cookies whereas in policy A it's clearly set out and it's got separate areas for each bit. You know exactly where you're going to look for what type of information."

A similar view was expressed in FG5:

> "The other ones [policy A and policy C] are more like sub sectioned so if I wanted to look at what is collected from me I go here; if I wanted to look at the uses of my information I go here. Whereas this [policy B] you would really have to look through it if you were searching for something in particular."

Furthermore, this opinion was also evident in FG2; one user in this focus group described finding information using policy A as straightforward because the statement was "clearly set out and has got separate areas for each bit."

5.5.3 Terminology

The terminology used in the policies and extracts was the subject of discussion during the focus groups. Individuals paid attention to the Data Protection Act 1998, third party sharing recipients, the terms "may" and from "time to time" and personal data security.

5.5.3.1 Data Protection Act 1998

Policy A and policy C referred to the Data Protection Act 1998. Participants in FG3 and FG4 felt that mentioning the Data Protection Act 1998 provided a source of reassurance that personal data would be processed securely. One individual in FG3 stated that referring to the Data Protection Act 1998 "confirmed the professionalism" of the organisation responsible for handling personal data. Furthermore, in FG5 one individual stated that she placed more belief in the organisation processing personal data because they had cited the Data Protection Act 1998. Along with this, participants in FG2 and FG5 commented that the legislation increased their levels of trust in the company publishing the document. Users also felt that referring to the Data Protection Act 1998 suggested that the organisation producing the privacy policy was both aware of the legal requirements and would adhere to them. One person in FG5 stated:

> "If they reference it [the Data Protection Act 1998], it makes you think that they know what they are talking about as well"

5.5.3.2 Third Party Sharing Recipients

Extract A stated that personal information might be shared with an affiliated company called Offspring. Extract B stated that personal data may be shared with "associated companies within the Group and other carefully selected third party organisations outside the Group" while extract C mentioned that personal data might be shared with "with our partners, subsidiaries or subsidiary companies." Most participants in each focus group felt that extract A was the most effective of the three extracts at describing who personal data would be shared with because this statement had included the specific name of an organisation. Some individuals in FG4 and FG5 felt reassured that extract A stated that personal data would only be shared with one organisation however some participants in FG3 and FG4 noted that they did not know anything about the credentials of the company Offspring. That said, during FG2 it was noted that providing the specific name of an organisation offers users more flexibility to find out about more about what Offspring does.

Participants were critical of the terms used to describe who personal data would or might be shared with in extract B and extract C. Individuals questioned the companies that formed part of the group of companies mentioned in extract B (FG2 and FG4). One participant in FG1 stated:

> "[Extract] A did give you name of a company whereas the others [extract B and extract C] just say with "our partners" or a "third party" and you're like who is that? You haven't got a clue who the hell that is."

The terms used in extract B and extract C were described as "vague" (FG2), "grey" (FG4) and "meaningless" (FG4). These terms also gave some participants the impression that personal data would be shared with "any old organisation" (FG2) that offered the company the most money. In FG5 one person commented:

> "They [the organisation publishing extract B and C] don't really care about who uses the information, as long as they get paid for it."

Participants were asked how they felt about the use of the terms carefully selected third parties, companies within the group and partners and how they perceive the organisation publishing extract B and extract C considering these descriptions. Individuals in FG1, FG2, FG4 and FG5 responded with comments about the perceived trustworthiness and honesty of the organisations processing personal data:

> "It says they are trying to hide something. Otherwise they would have told us who they [the organisations] were." [FG1]

> “It doesn’t make you trust them at all. Especially when they say carefully selected. Could be anyone.” [FG2]

> “Carefully selected doesn’t necessarily give you piece of mind.” [FG4]

> “I probably don’t believe it but they have purposefully used that language to be reassuring to people that they think they can fool.” [FG5]

> “Who knows if it is a respectable company or not?” [FG5]

5.5.3.3 May and From Time to Time

Extract A, extract B and extract C stated that personal data “may” be shared for direct marketing purposes. Extract A also stated that personal data may be shared “from time to time”. Focus group participants were asked about their feelings towards these terms. During FG3 these terms were described as “grey” and “non-committal” while one research participant in FG4 described the terms as “wishy washy”. Additionally, individuals in FG1 and FG3 felt that the organisations that use the terms “may” and “from time to time” were “not being honest” and “not being up front” respectively. One person in FG3 stated that the same terms “don’t give you much trust” while a participant in FG1 thought the terms were unprofessional. Users in FG4 thought that even though policies only state that they may share personal data for direct marketing the likelihood is they will. Some users appear to feel that use of vague keywords such as may and from time to time are not transparent.

5.5.3.4 Security

The language used to describe the security practices in policy A was a discussion point for some individuals. Policy A stated:

> “We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy.”

> “All information you provide to us is stored on secure servers. Any payment transactions will be encrypted (using SSL technology). Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for

> keeping this password confidential. We ask you not to share a password with anyone.”

> “Unfortunately, the transmission of information via the internet is not completely secure. Athough (sic) we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk.”

One participant in FG1 felt that the use of the term “unfortunately” did not instil much confidence in the policy. Additionally, one user in FG2 picked out the wording “all steps reasonably necessary” and perceived this as being non-committal. This person questioned whether the organisation would put in place measures to protect the security of personal data. As well as this, one individual in FG4 described the terms “we will do our best” as “not acceptable” and felt that the organisation should “make sure” that personal data is secure. Finally, a participant in FG5 felt the use of the terms “at your own risk” was “worrying”.

5.5.4 Personal Data Processing Practices

The various attitudes towards personal data handling practices mentioned in the policies and extracts are discussed in this section beginning with perceptions about the subject of transferring personal data outside the EEA.

5.5.4.1 Transferring Personal Data Outside the EEA

Policy A mentioned that personal data might be transferred to a destination outside the EEA while policy C stated that consent would be obtained if personal data were to be transferred outside the EEA. Policy B made no mention of transferring personal data outside the EEA. One person in FG1 explained that she felt “that other people don’t really know” what transferring personal data outside the EEA is or what it means while during FG5 one individual felt that it was illegal to store personal data outside the EEA. In FG4 the transfer of personal data outside the EEA was described as “suspicious” and “sketchy” while one person in FG2 felt that this practice was not very reassuring. Individuals also questioned where personal data would be transferred to outside the EEA. One participant in FG4 stated:

> “If they have openly said it is going out of the European Economic Area it could end up in a third world country…”

In addition, someone in FG3 pointed out that transferring personal data outside the EEA meant that “it could go anywhere.” The governance of personal data outside the EEA was also questioned. An individual in FG3 pointed out:

> “Because obviously sending it [personal data] out of the European area…the EEA…you don’t know what their regulations are with data protection; they could be different to ours.”

A similar point was made in FG4:

> “If it goes outside of the European Economic Area, does that mean that things are still governed?”

5.5.4.2 Subject Access Request Charges

The DPA 1998 stipulates that data controllers can charge £10 to offset any costs associated with complying with a subject access request. Policy A stated that individuals would not be charged to access a copy of any personal data being processed; policy B made no mention of any charge and policy C stated that the organisation is entitled to charge individuals £10 to comply with the DPA 1998. Individuals in FG2 agreed that they did not appreciate having to pay to obtain a copy of personal data while one participant in FG4 described the subject access request charge as “a cheek”. In addition to this one individual in FG3 felt that an organisation charging for access to personal data implied that they owned the data and could therefore sell it on. This individual went on to state that he felt that any personal data being processed about him belonged to him and therefore he should be entitled to it free of charge.

5.5.4.3 Choice

Policy A and policy C mentioned that consent would be obtained prior to the organisation carrying out direct marketing or sharing personal data with a third party for direct marketing. Policy C also mentioned that consent would be obtained should personal data be transferred outside the EEA while policy A stated that personal data might be stored outside the EEA but did not mention user consent. Policy B did not state that consent would be obtained prior to sending consumers direct marketing material or sharing personal data with third parties for marketing. In addition, policy B and policy C provided a mechanism to opt out of personal data being used for direct marketing or being shared with third party marketing organisations.

A participant in FG1 thought that the approach taken by policy A to offer users the choice to opt in to personal data being used for direct marketing was more convenient than the opt out strategy taken by policy B. Furthermore, the default opt in protocol adopted by policy A was considered as “the way it should be” (FG3) while the practice of obtaining consent prior to transferring personal data outside the EEA was described as “quite a good thing” (FG*4).*

Two individuals in FG2 agreed that it was “nice” that policy C stated that users would not be contacted in the future about products or services offered by the organisation without consent. One individual in FG1 felt reassured that policy C would not use personal data to send marketing communications or share personal data with a third party without consent while an individual from FG5 stated that he would feel more comfortable disclosing personal data to the organisation publishing policy C because consent is obtained prior to processing.

Policy B did not state that consent would be obtained prior to personal data being used for direct marketing or shared with third party marketing organisations and this gave some participants in FG1, FG2 and FG3 the impression that personal data would be used by default for those purposes. These individuals felt frustrated that the onus was then placed on them to contact the organisation to opt out of personal data being processed.

5.6 Summary

This chapter presented the results of five focus groups with e-commerce users. The purpose of the focus groups was to address research questions two and three. Research question two was: **why do e-commerce users ignore UK e-commerce privacy policies?** Privacy policies are synonymous with “that tick box” and “the small print” and the findings evidence the existence of several barriers to reading privacy policies. E-commerce is associated with quick transactions and some individuals feel that privacy policies erode the convenient aspect of purchasing goods and services online. Some users do not expect to understand privacy policies and focus group findings suggested that parts of these policies are confusing. Policy length and the format of policies also prevents users from reading policies. Furthermore, many users feel that they have no choice but to accept the personal data handling practices of organisations. Evidence suggested that some consumers also felt that privacy policies serve to benefit organisations and not consumers. Along with this, some individuals are just not that concerned about the personal data processing and therefore do not read privacy policies.

Research question three was: **what do e-commerce users feel are the positive and negative characteristics of UK e-commerce privacy policies?** After reviewing three different privacy policies some users felt that the organisation that published the policy with the most personal data processing topics was more competent and trustworthy. On the other hand, the organisation publishing the policy that disclosed the least personal data processing information topics was considered by some as lacking legitimacy and competency. Findings also suggested that information retrieval was easier where policies used clearly separated paragraphs and headings as opposed to numbered statements.

Mentioning the Personal Data Protection Act 1998 was viewed positively by users and was associated with perceived trust and compliance. Users also supported statements that asked for consent before personal data is processed. E-commerce users perceived some of the third-party data sharing descriptions found in phase one as grey and meaningless. Such descriptions were associated with a lack of trust. The transfer of personal data outside of the EEA was viewed with caution by some individuals. The governance of personal data processed outside the EEA was questioned by users. There was a dislike for subject access request charges.

Chapter 6 - Phase Three: Policy Design

6.1 Introduction

In phase three a prototype privacy policy was designed. This chapter outlines the process and factors considered when designing the prototype. Figure 6.1 provides an overview of the different research phases in this study showing how phase three fits in with the overall research design.

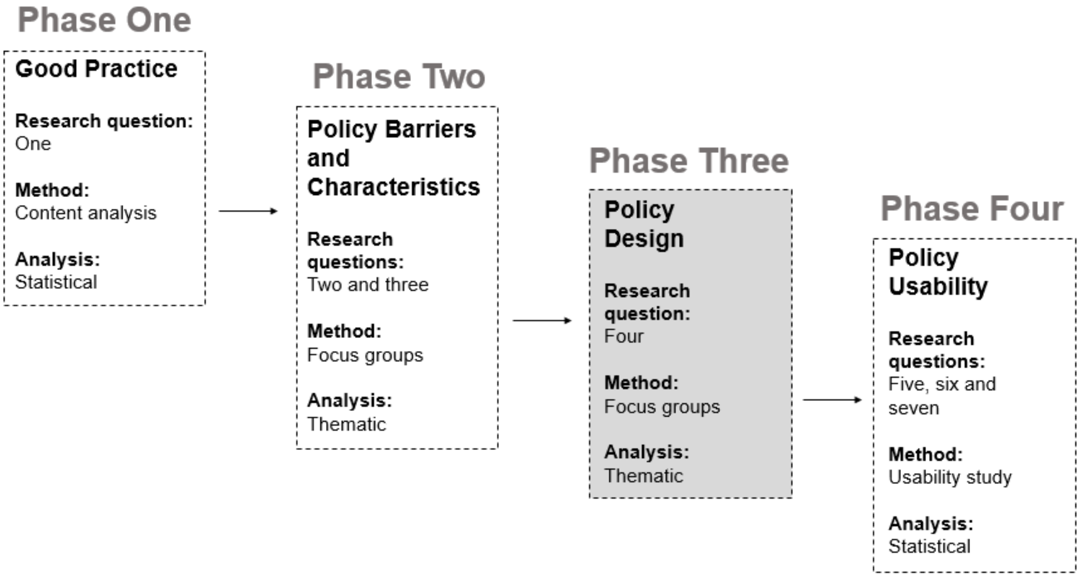


Figure 6.1 - Research design

6.2 Policy Design Justification

In the Privacy Notices Code of Practice published in 2010 (Information Commissioner 2010), the Information Commissioner recommended that organisations implement layered privacy policies. The publication of layered privacy policies is still recommended as current good practice by the Information Commissioner (Information Commissioner's Office, 2018c) and the Article 29 Working Party (2018b). However, at the time of carrying out the research phase, the ICO published little guidance to help organisations to publish a layered notice. In addition, there is some evidence to suggest that organisations support more prescriptive guidance. In 2016, the ICO asked organisations to provide feedback on the privacy notices code of practice that was being developed to help organisations comply with the requirements of the GDPR

(Information Commissioners Office, 2016b). Findings from the consultation (Information Commissioners Office 2016b, p. 2) stated: "the code should make clear which information should go into which layer of a layered privacy notice." With these points in mind, the development of a prototype layered privacy policy was suitable both in the context of this research and the broader personal data processing environment.

6.3 Integration of Findings from Research Phase Two

Phase two examined user attitudes towards UK e-commerce privacy policies. At the outset of phase four, some of the key findings from phase two were translated into five prototype design objectives. These are outlined in table 6.1. The prototype objectives underpinned the design decisions taken during the development of the prototype. Figure 6.2 outlines the five-stage prototype design process. The prototype design was evaluated by the researcher and e-commerce users. Findings from these evaluations supported the subsequent prototype design iterations. The remainder of this chapter outlines the development of the prototype privacy policy.

	Phase two finding	Associated prototype design objective
1	First impressions are important. Policy length can influence desire to read and perceived readability.	The prototype should not be perceived as a long document. Users do not want to open a privacy policy and be presented with numerous paragraphs of text.
2	The format of a policy can influence perceptions of information retrieval. Users reported that the use of clearly labelled headings and bullet points helped when locating information.	The prototype design should allow consumers to feel that they can locate and retrieve information easily and quickly.
3	Following best practice and communicating other personal information processing topics can be associated with perceived trust, perceived competence and perceived compliance.	The prototype design should follow with best practice guidelines.

4	Some users feel reassured that policies state that consent is obtained before personal data is shared or processed.	The prototype design should mention that consent is obtained prior to processing.
5	Some users perceive policies that state compliance with the Data Protection Act 1998 to be more trustworthy and competent.	The prototype design should refer to the relevant legislation.

Table 6.1 - Phase two findings and associated prototype design objectives

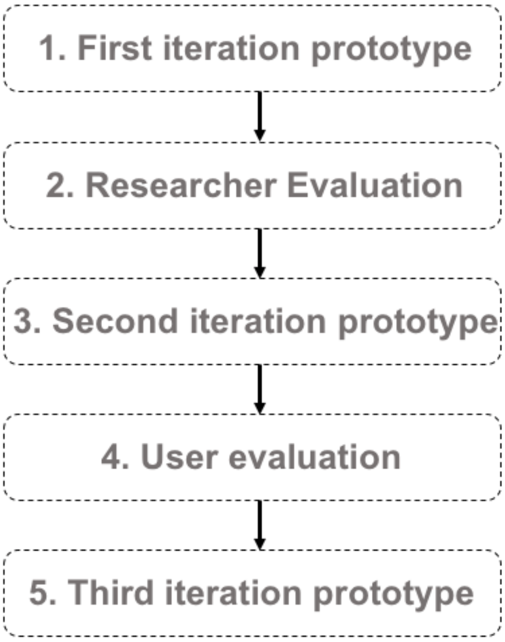

1. First iteration prototype
2. Researcher Evaluation
3. Second iteration prototype
4. User evaluation
5. Third iteration prototype

Figure 6.2 - Prototype design process

6.4 First Iteration Prototype

The first iteration prototype was an initial attempt to satisfy the prototype design objectives. The next two sections describe salient components of the first iteration. The design of the summary layer was focus during the first iteration.

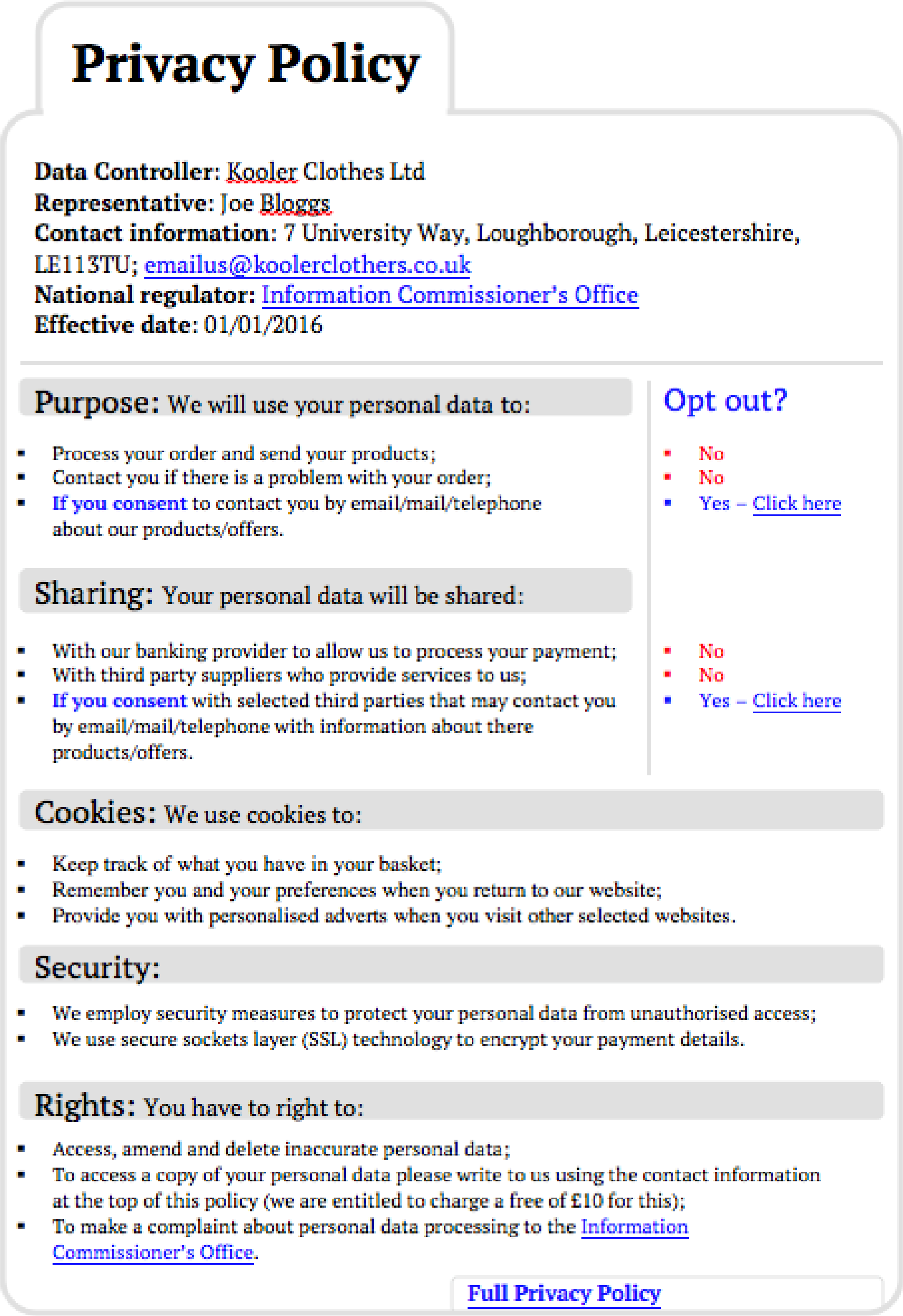
6.4.1 Format

A header section is provided at the very top of the summary layer. This provides objective policy information. Headings were used to divide summary layer content. Each heading was placed inside a grey rectangular container that spanned the width of the page. Content was presented below each heading. Based on the findings from phase two bullet points were used to communicate policy information. An opt out menu indicator was displayed on the right-hand side of the purpose and sharing sections. This informs users whether they can opt out of specified uses of personal data. A link is provided to give users some guidance as to how they can opt out where applicable.

6.4.2 Content

Six categories of information were provided in the first iteration prototype, namely: header information (including data controller identity, representative, address, national regulator and an effective date), purpose for processing, sharing, cookies, security and rights. Short, objective policy information was presented in the summary layer.

Two prominent personal data processing concerns are the sharing of personal data and unauthorised access to personal data. For that reason, these two categories were included in the summary layer. The Data Protection Act 1998 and the GDPR state that data controllers should notify users of the purpose or purposes for which personal data is processed. Furthermore, the Privacy and Electronic Communications Act 2003 states that organisations should provide clear and comprehensive information to users regarding the purpose or purposes for which cookies (and other similar technologies) are used. These two categories were also included within the summary layer. Finally, a data rights category was included in the summary layer.



Privacy Policy

Data Controller: Kooler Clothes Ltd
Representative: Joe Bloggs
Contact information: 7 University Way, Loughborough, Leicestershire, LE113TU; emailus@koolerclothers.co.uk
National regulator: Information Commissioner's Office
Effective date: 01/01/2016

Purpose: We will use your personal data to:	Opt out?
Process your order and send your products;	No
Contact you if there is a problem with your order;	No
If you consent to contact you by email/mail/telephone about our products/offers.	Yes – Click here
Sharing: Your personal data will be shared:	
With our banking provider to allow us to process your payment;	No
With third party suppliers who provide services to us;	No
If you consent with selected third parties that may contact you by email/mail/telephone with information about there products/offers.	Yes – Click here

Cookies: We use cookies to:

- Keep track of what you have in your basket;
- Remember you and your preferences when you return to our website;
- Provide you with personalised adverts when you visit other selected websites.

Security:

- We employ security measures to protect your personal data from unauthorised access;
- We use secure sockets layer (SSL) technology to encrypt your payment details.

Rights: You have to right to:

- Access, amend and delete inaccurate personal data;
- To access a copy of your personal data please write to us using the contact information at the top of this policy (we are entitled to charge a free of £10 for this);
- To make a complaint about personal data processing to the Information Commissioner's Office.

Full Privacy Policy

Figure 6.3 - First iteration prototype summary layer

6.5 Researcher Evaluation

The researcher evaluated the first iteration prototype summary layer. On reflection, the researcher felt that there were several drawbacks of the first iteration design. These were:

1. The link to the full layer was placed in the bottom right hand side of the summary layer. This would be better placed towards the top of the summary layer where users would not have to scroll down the page to access the link. McDonald et al (2009) found that some users did not click through to the full privacy policy. Placing the link in a more noticeable area at the top of the privacy policy would improve the probability of users seeing the link;

2. There was no explicit mention within the summary layer that it was a summary of the privacy policy. Including some form of label indicating that this page was a summary would be beneficial;

3. There was no clear separation between the different sections of the summary. Placing containers around each section like that in the Kleinmann Communication Group (2006) design would provide clear separation between each policy section.

4. It could be confusing for users to understand which opt out bullet points relate to which sharing bullet point. A tabular design like the privacy nutrition label (Kelley et al 2009) and the Kleinmann Communication Group (2006) policy for that section would provide less confusion.

6.6 Second Iteration Prototype

The second iteration prototype was developed using HTML (Hypertext mark-up language) and CSS (Cascading stylesheets). The summary layer along with the full privacy and full cookie policy layer were included in the second iteration design. These designs are shown in figure 6.4, figure 6.5 and figure 6.6. The logo of a fictitious organisation selling footwear products was added to the prototype design along with header and footer information to give the impression that the policy was part of a live e-commerce website. Changes to the layout of the summary layer based on the researcher evaluation were:

1. Containers were placed around content to provide clear separation. This addressed point three of the first iteration limitations.

2. Inspired by the paper-based layout in Kleinmann Communication Group (2006) and the finding that more time is spent looking at the left-hand side of a webpage (Nielsen, 2010; Fessenden, 2017), headings for each section were placed inside containers and positioned towards the left-hand side of the page. This provided a cleaner look and feel. It was envisioned that the user would view these containers as a menu or a first place to begin information seeking.

3. A marketing section was added. This section and the sharing sections were redesigned using a table format. This removes the potential confusion around opt out bullet points made in point four of the first iteration drawbacks. The use of white space around the column indicating whether users can opt out is less cluttered.

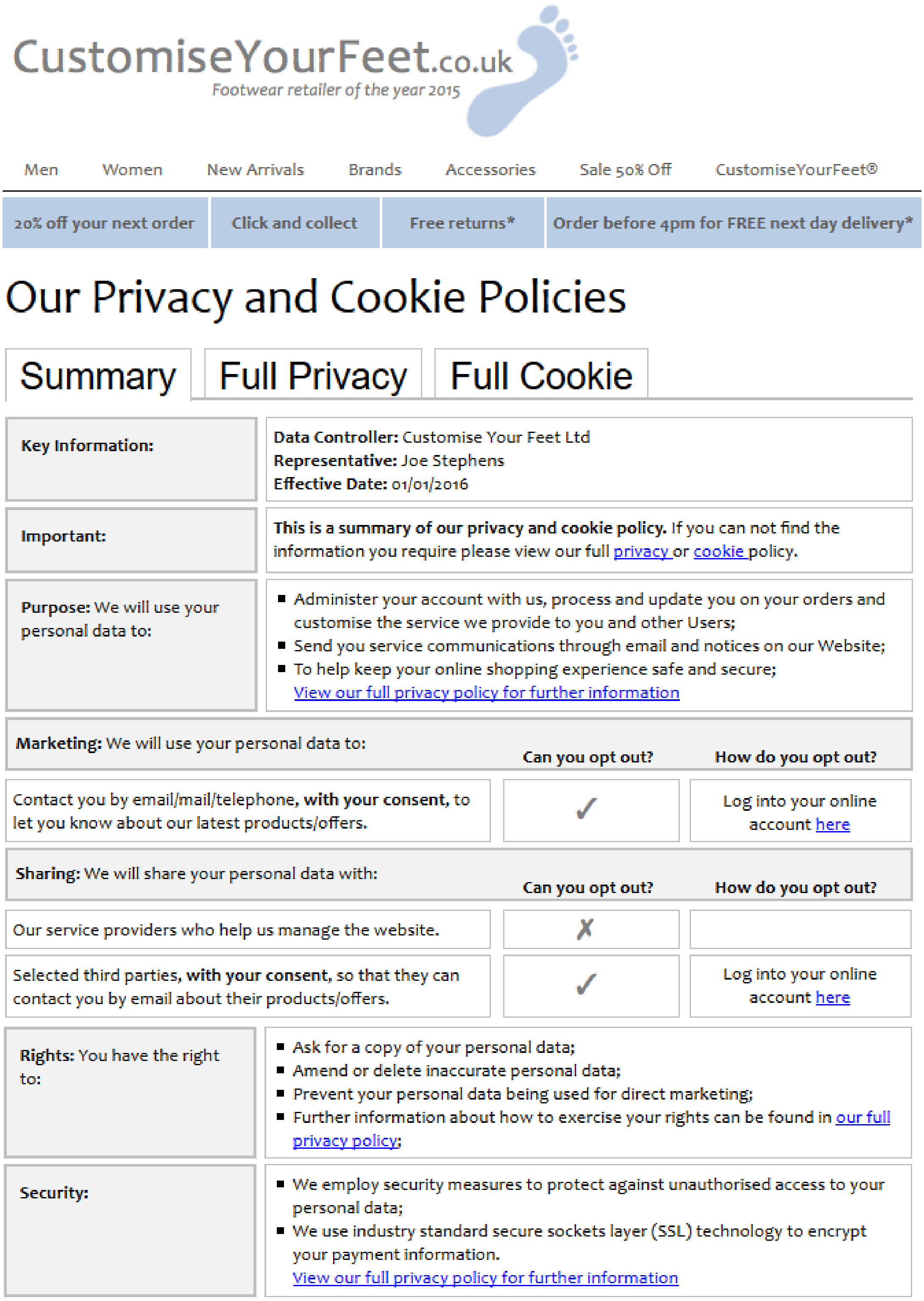
4. The privacy policy title in the first iteration design was replaced with a summary tab, a full privacy tab and a full cookie tab. The current tab that the user has open does not have a line break between the main link and the rest of the policy information allowing the user to easily recognise which tab is currently selected. In this respect, the user should know whether they are looking at the summary or the full policy.

5. A section was added under the key information section at the top of the summary clearly stating that the summary is only a summary and further information can be found within the full privacy policy. This addressed point two of the first iteration limitations.

6. A link to the full privacy policy was included within each information section. This addressed point one of the first iteration disadvantages.

7. The contact details and national regulator were removed from the key information section at the top of the summary.

8. A questions section was added at the bottom of the of the summary. The contact details of the data controller and the ICO were added to this section.



CustomiseYourFeet.co.uk

Footwear retailer of the year 2015

Men Women New Arrivals Brands Accessories Sale 50% Off CustomiseYourFeet®

20% off your next order | Click and collect | Free returns* | Order before 4pm for FREE next day delivery*

Our Privacy and Cookie Policies

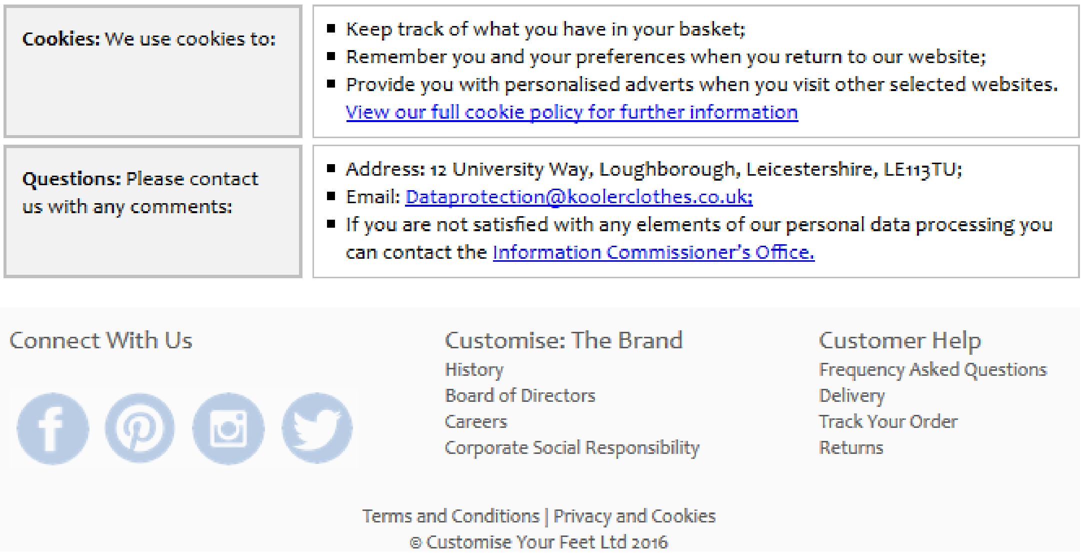
Summary | Full Privacy | Full Cookie

Key Information:	**Data Controller:** Customise Your Feet Ltd **Representative:** Joe Stephens **Effective Date:** 01/01/2016
Important:	**This is a summary of our privacy and cookie policy.** If you can not find the information you require please view our full privacy or cookie policy.
Purpose: We will use your personal data to:	▪ Administer your account with us, process and update you on your orders and customise the service we provide to you and other Users; ▪ Send you service communications through email and notices on our Website; ▪ To help keep your online shopping experience safe and secure; View our full privacy policy for further information

Marketing: We will use your personal data to:	**Can you opt out?**	**How do you opt out?**
Contact you by email/mail/telephone, **with your consent**, to let you know about our latest products/offers.	✓	Log into your online account here

Sharing: We will share your personal data with:	**Can you opt out?**	**How do you opt out?**
Our service providers who help us manage the website.	✗	
Selected third parties, **with your consent**, so that they can contact you by email about their products/offers.	✓	Log into your online account here

Rights: You have the right to:	▪ Ask for a copy of your personal data; ▪ Amend or delete inaccurate personal data; ▪ Prevent your personal data being used for direct marketing; ▪ Further information about how to exercise your rights can be found in our full privacy policy;
Security:	▪ We employ security measures to protect against unauthorised access to your personal data; ▪ We use industry standard secure sockets layer (SSL) technology to encrypt your payment information. View our full privacy policy for further information



Cookies: We use cookies to:	▪ Keep track of what you have in your basket; ▪ Remember you and your preferences when you return to our website; ▪ Provide you with personalised adverts when you visit other selected websites. View our full cookie policy for further information
Questions: Please contact us with any comments:	▪ Address: 12 University Way, Loughborough, Leicestershire, LE113TU; ▪ Email: Dataprotection@koolerclothes.co.uk; ▪ If you are not satisfied with any elements of our personal data processing you can contact the Information Commissioner's Office.

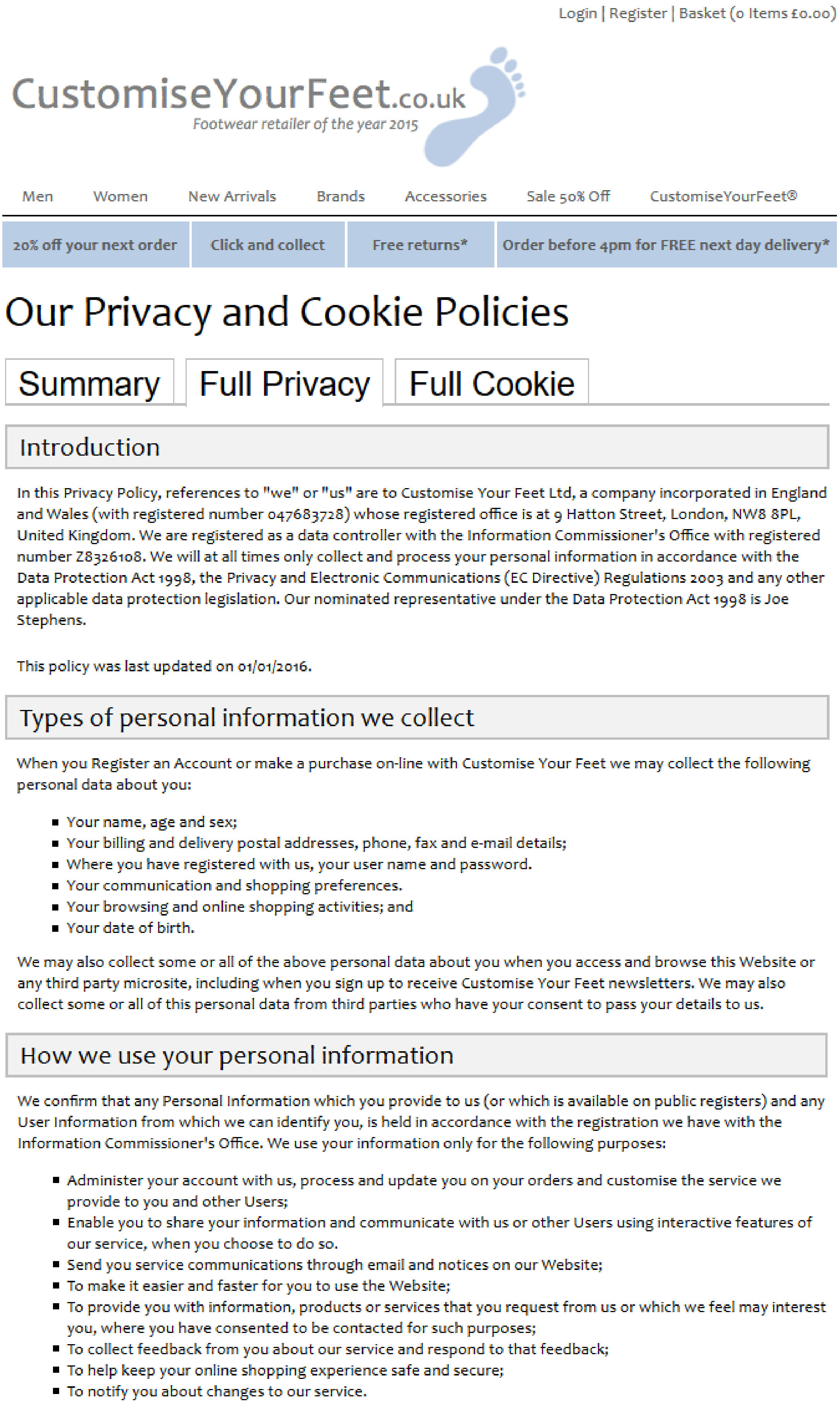
Connect With Us

Customise: The Brand
History
Board of Directors
Careers
Corporate Social Responsibility

Customer Help
Frequency Asked Questions
Delivery
Track Your Order
Returns

Terms and Conditions | Privacy and Cookies
© Customise Your Feet Ltd 2016

Figure 6.4 - Second iteration prototype summary layer



Our Privacy and Cookie Policies

Introduction

In this Privacy Policy, references to "we" or "us" are to Customise Your Feet Ltd, a company incorporated in England and Wales (with registered number 047683728) whose registered office is at 9 Hatton Street, London, NW8 8PL, United Kingdom. We are registered as a data controller with the Information Commissioner's Office with registered number Z8326108. We will at all times only collect and process your personal information in accordance with the Data Protection Act 1998, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any other applicable data protection legislation. Our nominated representative under the Data Protection Act 1998 is Joe Stephens.

This policy was last updated on 01/01/2016.

Types of personal information we collect

When you Register an Account or make a purchase on-line with Customise Your Feet we may collect the following personal data about you:

- Your name, age and sex;
- Your billing and delivery postal addresses, phone, fax and e-mail details;
- Where you have registered with us, your user name and password.
- Your communication and shopping preferences.
- Your browsing and online shopping activities; and
- Your date of birth.

We may also collect some or all of the above personal data about you when you access and browse this Website or any third party microsite, including when you sign up to receive Customise Your Feet newsletters. We may also collect some or all of this personal data from third parties who have your consent to pass your details to us.

How we use your personal information

We confirm that any Personal Information which you provide to us (or which is available on public registers) and any User Information from which we can identify you, is held in accordance with the registration we have with the Information Commissioner's Office. We use your information only for the following purposes:

- Administer your account with us, process and update you on your orders and customise the service we provide to you and other Users;
- Enable you to share your information and communicate with us or other Users using interactive features of our service, when you choose to do so.
- Send you service communications through email and notices on our Website;
- To make it easier and faster for you to use the Website;
- To provide you with information, products or services that you request from us or which we feel may interest you, where you have consented to be contacted for such purposes;
- To collect feedback from you about our service and respond to that feedback;
- To help keep your online shopping experience safe and secure;
- To notify you about changes to our service.

Sharing your personal information

If you are a new customer, and where we permit selected third parties to use your data, we (or they) will contact you by electronic means only if you have consented to this. If you do not want us to use your data in this way, or to pass your details on to third parties for marketing purposes, please tick the relevant box situated on the form on which we collect your data.

We may contract with third party companies, sub-contractors, service providers, agents or other persons to provide certain services including credit card processing, shipping, data management, web development, promotional services, etc (”Service Providers”). We call them our Service Providers and we shall be entitled to provide our Service Providers with the information needed for them to perform these services. We also ask our Service Providers to confirm that their privacy practices are consistent with ours.

We may also disclose your personal information to third parties:

- Who are a member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.
- In the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets.
- If we or substantially all of our assets are acquired by a third party, in which case personal data held by us about our customers will be one of the transferred assets.

Storage of your personal information

The Personal Information that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff maybe engaged in, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. By submitting your Personal Information, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your Personal Information, we cannot guarantee the security of your information transmitted to our Website; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Your rights

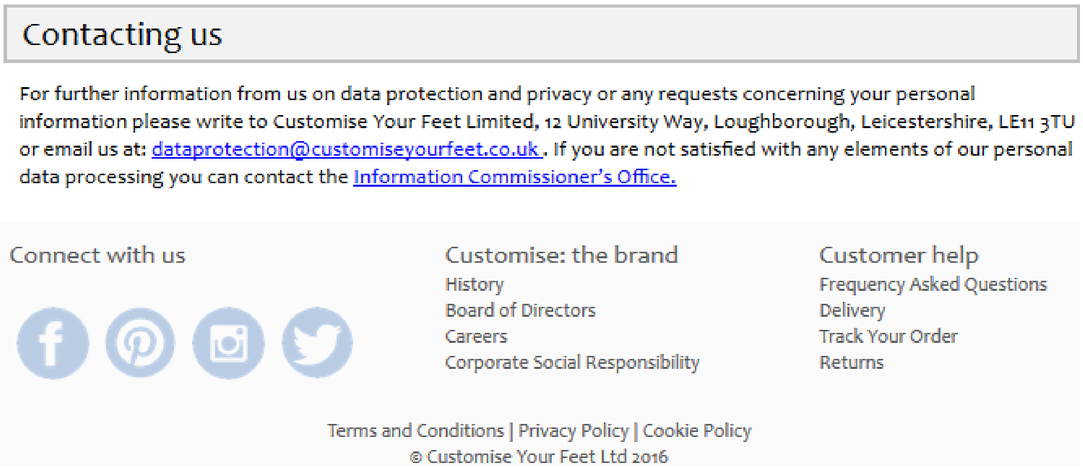
You have the following rights:

- the right to ask what personal data that we hold about you at any time, subject to a fee specified by law (currently £10);
- the right to ask us to update and correct any out-of-date or incorrect personal data that we hold about you free of charge; and
- the right to opt out of any marketing communications that we may send you.

If you wish to exercise any of the above rights, please contact us using the contact details specified below. However, if you wish to unsubscribe from e-mail marketing communications that we send you, you can easily do this by clicking on the unsubscribe link at the bottom of any e-mail newsletter we have sent to you. You can also amend any personal information you submitted when you registered with us by viewing your online account.

Security

We use Internet standard encryption technology ("SSL" or "Secure Socket Layer" technology) to encode personal data that you send to us when placing an order through the Website. To check that you are in a secure area of the Website before sending personal data to us, please look at the URL bar to check that it displays an image of a closed padlock and the text should show https. However, please note that whilst we take appropriate technical and organisational measures to safeguard the personal data that you provide to us, no transmission over the Internet can ever be guaranteed secure. Consequently, please note that we cannot guarantee the security of any personal data that you transfer over the Internet to us.

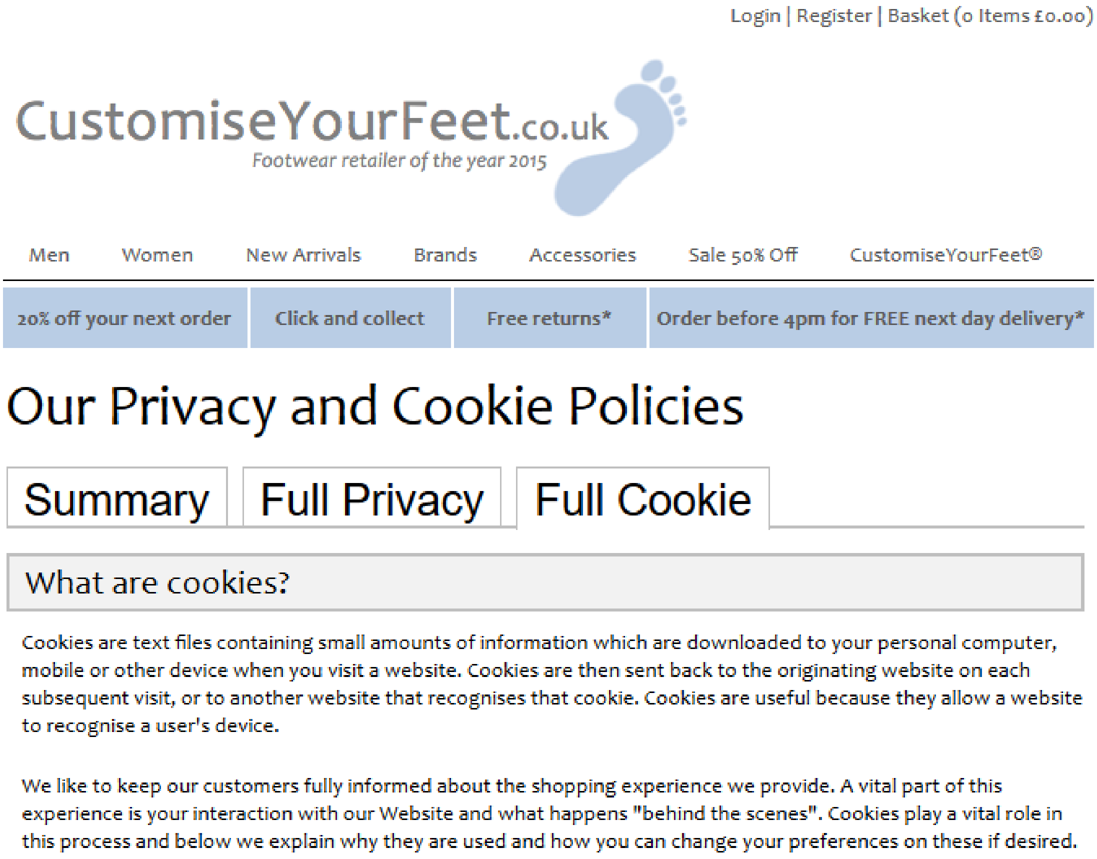


Contacting us

For further information from us on data protection and privacy or any requests concerning your personal information please write to Customise Your Feet Limited, 12 University Way, Loughborough, Leicestershire, LE11 3TU or email us at: dataprotection@customiseyourfeet.co.uk . If you are not satisfied with any elements of our personal data processing you can contact the Information Commissioner's Office.

Connect with us
Customise: the brand
History
Board of Directors
Careers
Corporate Social Responsibility
Customer help
Frequency Asked Questions
Delivery
Track Your Order
Returns
Terms and Conditions | Privacy Policy | Cookie Policy
© Customise Your Feet Ltd 2016

Figure 6.5 – Second iteration prototype full privacy policy

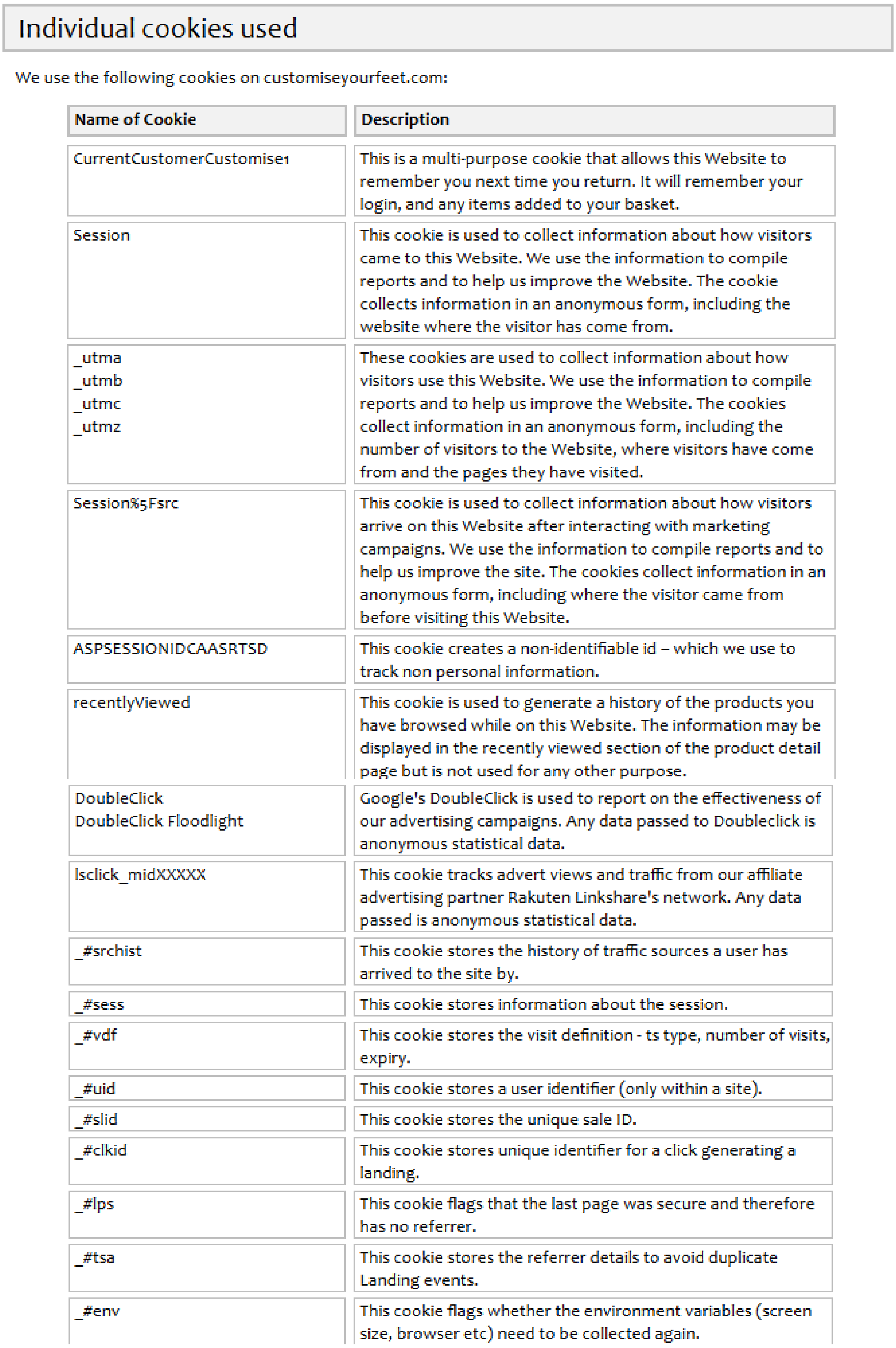


Our Privacy and Cookie Policies

What are cookies?

Cookies are text files containing small amounts of information which are downloaded to your personal computer, mobile or other device when you visit a website. Cookies are then sent back to the originating website on each subsequent visit, or to another website that recognises that cookie. Cookies are useful because they allow a website to recognise a user's device.

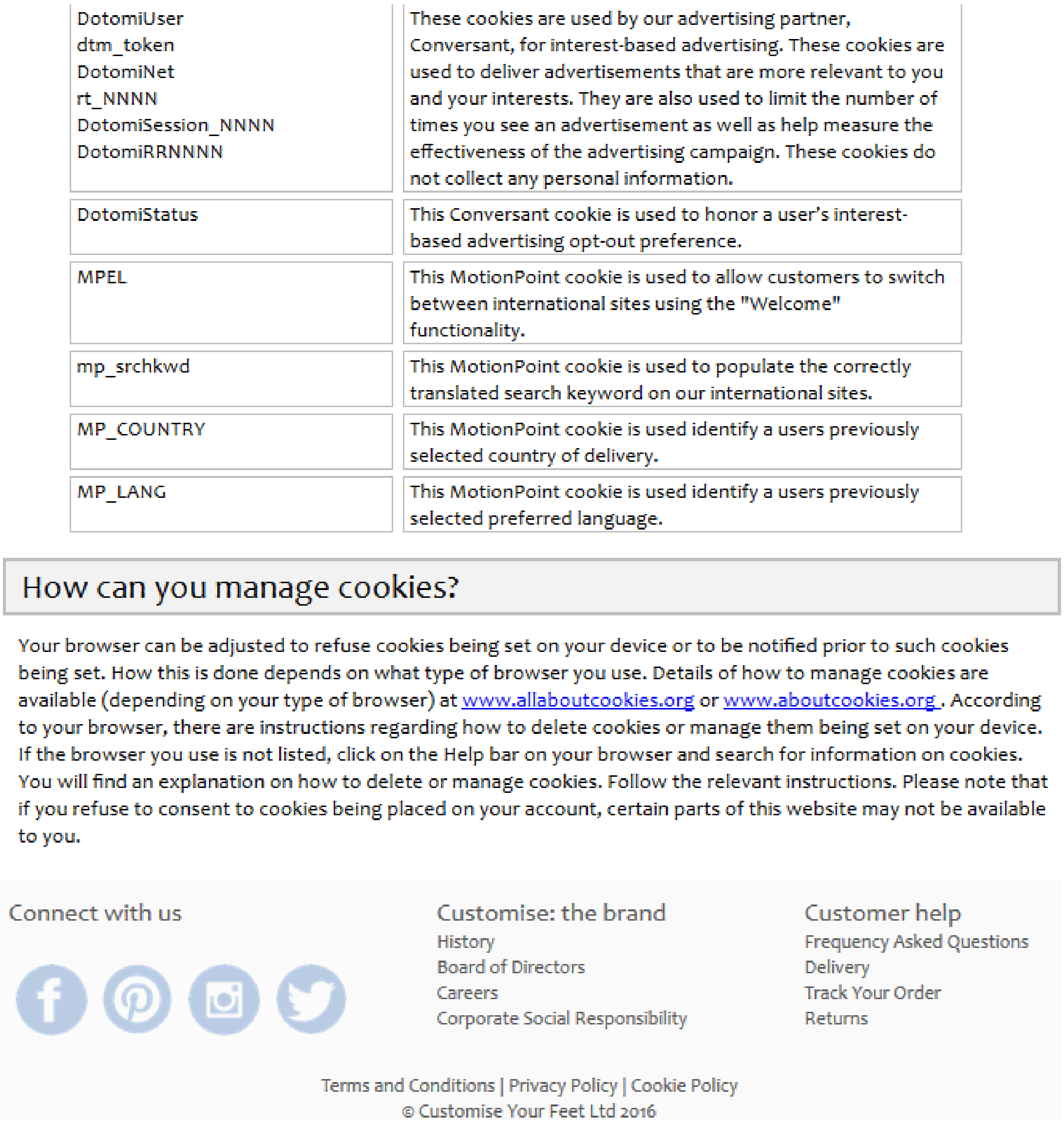
We like to keep our customers fully informed about the shopping experience we provide. A vital part of this experience is your interaction with our Website and what happens "behind the scenes". Cookies play a vital role in this process and below we explain why they are used and how you can change your preferences on these if desired.



Individual cookies used

We use the following cookies on customiseyourfeet.com:

Name of Cookie	Description
CurrentCustomerCustomise1	This is a multi-purpose cookie that allows this Website to remember you next time you return. It will remember your login, and any items added to your basket.
Session	This cookie is used to collect information about how visitors came to this Website. We use the information to compile reports and to help us improve the Website. The cookie collects information in an anonymous form, including the website where the visitor has come from.
_utma _utmb _utmc _utmz	These cookies are used to collect information about how visitors use this Website. We use the information to compile reports and to help us improve the Website. The cookies collect information in an anonymous form, including the number of visitors to the Website, where visitors have come from and the pages they have visited.
Session%5Fsrc	This cookie is used to collect information about how visitors arrive on this Website after interacting with marketing campaigns. We use the information to compile reports and to help us improve the site. The cookies collect information in an anonymous form, including where the visitor came from before visiting this Website.
ASPSESSIONIDCAASRTSD	This cookie creates a non-identifiable id – which we use to track non personal information.
recentlyViewed	This cookie is used to generate a history of the products you have browsed while on this Website. The information may be displayed in the recently viewed section of the product detail page but is not used for any other purpose.
DoubleClick DoubleClick Floodlight	Google's DoubleClick is used to report on the effectiveness of our advertising campaigns. Any data passed to Doubleclick is anonymous statistical data.
lsclick_midXXXXX	This cookie tracks advert views and traffic from our affiliate advertising partner Rakuten Linkshare's network. Any data passed is anonymous statistical data.
_#srchist	This cookie stores the history of traffic sources a user has arrived to the site by.
_#sess	This cookie stores information about the session.
_#vdf	This cookie stores the visit definition - ts type, number of visits, expiry.
_#uid	This cookie stores a user identifier (only within a site).
_#slid	This cookie stores the unique sale ID.
_#clkid	This cookie stores unique identifier for a click generating a landing.
_#lps	This cookie flags that the last page was secure and therefore has no referrer.
_#tsa	This cookie stores the referrer details to avoid duplicate Landing events.
_#env	This cookie flags whether the environment variables (screen size, browser etc) need to be collected again.



DotomiUser dtm_token DotomiNet rt_NNNN DotomiSession_NNNN DotomiRRNNNN	These cookies are used by our advertising partner, Conversant, for interest-based advertising. These cookies are used to deliver advertisements that are more relevant to you and your interests. They are also used to limit the number of times you see an advertisement as well as help measure the effectiveness of the advertising campaign. These cookies do not collect any personal information.
DotomiStatus	This Conversant cookie is used to honor a user's interest-based advertising opt-out preference.
MPEL	This MotionPoint cookie is used to allow customers to switch between international sites using the "Welcome" functionality.
mp_srchkwd	This MotionPoint cookie is used to populate the correctly translated search keyword on our international sites.
MP_COUNTRY	This MotionPoint cookie is used identify a users previously selected country of delivery.
MP_LANG	This MotionPoint cookie is used identify a users previously selected preferred language.

How can you manage cookies?

Your browser can be adjusted to refuse cookies being set on your device or to be notified prior to such cookies being set. How this is done depends on what type of browser you use. Details of how to manage cookies are available (depending on your type of browser) at www.allaboutcookies.org or www.aboutcookies.org . According to your browser, there are instructions regarding how to delete cookies or manage them being set on your device. If the browser you use is not listed, click on the Help bar on your browser and search for information on cookies. You will find an explanation on how to delete or manage cookies. Follow the relevant instructions. Please note that if you refuse to consent to cookies being placed on your account, certain parts of this website may not be available to you.

Connect with us

Customise: the brand
History
Board of Directors
Careers
Corporate Social Responsibility

Customer help
Frequency Asked Questions
Delivery
Track Your Order
Returns

Terms and Conditions | Privacy Policy | Cookie Policy
© Customise Your Feet Ltd 2016

Figure 6.6 - Second iteration prototype full cookie policy

6.7 User Evaluation

The user evaluation addressed research question four. Research question four was: **how useful is the standardised prototype?** Two focus groups were carried out to address research question four. The demographic characteristics of each focus group are presented in section 3.6 of the methodology chapter. A moderator's guide outlining focus group questions is presented in table 3.7 of the methodology chapter.

In each focus group participants were shown four privacy policies. One was the standardised prototype. The remaining three were the privacy policies of Argos.co.uk, Tesco.co.uk and Tkmaxx.com. These policies were chosen because of their different formats. The Argos privacy policy used links presented at the top of the page to allow users to navigate to content displayed within the privacy policy. The Tesco privacy policy displayed text within containers. The Tkmaxx privacy policy used accordion controls to present policy information. Participants explored these privacy policies during the focus group.

The themes that emerged from the focus group discussions are presented below. The findings are split into three themes. Section 6.6.1 discusses user responses to the categories of information within the summary layer. Section 6.6.2 outlines how users felt about the layout of the summary layer. Finally, section 6.6.3 describes privacy policy improvements. Focus groups are referred to throughout by the designation FG followed by a number. The terms users and consumers are used interchangeably to refer to focus group participants.

6.7.1 Summary Layer Categories of Information

At the beginning of the focus group, users were not shown the summary layer. Participants were asked to read the full privacy and cookie layers and note down any information that was new to them or that they had not come across before. Users were asked this question on the assumption that to be informative the summary layer should communicate information that users (a) want to know and (b) do not already know.

Findings showed that some users had little awareness of cookies. Two individuals in FG1 said they did not realise what cookies were. Furthermore, someone in FG2 stated:

> “There are just so many different [cookie] codes…there are loads of different ones. And the fact that if you disable those cookies then it doesn’t let you on the website.”

Participants in both focus groups were unaware about the processing of personal data outside the EEA. In FG2 one individual commented that he felt uncomfortable about information being transported “anywhere in the world” while two participants stated that they were surprised that personal data was transferred outside the EEA. In FG1 one user said he was “shocked” that personal data was transferred outside the EEA while another user said:

> “I suppose that it is something I have never thought about before. You just go online and buy something because it saves you going to the shop. But actually, there is a lot more that goes on behind the scenes that you do not think of.”

After discussing policy information that was new to users, participants were asked to read the summary layer. Users were asked whether the categories of information included within the summary layer were useful based on the comments and notes they had made about policy information they had not come across before.

Four individuals in FG1 felt that the transfer of personal data outside the EEA should be added to the summary layer. One user felt that that it was “not common sense” to know that personal data would be processed outside the EEA. Three other participants in FG1 agreed that this category of information would be a useful addition to the summary layer. One individual stated that he would want to know about processing outside the EEA “because it’s not just used in this country is it?”

6.7.2 Summary Page Layout

Participants were asked to evaluate the effectiveness of the summary layer format. In FG1 one person described the summary layer was “really useful” because it was “easy to pick up information quickly.” One individual in FG1 felt that the layered format was:

> "…massively useful because you are just bullet pointing the main points because not everyone has the time or can be bothered to read the full privacy policy. If there is something that does intrigue them then they can go in and read the full policy."

Importantly, participants in FG2 demonstrated that they understood the purpose of publishing a summary layer. One individual stated:

> "You go through the summary, click on your full policy and then say, I want to know something else about marketing which is not expanded upon in the summary. It is there; straight in front of you in the summary. You just click it and there is your information. You have not got to scroll through pages to find like an underlined heading that says marketing or something like that. It's straight there. It is very user friendly."

Another individual in the same focus group agreed. This person described the prototype design as: "easy to read…because you haven't got those headings and you don't have to trawl through them." Additionally, one user felt the summary page "flowed well" while another participant commented that it was easy to "pick up information".

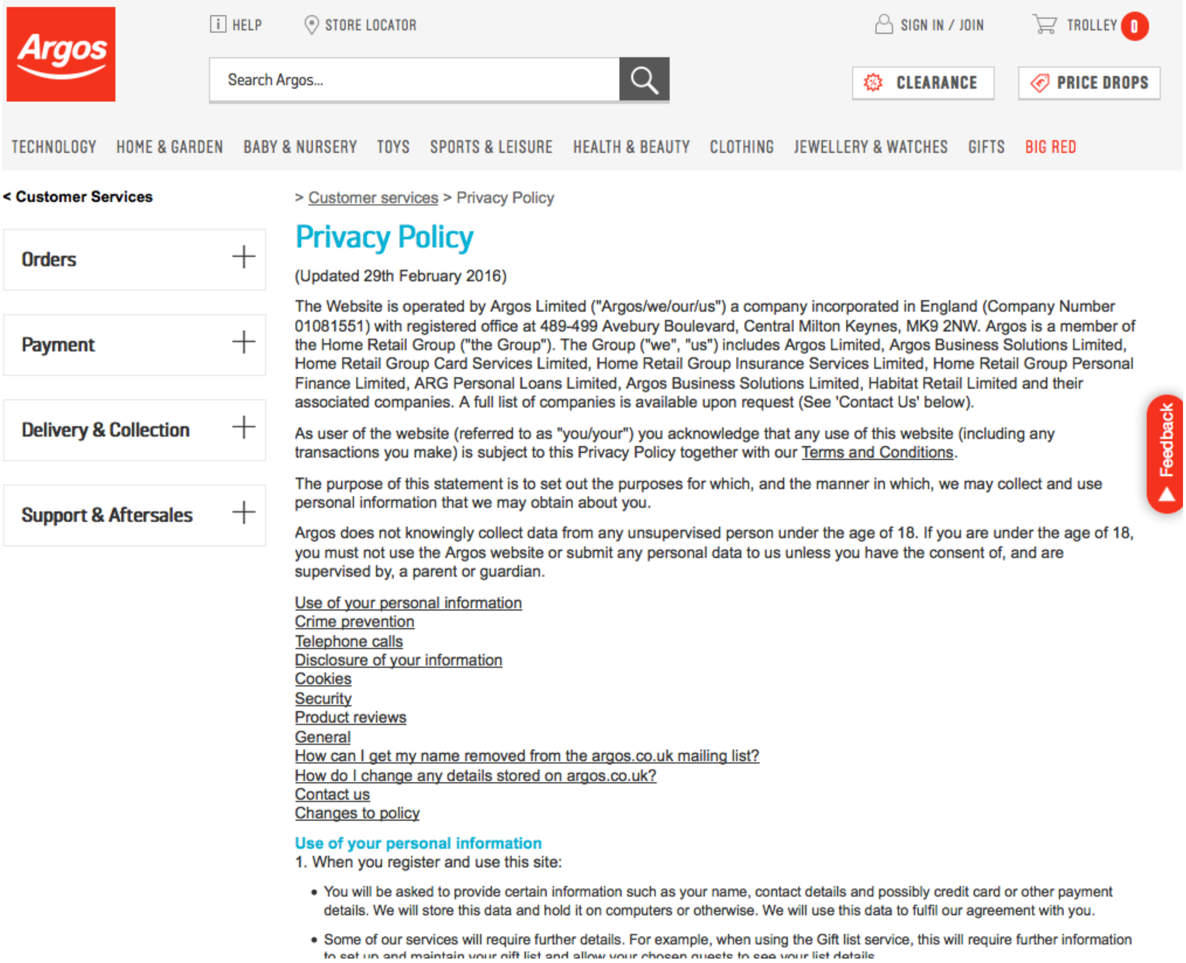
Users reacted positively to the changes made in the second iteration design phase. One user in FG1 described her feelings towards the use of containers to encapsulate policy information:

> "I think that it [the summary layer] is easy to read on the eye because everything is boxed up. I think that really helps."

Furthermore, one individual in FG1 felt that including a link to opt out of personal data being used for sharing or marketing was useful. In addition, one participant felt that the use of ticks and crosses was simple to understand while another individual pointed out that the links to the full policy "stood out" from the rest of the content.

6.7.3 Prototype Improvements

After evaluating the usefulness of the summary layer focus group participants were shown policy A, policy B and policy C. Policy A, shown in figure 6.7, was from Argos.co.uk; policy B. shown in figure 6.8, was from Tesco.com and policy C, shown in figure 6.9, was from Tkmaxx.com. Participants were asked to review policies A, B and C and highlight how the prototype design could be improved taking into consideration the format of the three other policies.



> Customer services > Privacy Policy

Privacy Policy

(Updated 29th February 2016)

The Website is operated by Argos Limited ("Argos/we/our/us") a company incorporated in England (Company Number 01081551) with registered office at 489-499 Avebury Boulevard, Central Milton Keynes, MK9 2NW. Argos is a member of the Home Retail Group ("the Group"). The Group ("we", "us") includes Argos Limited, Argos Business Solutions Limited, Home Retail Group Card Services Limited, Home Retail Group Insurance Services Limited, Home Retail Group Personal Finance Limited, ARG Personal Loans Limited, Argos Business Solutions Limited, Habitat Retail Limited and their associated companies. A full list of companies is available upon request (See 'Contact Us' below).

As user of the website (referred to as "you/your") you acknowledge that any use of this website (including any transactions you make) is subject to this Privacy Policy together with our Terms and Conditions.

The purpose of this statement is to set out the purposes for which, and the manner in which, we may collect and use personal information that we may obtain about you.

Argos does not knowingly collect data from any unsupervised person under the age of 18. If you are under the age of 18, you must not use the Argos website or submit any personal data to us unless you have the consent of, and are supervised by, a parent or guardian.

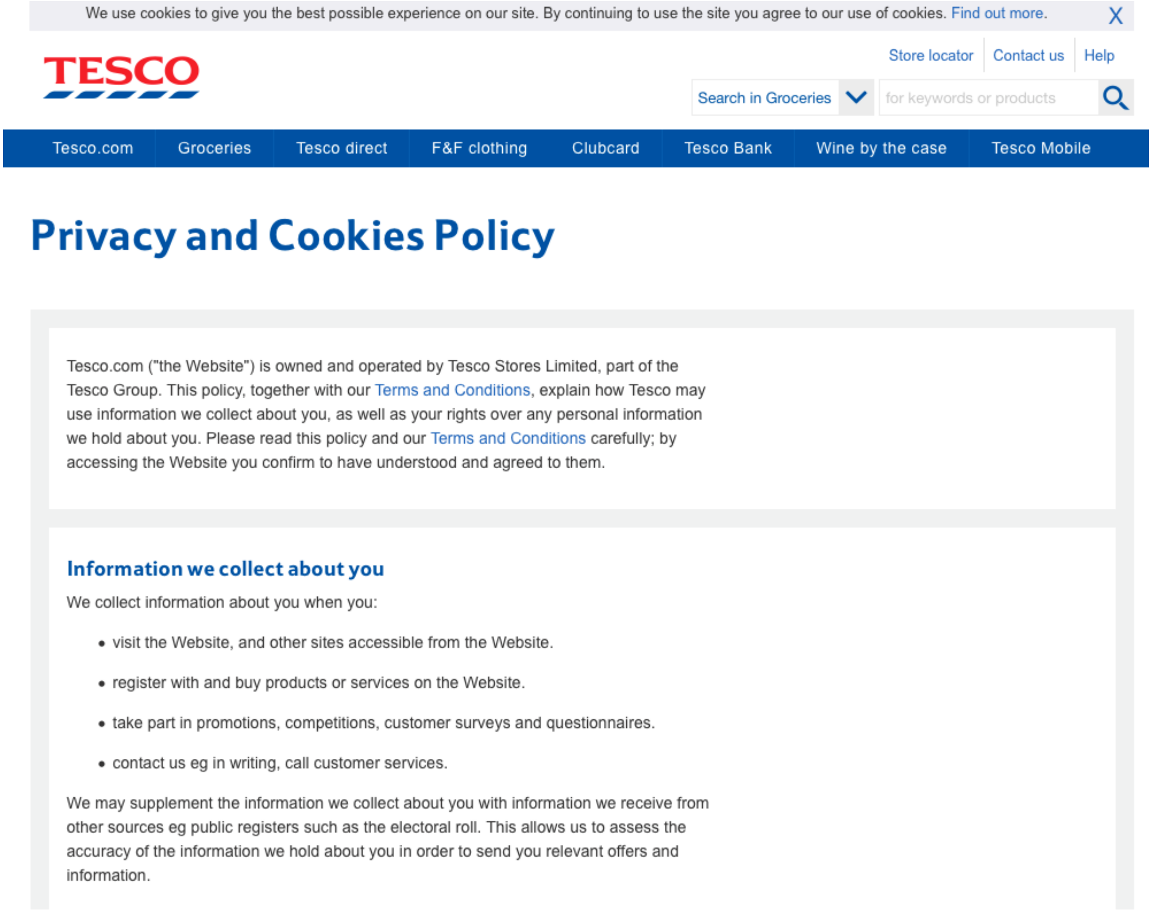
Use of your personal information
Crime prevention
Telephone calls
Disclosure of your information
Cookies
Security
Product reviews
General
How can I get my name removed from the argos.co.uk mailing list?
How do I change any details stored on argos.co.uk?
Contact us
Changes to policy

Use of your personal information

1. When you register and use this site:

- You will be asked to provide certain information such as your name, contact details and possibly credit card or other payment details. We will store this data and hold it on computers or otherwise. We will use this data to fulfil our agreement with you.
- Some of our services will require further details. For example, when using the Gift list service, this will require further information to set up and maintain your gift list and allow your chosen guests to see your list details

Figure 6.7 - Policy A (Argos.co.uk)



We use cookies to give you the best possible experience on our site. By continuing to use the site you agree to our use of cookies. Find out more.

Privacy and Cookies Policy

Tesco.com ("the Website") is owned and operated by Tesco Stores Limited, part of the Tesco Group. This policy, together with our Terms and Conditions, explain how Tesco may use information we collect about you, as well as your rights over any personal information we hold about you. Please read this policy and our Terms and Conditions carefully; by accessing the Website you confirm to have understood and agreed to them.

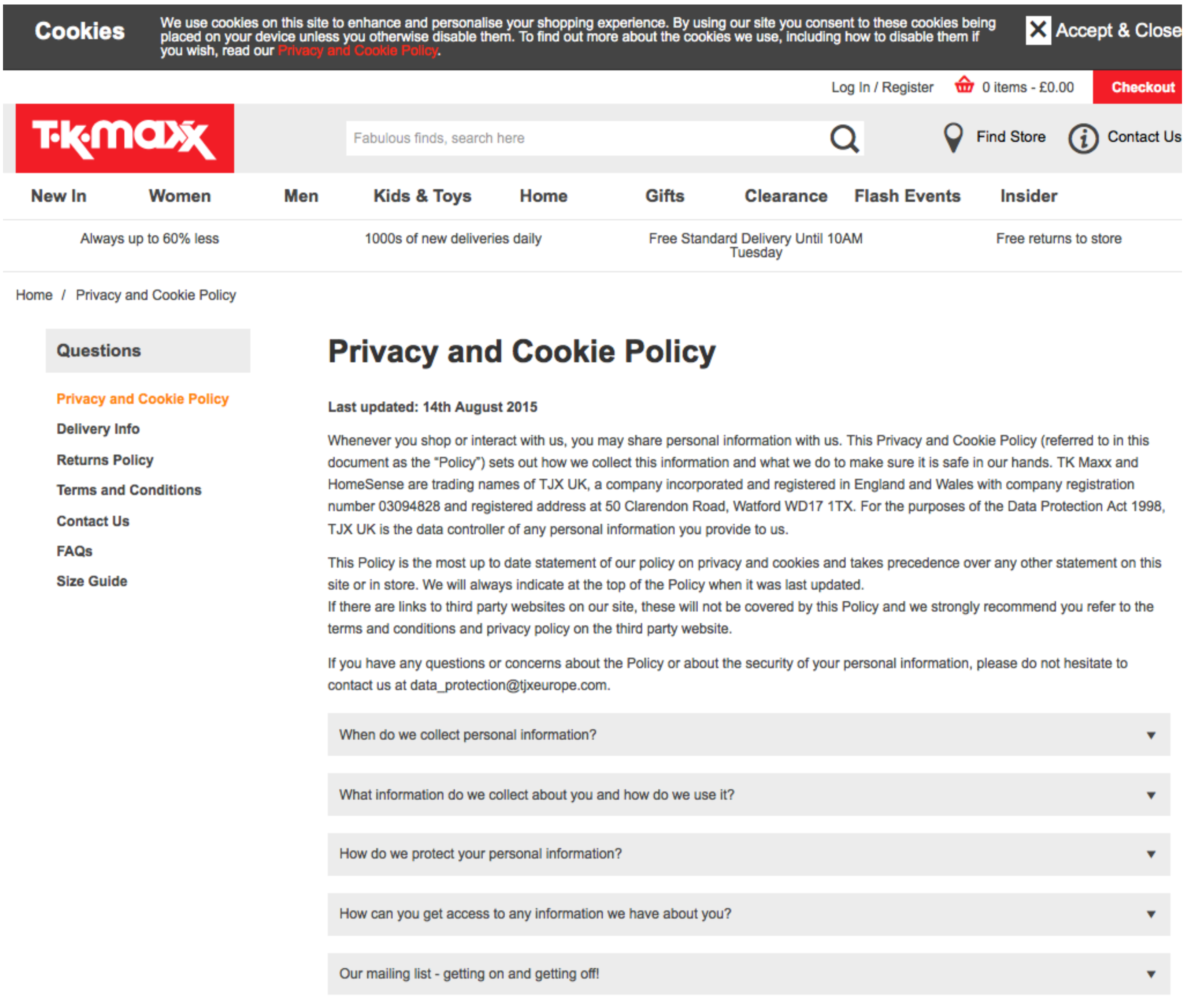
Information we collect about you

We collect information about you when you:

- visit the Website, and other sites accessible from the Website.
- register with and buy products or services on the Website.
- take part in promotions, competitions, customer surveys and questionnaires.
- contact us eg in writing, call customer services.

We may supplement the information we collect about you with information we receive from other sources eg public registers such as the electoral roll. This allows us to assess the accuracy of the information we hold about you in order to send you relevant offers and information.

Figure 6.8 - Policy B (Tesco.com)



We use cookies on this site to enhance and personalise your shopping experience. By using our site you consent to these cookies being placed on your device unless you otherwise disable them. To find out more about the cookies we use, including how to disable them if you wish, read our Privacy and Cookie Policy.

Privacy and Cookie Policy

Last updated: 14th August 2015

Whenever you shop or interact with us, you may share personal information with us. This Privacy and Cookie Policy (referred to in this document as the "Policy") sets out how we collect this information and what we do to make sure it is safe in our hands. TK Maxx and HomeSense are trading names of TJX UK, a company incorporated and registered in England and Wales with company registration number 03094828 and registered address at 50 Clarendon Road, Watford WD17 1TX. For the purposes of the Data Protection Act 1998, TJX UK is the data controller of any personal information you provide to us.

This Policy is the most up to date statement of our policy on privacy and cookies and takes precedence over any other statement on this site or in store. We will always indicate at the top of the Policy when it was last updated.
If there are links to third party websites on our site, these will not be covered by this Policy and we strongly recommend you refer to the terms and conditions and privacy policy on the third party website.

If you have any questions or concerns about the Policy or about the security of your personal information, please do not hesitate to contact us at data_protection@tjxeurope.com.

When do we collect personal information? ▼

What information do we collect about you and how do we use it? ▼

How do we protect your personal information? ▼

How can you get access to any information we have about you? ▼

Our mailing list - getting on and getting off! ▼

Figure 6.9 - Policy C (Tkmaxx.com)

Policy C used an accordion control. An accordion control is used to display collapsible information. A user clicks on the control and a panel appears below displaying information. All ten focus group participants agreed that the full privacy and cookie layers of the prototype would benefit from an accordion control. One user in FG1 felt that an accordion control helped to “break down” policy information while a participant in FG2 stated that an accordion control “saves you scrolling through masses and it probably standards out a bit more.”

Policy C used a question format for headings and seven focus group participants felt that this was effective. One participant in FG1 stated that this style of headings worked well because:

> "…they are probably questions that you are likely to have as well. It is not just listing a load of legal stuff. Like you would be looking at this thinking, how do I get off their mailing list? Oh, it's there. So, it's really easy. It's user friendly."

Another user in FG1 agreed. This person felt that using questions as headings created a "more personal" feel to the policy while a third participant commented that the questions were useful because they were the type of questions "you think of in your head." Similar findings emerged from the second focus group. One individual mentioned:

> "I think the questions do work well. I think if you read that summary and you think, right I want to know a bit more about this, you've probably got questions in your head that you sort of want to really answer and then you go onto that full policy and your headings are there as questions."

When asked whether they preferred the heading as a question one individual in focus group two stated that it "made sense" because "you are answering the question in your head as you read the information". This response generated agreement from two other participants.

In FG2, one user pointed out that he felt that the table used in the summary layer to display personal data sharing information would also be useful in the summary layer. He stated that "it would be easier to have a table in there [the full privacy layer] than just a load of text. It helps to break everything up as well." Three other individuals agreed, and one user commented "yeah it makes sense, just like the table in the summary bit. That was clear and easy to follow."

6.8 Third Iteration Prototype

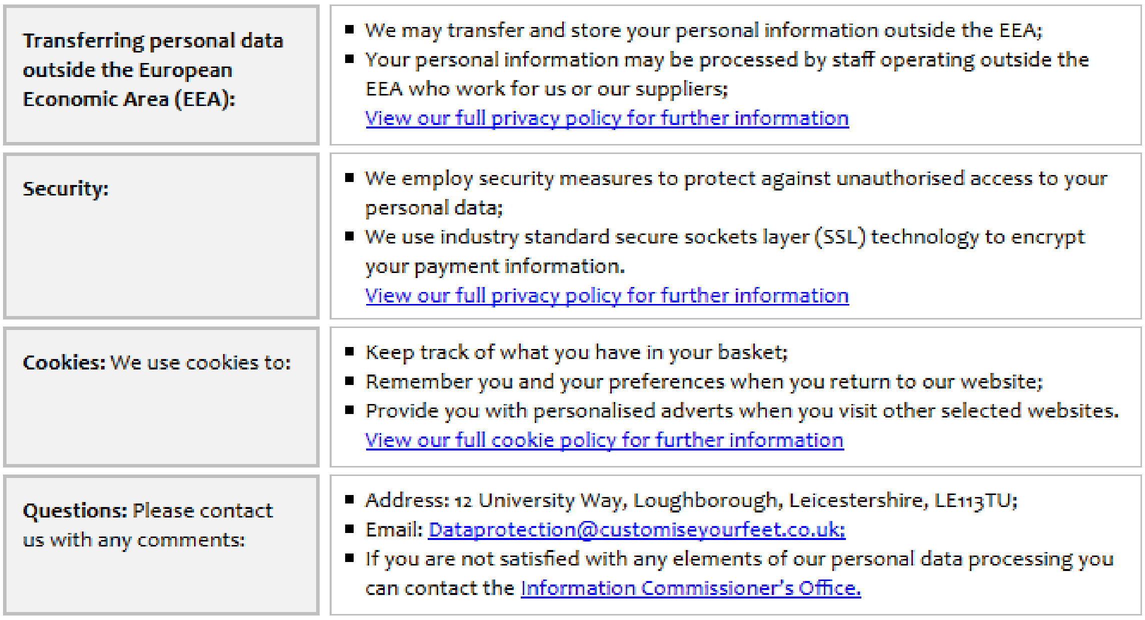
Following the two user evaluation focus groups a third iteration prototype was produced. Four changes to the second iteration prototype were made based on the findings from the user evaluation. These changes were:

1. The section on subject rights was removed from the summary layer and replaced with information about transferring personal data outside the EEA. Users felt that this change was necessary because they would like to know whether personal data is transferred outside the EEA. The change is shown in figure 6.10.

2. Accordion controls were added to the full privacy and full cookie layer. This will benefit users because there is no longer the requirement to scroll through the entire webpage to locate information towards the latter part of the policy. The change is shown in figure 6.11.

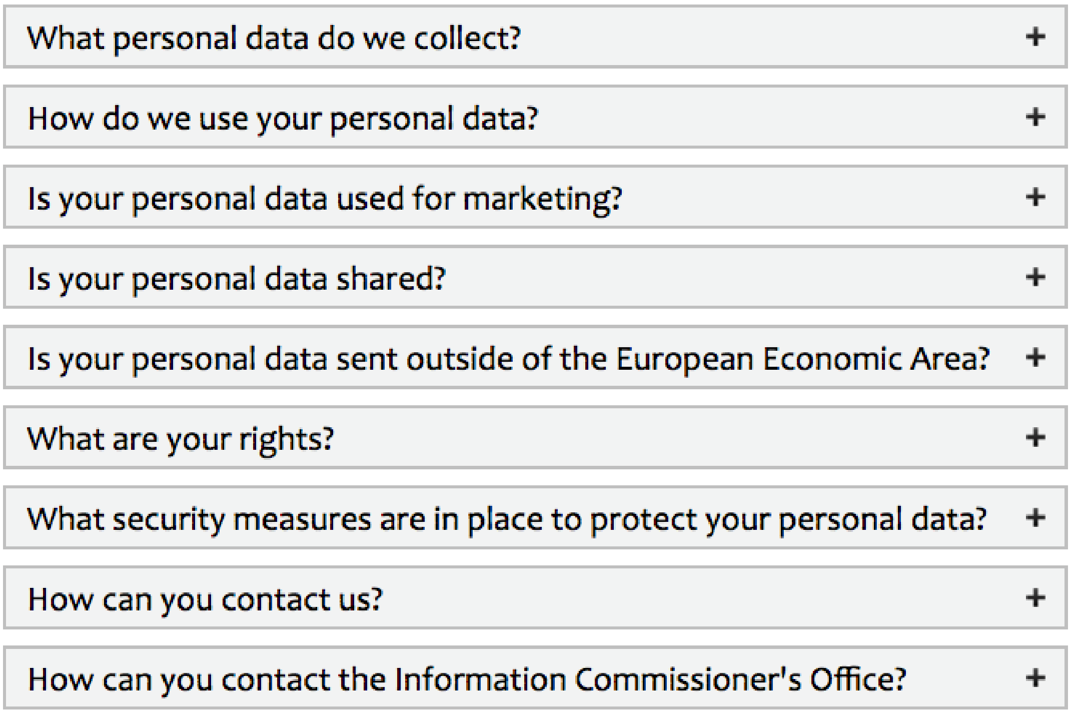
3. The full privacy and full cookie layer headings were changed to questions. This change is shown in figure 6.11.

4. A table was added to the sharing section of the full privacy layer. This change is shown in figure 6.12.



Transferring personal data outside the European Economic Area (EEA):	▪ We may transfer and store your personal information outside the EEA; ▪ Your personal information may be processed by staff operating outside the EEA who work for us or our suppliers; View our full privacy policy for further information
Security:	▪ We employ security measures to protect against unauthorised access to your personal data; ▪ We use industry standard secure sockets layer (SSL) technology to encrypt your payment information. View our full privacy policy for further information
Cookies: We use cookies to:	▪ Keep track of what you have in your basket; ▪ Remember you and your preferences when you return to our website; ▪ Provide you with personalised adverts when you visit other selected websites. View our full cookie policy for further information
Questions: Please contact us with any comments:	▪ Address: 12 University Way, Loughborough, Leicestershire, LE113TU; ▪ Email: Dataprotection@customiseyourfeet.co.uk; ▪ If you are not satisfied with any elements of our personal data processing you can contact the Information Commissioner's Office.

Figure 6.10 - Third iteration prototype summary layer changes



What personal data do we collect? +

How do we use your personal data? +

Is your personal data used for marketing? +

Is your personal data shared? +

Is your personal data sent outside of the European Economic Area? +

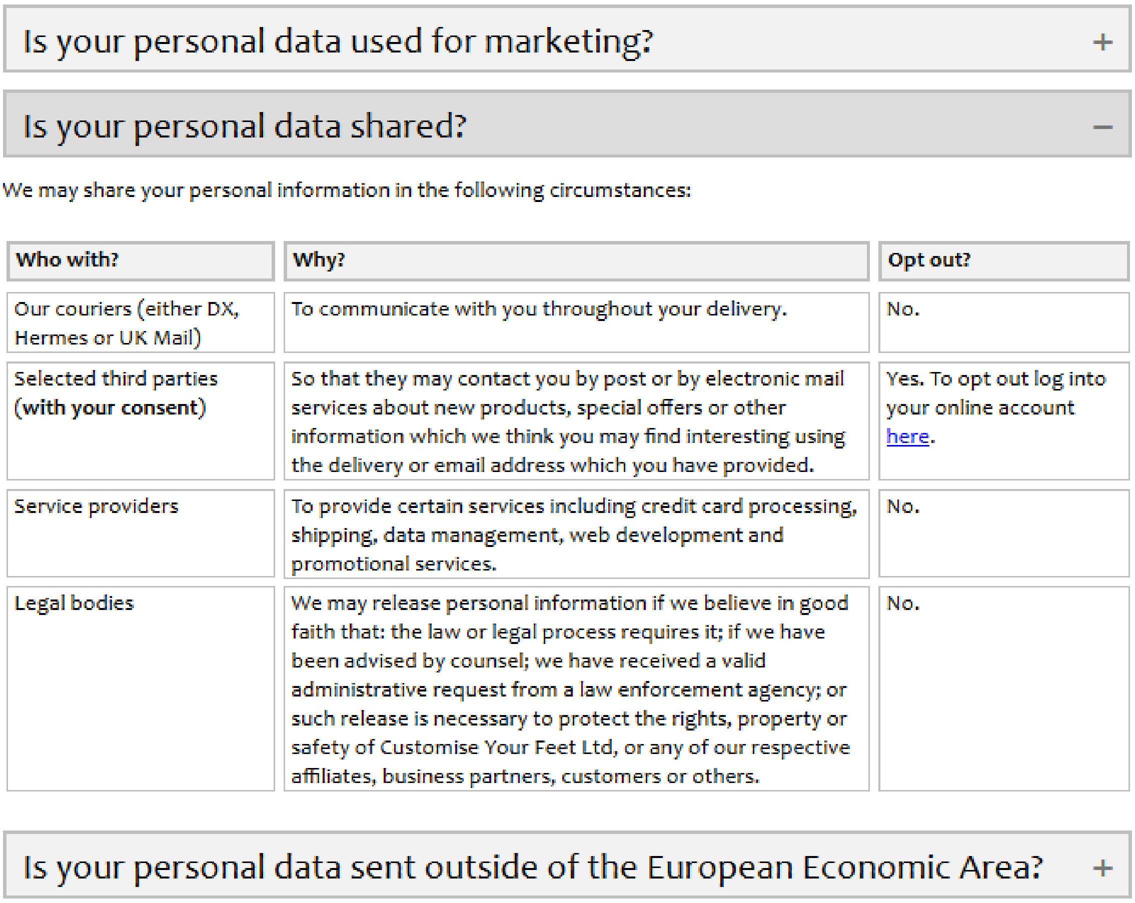
What are your rights? +

What security measures are in place to protect your personal data? +

How can you contact us? +

How can you contact the Information Commissioner's Office? +

Figure 6.11 - Third iteration prototype full privacy layer changes



Is your personal data used for marketing? +

Is your personal data shared? –

We may share your personal information in the following circumstances:

Who with?	**Why?**	**Opt out?**
Our couriers (either DX, Hermes or UK Mail)	To communicate with you throughout your delivery.	No.
Selected third parties (**with your consent**)	So that they may contact you by post or by electronic mail services about new products, special offers or other information which we think you may find interesting using the delivery or email address which you have provided.	Yes. To opt out log into your online account here.
Service providers	To provide certain services including credit card processing, shipping, data management, web development and promotional services.	No.
Legal bodies	We may release personal information if we believe in good faith that: the law or legal process requires it; if we have been advised by counsel; we have received a valid administrative request from a law enforcement agency; or such release is necessary to protect the rights, property or safety of Customise Your Feet Ltd, or any of our respective affiliates, business partners, customers or others.	No.

Is your personal data sent outside of the European Economic Area? +

Figure 6.12 - Third iteration prototype sharing section changes

6.9 Summary

This chapter outlined the design process and decisions taken when the standardised prototype privacy policy was developed. Design objectives were outlined at the start of the chapter. Table 6.2 summarises how each design objective was operationalised. Three iterative policy designs were produced. The designs were evaluated by the researcher and e-commerce users. Two focus groups were carried out with e-commerce users. These focus groups addressed research question four. Research question four was: **how useful is the standardised prototype?** Findings showed that users preferred accordion controls as a method of presenting policy information. Results also showed that users welcomed the layered approach to presenting information. The standardised prototype privacy policy was the subject of usability testing in the next phase.

	Prototype design objective	Operationalisation
1	The prototype should not be perceived as a long document. Users do not want to open a privacy policy and be presented with numerous paragraphs of text.	A layered approach divides policy content over three pages. The first page a user is presented with is the summary layer and not a lengthy unstructured document.
2	The prototype design should allow consumers to feel that they can locate and retrieve information easily and quickly.	Consistent headings will allow users to become familiar with where information is located facilitating quicker and easier information retrieval. This is examined in more detail in phase four.
3	The prototype design should follow with best practice guidelines.	
4	The prototype design should mention that consent is obtained prior to processing.	The prototype design uses a tabular format to display sharing and marking information within the summary layer. A tabular display is also used in the full layer to display sharing information. The first column in each table describes how personal data is used and uses an emphasised style to state whether consent is obtained prior to processing.

5	The prototype design should refer to the relevant legislation.	The prototype design refers to the relevant legislation in the introduction of the full privacy layer.

Table 6.2 - A summary of how the prototype design objectives were operationalised

Chapter 7 - Phase Four: Policy Usability

7.1 Introduction

In phase three several prototype design objectives were outlined. Prototype design objective six was: the prototype should allow users to feel that information can be retrieved quickly and easily. Phase four determined the extent to which this criterion was met. Two research questions were devised based on design objective six. These questions were:

5. **Do users feel the standardised prototype privacy policy is easier to use than a typical privacy policy?**
6. **Do users feel the standardised prototype privacy policy can be used to retrieve information more efficiently than a typical privacy policy?**

To address research question five and six a usability study was carried out. The opportunity to assess user attitudes also enabled a seventh research question to be addressed. Research question seven was:

7. **Do users support the idea of a standardised format privacy policy like the standardised prototype design?**

Figure 7.1 provides an overview of the different research phases in this study showing how phase four fits in with the overall research design.

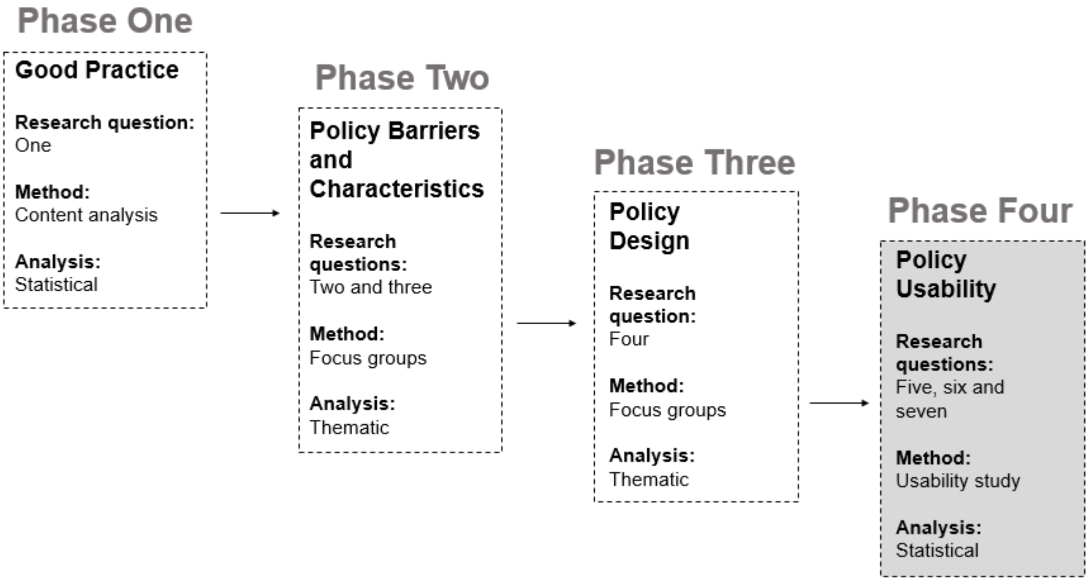


Figure 7.1 - Research design

7.2 Integration of Findings from Research Phases One, Two and Three

The standardised prototype design produced in phase three was the subject of usability testing in phase four. The user evaluation carried out in phase three provided useful insights that informed the development of the prototype however the evaluation was qualitative in nature and only involved two small groups of users. The usability study in phase four continued the process of evaluation albeit with a different focus. Usability metrics were used to assess attitudes towards the standardised prototype privacy policy and a typical privacy policy. The tasks users were asked to perform, along with the post-task and post-study statements used to measure perceived ease of use, perceived efficiency and attitudes towards standardisation can be found in appendix G.

The typical format privacy policy was influenced by the findings of phase one. The typical privacy policy was not presented in a layered format. This is because findings from 2015 showed no evidence of layered privacy policies. Results from phase one also showed that over half of the privacy policies sampled in 2015 published a cookie policy on a separate webpage to the privacy policy. The typical policy made a provision for this finding as well. Table 7.1 shows the format characteristics for both policies. Table 7.2 outlines the content characteristics of both policies. The content of the standardised and typical privacy policies was very similar. This was to ensure that any attitudinal differences between the two policies could be attributed to the format of the policy and not the content. There were minor differences in policy content. This was to ensure that there were some differences in the outcome of each task. The standardised and typical privacy policies are presented in appendix H and appendix I.

Format characteristic	Policy	
	Standardised prototype	Typical
Is the privacy policy presented in a layered format?	✓	✗
Is a separate cookie policy published?	✓	✓
Is the privacy policy presented using an accordion control?	✓	✗
Does the privacy policy include a summary layer?	✓	✗
Does the privacy policy present data sharing information within a table?	✓	✗

Table 7.1 - Standardised and typical privacy policy format characteristics

Good practice guidelines from phase one	Policy	
	Standardised prototype	Typical
Does the privacy policy mention when the policy was last updated?	✓	✓
Does the privacy policy explicitly mention the identity of the data controller?	✓	✓
Is it possible to infer who the data controller is from the privacy policy?	N/A	N/A
Does the privacy policy identify the purpose or purposes for which personal data will be processed?	✓	✓
Does the privacy policy identify a named individual to contact regarding personal data processing?	✓	✓
Does the privacy policy mention that personal data is or might be shared for direct marketing purposes (with or without the consent of the user)?	✓	✓
Does the privacy policy mention with whom personal data will be shared?	✓	✓

Are any names of organisations mentioned?	✓	✓
Does the privacy policy mention that it is possible to view or amend personal data?	✓	✓
Does the privacy policy mention that it is the right of the user to request a copy of the personal data being processed?	✓	✓
Does the privacy policy mention that it is the right of the user to amend inaccurate personal data being processed?	✓	✓
Does the privacy policy mention that it is the right of the user to remove inaccurate personal data being processed?	✓	✓
Does the privacy policy mention that it is possible to prevent personal data being used for direct marketing?	✓	✓
Does the privacy policy mention that it is the right of the user to prevent personal data being processed for direct marketing purposes?	✓	✓
Does the privacy policy mention that the user has the option to contact the Information Commissioner’s Office should a dispute arise?	✓	✗
Does the privacy policy mention any contact details for the organisation?	✓	✓
Does the privacy policy mention a specific length of time personal data will be retained for?	✗	✗
Does the privacy policy mention anything about the technology or technologies used to keep personal data secure?	✓	✓
Does the cookie policy describe the purpose or purposes for which cookies are used?	✓	✓

Table 7.2 - Standardised and typical privacy policy content characteristics

7.3 Individual and Group Demographics

Thirty-five individuals participated in the user study however eight responses were unusable because they were either incomplete, selected more than one option for a question or were completed by individuals from outside the UK. Responses from these participants were rejected from the study leaving twenty-seven usable responses. Participants were randomly divided into two groups to reduce the possibility of the learning effect biasing the findings. Group one consisted of fourteen participants and thirteen participants were in group two. Approximately three quarters of responses were from participants aged 18-20 and of male gender. Approximately two thirds of respondents stated they had used a website to buy a product in the last week. The overall and group demographic characteristics of participants are shown in table 7.3 and table 7.4. The reported purchase behaviour of participants is shown in table 7.5.

What is your age?								
	18-20	21-25	26-30	31-35	36-40	41-45	46-50	50+
Overall	20 (74.1)	6 (22.2)	0 (0.0)	0 (0.0)	0 (0.0)	1 (3.7)	0 (0.0)	0 (0.0)
Group 1	10 (71.2)	4 (28.6)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
Group 2	10 (76.9)	2 (15.4)	0 (0.0)	0 (0.0)	0 (0.0)	1 (7.7)	0 (0.0)	0 (0.0)

Table 7.3 – Participant age distribution

What is your gender?			
	Male	Female	Prefer not to say
Overall	20 (74.1)	7 (25.9)	0 (0.0)
Group 1	11 (78.6)	3 (21.4)	0 (0.0)
Group 2	9 (69.2)	4 (30.8)	0 (0.0)

Table 7.4 - Participant gender distribution

When did you last purchase something from an online website?				
	Within the last week	Within the last month	Within the last six months	Longer than six months ago
Overall	18 (66.7)	8 (29.6)	1 (3.7)	0 (0.0)
Group 1	8 (57.1)	5 (35.7)	1 (7.1)	0 (0.0)
Group 2	10 (76.9)	3 (23.1)	0 (0.0)	0 (0.0)

Table 7.5 - Participant purchasing distribution

7.4 Task Accuracy and Post-Task Responses

Participants completed five tasks. The accuracy results of each task and the associated post-task responses are presented in this section. Each task required the participant to answer the same question using the standardised prototype and typical privacy policy. Participants were provided with a choice of possible answers depending on the question. After answering each question participants were then asked to respond to two post-task statements. One statement related to perceived ease of use and one statement related to perceived efficiency (Davis, 1989). A five-point Likert scale was used to record post-task responses, with options ranging from strongly disagree to strongly agree. Participants in group one performed each task using the standardised prototype first followed by the typical format. Individuals in group two did the opposite.

The proportion of correct responses for each task is reported along with a cross tabulation showing the differences between policy formats. Following this, post-task responses are presented. Possible answers in task accuracy tables are abbreviated to N (No); Y (yes); YWC (yes with consent) and PDNS (policy does not say). In each post-task response table responses are abbreviated to St A (strongly agree); A (agree); N (neutral); D (disagree) and St D (strongly disagree). In both the task accuracy and post-task response tables the standardised prototype policy is abbreviated to SP and the typical format is abbreviated to T. Overall and group (one and two) responses are provided for both task accuracy and post-task responses. At the end of this section a cumulative mean task accuracy is provided.

For task accuracy, a McNemar’s test was performed to determine whether there was a statistically significant difference between the proportion of correct answers for each policy format. For post-task responses a paired samples t-test was performed to determine whether there was a statistically significant mean difference between policy formats.

7.4.1 Task One: Direct Marketing

Question one stated: based on the policies, can you prevent your personal data being used to send you information about products or services? The correct response to this question was yes for both policy formats. Table 7.6 shows that overall, twenty-two (81.5%) participants answered correctly for the standardised prototype and the typical policy. A McNemar's test was not performed for this question because it was clear there were no differences between formats. This is shown table 7.7.

Question: Based on the policies, can you prevent your personal data being used to send you information about products or services? Correct answer: SP: Yes; T; Yes						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
N	3 (21.4)	1 (7.1)	4 (30.8)	2 (15.4)	5 (18.5)	5 (18.5)
Y	11 (78.6)	13 (92.9)	9 (69.2)	11 (84.6)	22 (81.5)	22 (81.5)
PDNS	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)

Table 7.6 – Direct marketing accuracy responses

Question: Based on the policies, can you prevent your personal data being used to send you information about products or services?				
		T (%)		
		Incorrect	Correct	Total
SP (%)	Incorrect	3 (11.1)	2 (7.4)	5 (18.5)
	Correct	2 (7.4)	20 (74.1)	22 (81.5)
	Total	5 (18.5)	22 (81.5)	27 (100.0)

Table 7.7 - Direct marketing accuracy differences

Table 7.9 shows that for the standardised prototype over three quarters (77.8%) of the twenty-seven participants agreed to some extent that they could locate the information required to answer question one with ease. Additionally, under two thirds (59.2%) of individuals responded the same way for the typical format. The results also show that six (22.2%) individuals disagreed that they could locate the answer to question one with ease when using the typical policy while just two (7.4%) individuals felt the same about the standardised prototype. On average participants felt that the standardised prototype (mean: 3.96; SD: 0.85) allowed them to locate the answer to question one with more ease compared to the typical format (mean: 3.52; SD: 1.01). A paired samples t-test determined that the mean difference between policy formats (0.44; 95% CI 0.11 to 0.78) was statistically significant (t=2.726; df=26; p=0.011).

Table 7.9 demonstrates that eleven (40.7%) participants agreed that they could locate the information required to answer question one quickly for the standardised prototype while approximately 10% fewer individuals responded in the same way for the typical policy. Additionally, just over one quarter (25.9%) of participants strongly agreed that they could find the answer to question one quickly using the standardised prototype compared to under 15% for the typical format. The typical policy also saw a higher proportion of individuals disagreeing to some extent that they could locate the answer to question one quickly. In total, almost 30% of participants felt this way about the typical format compared to just over 10% for the standardised prototype. On average participants felt that the standardised prototype (mean: 3.78; SD: 1.05) allowed them to locate the information required to answer question one quicker than the typical format (mean: 3.26; SD 1.13). A paired samples t-test determined that the mean difference between policy formats (0.52; 95% CI 0.01 to 1.03) was statistically significant (t=2.101; df=26; p=0.045).

Statement 1a and 1c: I could locate the information required to answer question one with ease.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
D	0 (0.0)	1 (7.1)	5 (38.5)	2 (15.4)	2 (7.4)	6 (22.2)
N	2 (14.3)	2 (14.3)	3 (23.1)	2 (15.4)	4 (14.8)	5 (18.5)
A	9 (64.3)	7 (50.0)	5 (38.5)	5 (38.5)	14 (51.9)	12 (44.4)
St A	3 (21.4)	4 (28.6)	0 (0.0)	4 (30.8)	7 (25.9)	4 (14.8)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
M	4.07	4.00	3.00	3.85	3.96	3.52
SD	0.62	0.88	0.91	1.07	0.85	1.01

Table 7.8 - Direct marketing post-task perceived ease of use responses

Statement 1b and 1d: I could locate the information required to answer question one quickly.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	1 (7.7)	1 (7.7)	1 (3.7)	1 (3.7)
D	1 (7.1)	1 (7.1)	6 (46.2)	1 (7.7)	2 (7.4)	7 (25.9)
N	3 (21.4)	2 (14.3)	5 (38.5)	3 (23.1)	6 (22.2)	7 (25.9)
A	7 (50.0)	7 (50.0)	1 (7.7)	4 (30.8)	11 (40.7)	8 (29.6)
St A	3 (21.4)	4 (28.6)	0 (0.0)	4 (30.8)	7 (25.9)	4 (14.8)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
M	3.86	4.00	2.46	3.69	3.78	3.26
SD	0.86	0.88	0.77	1.25	1.05	1.13

Table 7.9 - Direct marketing post-task perceived efficiency responses

7.4.2 Task Two: Cookie Links

Question two stated: do the policies provide any links to external websites about cookies? The correct response to this question was yes for the standardised prototype and no for the typical policy. Table 7.10 shows that overall twenty-three (82.5%) participants responded correctly for both policies. A McNemar's test was not performed for this question because it was clear there were no differences. This is shown in table 7.11.

Question: Do the policies provide any links to external websites about cookies? Correct answer: SP: Yes; T: No						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
N	2 (14.3)	13 (92.9)	10 (76.9)	2 (15.4)	4 (14.8)	23 (85.2)
Y	12 (85.7)	1 (7.1)	2 (15.4)	11 (84.6)	23 (85.2)	3 (11.1)
PDNS	0 (0.0)	(0.0)	1 (7.7)	0 (0.0)	0 (0.0)	1 (3.7)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)

Table 7.10 - Cookie links accuracy responses

Question: Do the policies provide any links to external websites about cookies?				
		T (%)		
		Incorrect	Correct	Total
SP (%)	Incorrect	1 (3.7)	3 (11.1)	4 (14.8)
	Correct	3 (11.1)	20 (74.1)	23 (85.2)
	Total	4 (14.8)	23 (85.2)	27 (100.0)

Table 7.11 - Cookie links accuracy differences

Findings in table 7.12 show that ten (37%) participants agreed that they could locate the information required to answer question two with ease when using the standardised prototype and the typical format. Additionally, just over 40% of participants strongly agreed that they could locate the answer to question two with ease using the standardised prototype while only approximately 15% of individuals responded in the same way for the typical format. A higher proportion of participants disagreed to some extent that the answer to question two could be located with ease for the typical format (29.6%) compared to the prototype (11.1%). On average participants felt that they could locate the information required to answer two with more ease using the standardised prototype (mean: 4.07; SD: 1.00) compared to the typical format (mean: 3.22; SD: 1.31). A paired samples t-test determined that the mean difference between policy formats (0.85; 95% CI 0.21 to 1.49) was statistically significant (t=2.749; df=26; p=0.011).

Table 7.13 shows that just over 40% of participants agreed that they could locate the answer to question two quickly when using the standardised prototype while approximately 30% of individuals responded in the same way for the typical format. Furthermore, when using the standardised prototype just over 40% of participants strongly agreed that the information required to answer question two could be located quickly while only approximately 11% of individuals felt the same could be said about the typical format. In contrast, one third of the twenty-seven participants disagreed to some extent that the typical format allowed them to locate the answer to question two quickly compared to just over 10% for the standardised prototype. On average participants felt that the standardised prototype (mean: 4.11; SD: 0.98) allowed them to locate the information required to answer question two quicker than the typical format (mean: 3.00; SD 1.30). A paired samples t-test determined that the mean difference between policy formats (1.11; 95% CI 0.51 to 1.72) was statistically significant (t=3.780; df=26; p=0.001).

Statement 2a and 2c: I could locate the information required to answer question two with ease.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	1 (7.1)	3 (32.1)	0 (0.0)	0 (0.0)	4 (14.8)
D	2 (14.3)	1 (7.1)	3 (23.1)	1 (7.7)	3 (11.1)	4 (14.8)
N	2 (14.3)	4 (28.6)	1 (7.7)	1 (7.7)	3 (11.1)	5 (18.5)
A	5 (35.7)	5 (35.7)	5 (38.5)	5 (38.5)	10 (37.0)	10 (37.0)
St A	5 (35.7)	3 (21.4)	1 (7.7)	6 (46.2)	11 (40.7)	4 (14.8)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
M	3.93	3.57	2.85	4.23	4.07	3.22
SD	1.07	1.16	1.41	0.93	1.00	1.31

Table 7.12 - Cookie links post-task perceived ease of use responses

Statement 2b and 2d: I could locate the information required to answer question two quickly.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	1 (7.1)	4 (30.8)	0 (0.0)	0 (0.0)	5 (18.5)
D	1 (7.1)	2 (14.3)	2 (15.4)	2 (15.4)	3 (11.1)	4 (14.8)
N	2 (14.3)	5 (35.7)	2 (15.4)	0 (0.0)	2 (7.4)	7 (25.9)
A	5 (35.7)	4 (28.6)	4 (30.8)	6 (46.2)	11 (40.7)	8 (29.6)
St A	6 (42.9)	2 (14.3)	1 (7.7)	5 (38.5)	11 (40.7)	3 (11.1)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	4.14	3.29	2.69	4.08	4.11	3.00
SD	0.95	1.14	1.44	1.04	0.97	1.30

Table 7.13 - Cookie links post-task perceived efficiency responses

7.4.3 Task Three: Personal Data Sharing

Question three stated: based on the policies, might your personal data be shared with another organisation that may use it to send you information about products or services? The correct response to this question was either yes or yes with consent for the standardised prototype and yes for the typical format. The results table 7.14 show that all participants answered this question correctly for the standardised prototype while 88.9% of individuals selected the right answer for the typical format. The difference in proportion of correct responses was a consequence of three individuals answering the question correctly for the standardised prototype and not so for the typical format. This is shown in table 7.15. An exact McNemar's test determined that the difference between the proportion of correct answers for both policy formats was not statistically significant (n=27; p=0.250).

Question: Based on the policies, might your personal data be shared with another organisation that may use it to send you information about products or services? Answer: SP: Yes or Yes with consent; T: Yes						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
N	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
Y	5 (35.7)	12 (85.7)	12 (92.3)	4 (30.8)	9 (33.3)	24 (88.9)
YWC	9 (64.3)	2 (14.3)	0 (0.0)	9 (69.2)	18 (66.7)	2 (7.4)
PDNS	0 (0.0)	0 (0.0)	1 (7.7)	0 (0.0)	0 (0.0)	1 (3.7)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)

Table 7.14 - Sharing accuracy responses

Question: Based on the policies, might your personal data be shared with another organisation that may use it to send you information about products or services?				
		T (%)		
		Incorrect	Correct	Total
SP (%)	Incorrect	0 (0.0)	0 (0.0)	0.(0.0)
	Correct	3 (11.1)	24 (88.9)	27 (100.0)
	Total	3 (11.1)	24 (88.9)	27 (100.0)

Table 7.15 - Sharing accuracy differences

Table 7.16 highlights that over half (55.6%) of respondents agreed that the answer to question three could be located with ease using the typical format with two (7.4%) individuals strongly agreeing for the same format. In comparison, almost half (48.1%) of individuals strongly agreed that they could locate the information required to answer question three with ease using the standardised prototype while close to 30% of participants agreed with the same statement for the same policy. On average, participants felt that they could locate information with more ease using the standardised prototype (mean: 4.19; SD: 0.96) compared to the typical format (mean: 3.52; SD: 0.94). A paired samples t-test determined that the mean difference between policy formats (0.67; 95% CI 0.24 to 1.09) was statistically significant (t=3.225; df=26; p=0.003).

Findings in table 7.17 for question three show almost half (48.1%) of the twenty-seven participants strongly agreed that they could locate the answer quickly for the standardised prototype while only two (7.4%) out of twenty-seven individuals responded the same way for the typical format. Seven (25.9%) individuals either disagreed or strongly disagreed that they could find information quickly using the typical format while only two (7.4%) participants responded in the same way for the standardised prototype. On average participants felt that the standardised prototype (mean: 4.19; SD: 0.96) allowed them to locate the information required to answer question three quicker than the typical format (mean: 3.26; SD 1.10). A paired samples t-test determined that the mean difference between policy formats (0.93; 95% CI 0.46 to 1.39) was statistically significant (t=4.097; df=26; p<0.001).

Statement 3a and 3c: I could locate the information required to answer question three with ease.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	1 (7.1)	0 (0.0)	0 (0.0)	0 (0.0)	1 (3.7)
D	2 (14.3)	1 (7.1)	2 (15.4)	0 (0.0)	2 (7.4)	3 (11.1)
N	3 (21.4)	1 (7.1)	5 (38.5)	1 (7.7)	4 (14.8)	6 (22.2)
A	2 (14.3)	10 (71.4)	5 (38.5)	6 (46.2)	8 (29.6)	15 (55.6)
St A	7 (50.0)	1 (7.1)	1 (7.7)	6 (46.2)	13 (48.1)	2 (7.4)
Mean	4.00	3.64	3.38	4.38	4.19	3.52
SD	1.18	1.01	0.87	0.65	0.96	0.94
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)

Table 7.16 - Sharing post-task perceived ease of use responses

Statement 3b and 3d: I could locate the information required to answer question three quickly.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	1 (7.1)	1 (7.7)	0 (0.0)	0 (0.0)	2 (7.4)
D	2 (14.3)	1 (7.1)	4 (30.8)	0 (0.0)	2 (7.4)	5 (18.5)
N	3 (21.4)	2 (14.3)	4 (30.8)	1 (7.7)	4 (14.8)	6 (22.2)
A	2 (14.3)	9 (64.3)	3 (23.1)	6 (46.2)	8 (29.6)	12 (44.4)
St A	7 (50.0)	1 (7.1)	1 (7.7)	6 (26.2)	13 (48.1)	2 (7.4)
Mean	4.00	3.57	2.92	4.38	4.19	3.26
SD	1.18	1.02	1.12	0.65	0.96	1.10
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)

Table 7.17 - Sharing post-task perceived efficiency responses

7.4.4 Task Four: Transfer Outside the EEA

Question four stated: based on the policies, might your personal data be sent outside the European Economic Area (EEA)? The correct answer for the standardised prototype and typical format was yes. In total 100% of respondents answered this question correctly. This is shown in table 7.18. A McNemar's test was not performed for this question because it was clear there were no differences between formats. This is shown in table 7.19.

Question: Based on the policies, might your personal data be sent outside the European Economic Area (EEA)? Correct answer: SP: Yes; T: Yes						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
N	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
Y	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
PDNS	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)

Table 7.18 - Transfer outside the EEA accuracy

Question: Based on the policies, might your personal data be sent outside the European Economic Area (EEA)?				
		Typical format (%)		
		Incorrect	Correct	Total
Prototype (%)	Incorrect	0 (0.0)	0 (0.0)	0 (0.0)
	Correct	0 (0.0)	27 (100.0)	27 (100.0)
	Total	0 (0.0)	27 (100.0)	27 (100.0)

Table 7.19 - Transfer outside the EEA accuracy differences

Findings in Table 7.20 highlight that twenty-four (88.8%) out of twenty-seven participants agreed to some extent that they could locate the answer to question four with ease for the standardised prototype while twenty-one (77.7%) individuals felt the same about the typical format. On average, participants felt they could locate the information required to answer question four with slightly more ease using the standardised prototype (mean: 4.37; SD: 0.69) compared to the typical format (mean: 4.22; SD 0.80). A paired samples t-test determined that the mean difference between policy formats (0.15; 95% CI -0.14 – 0.43) was not statistically significant (t=1.072; df=26; p=0.294).

In total twenty-four (88.9%) and twenty-one (77.7%) individuals agreed to some extent that they could locate the information required to answer question four quickly for the standardised prototype and typical format respectively. This is shown in table 7.21. On average, participants felt that the prototype (mean: 4.41; SD: 0.80) could be used to locate the information required to answer question four quicker than the typical format (mean: 4.19; SD:0.88). A paired samples t-test determined that the mean difference between formats (0.22; 95% CI -0.24 – 0.68) was not statistically significant (t=1.000; df=26; p=0.327).

Statement 4a and 4c: I could locate the information required to answer question four with ease.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
D	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
N	1 (7.1)	3 (21.4)	3 (32.1)	2 (15.4)	3 (11.1)	6 (22.2)
A	6 (42.9)	4 (28.6)	5 (38.5)	5 (38.5)	11 (40.7)	9 (33.3)
St A	7 (50.0)	7 (50.0)	5 (38.5)	6 (46.2)	13 (48.1)	12 (44.4)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	4.43	4.29	4.15	4.31	4.37	4.22
SD	0.65	0.83	0.80	0.75	0.69	0.80

Table 7.20 - Transfer outside the EEA post-task perceived ease of use responses

Statement 4b and 4d: I could locate the information required to answer question four quickly.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
D	1 (7.1)	0 (0.0)	1 (7.7)	0 (0.0)	1 (3.7)	1 (3.7)
N	0 (0.0)	2 (14.3)	3 (23.1)	2 (15.4)	2 (7.4)	5 (18.5)
A	5 (35.7)	5 (35.7)	4 (30.8)	4 (30.8)	9 (33.3)	9 (33.3)
St A	8 (57.1)	7 (50.0)	5 (38.5)	7 (53.8)	15 (55.6)	12 (44.4)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	4.43	4.36	4.00	4.38	4.41	4.19
SD	0.85	0.75	1.00	0.77	0.80	0.88

Table 7.21 - Transfer outside the EEA post-task perceived efficiency responses

7.4.5 Task Five: Contacting an Independent Organisation

Question five stated: based on the policies, can you contact an independent organisation and complain about the processing of your personal data? The correct answer for the standardised prototype was yes. The typical format made no mention of contacting an independent organisation to complain about the processing of personal data and therefore the answers no or policy does not say were accepted as correct for this question. Table 7.22 shows that twenty (74.1%) individuals answered this question correctly for the standardised prototype while nineteen (70.4%) answered correctly for the typical format. Table 7.23 highlights that the difference in proportion was a consequence of six individuals answering correctly using the standardised prototype but not so with the typical format while five participants answered correctly using the typical format but did not so using the standardised prototype. An exact McNemar's test determined that difference between the proportion of correct answers for the prototype and typical format was not statistically significant (n=27; p=1.000).

Question: Based on the policies, can you contact an independent organisation and complain about the processing of your personal data? Correct answer: SP: Yes; T: No or policy does not say						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
N	1 (7.1)	6 (42.9)	7 (53.8)	2 (15.4)	3 (11.1)	13 (48.1)
Y	12 (85.7)	5 (35.7)	3 (23.1)	8 (61.5)	20 (74.1)	8 (29.6)
PDNS	1 (7.1)	3 (21.4)	3 (23.1)	3 (23.1)	4 (14.8)	6 (22.2)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)

Table 7.22 – Contacting an independent organisation accuracy

Question: Based on the policies, can you contact an independent organisation and complain about the processing of your personal data?				
		Typical format (%)		
		Incorrect	Correct	Total
Prototype (%)	Incorrect	2 (7.4)	5 (18.5)	7 (25.9)
	Correct	6 (22.2)	14 (51.9)	20 (74.1)
	Total	8 (29.6)	19 (70.4)	27 (100.0)

Table 7.23 – Contacting an independent organisation accuracy differences

Just over one fifth (22.2%) of participants disagreed that they could find the information required to answer question five with ease for both the standardised prototype and typical format. This is shown in table 7.24. Furthermore, ten (37%) individuals felt they neither agreed or disagreed that they could locate the answer to question five with ease for the typical format while in comparison one third of participants strongly agreed with the same statement for the standardised prototype. On average, participants felt that the standardised prototype (mean: 3.63; SD: 1.28) allowed them to locate the answer to question five with more ease compared to the typical format (mean: 3.04; SD: 1.06). A paired samples t-test determined that the mean difference between policy formats (0.59; 95% CI -0.03 – 1.22) was not statistically significant (t=1.955; df=26; p=0.061).

Table 7.25 shows that sixteen (59.2%) participants agreed to some extent that the that they could locate the answer to question five quickly using the standardised prototype although only nine (33.3%) individuals felt the same way about the typical format. Similar proportions for both policies (25.9% for the standardised prototype and 29.6% for the typical format) disagreed to some extent that they could find the answer to question five quickly. Moreover, close to four fifths (37.0%) of participants neither agreed or disagreed that they could locate the answer to question five quickly for the typical format. On average participants felt that the standardised prototype (mean: 3.56; SD: 1.31) allowed them to locate the information required to answer question five quicker than the typical format (mean: 3.11; SD: 1.05). A paired samples t-test determined that the mean difference between policy formats (0.44; 95% CI -0.19 – 1.08) was not statistically significant (t=1.442; df=26; p=0.161).

Statement 5a and 5c: I could locate the information required to answer question five with ease.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	2 (15.4)	1 (7.7)	1 (3.7)	2 (7.4)
D	3 (21.4)	3 (21.4)	3 (23.1)	3 (23.1)	6 (22.2)	6 (22.2)
N	2 (14.3)	5 (25.7)	5 (38.5)	2 (15.4)	4 (14.8)	10 (37.0)
A	3 (21.4)	4 (28.6)	3 (23.1)	4 (30.8)	7 (25.9)	7 (25.9)
St A	6 (42.9)	2 (14.3)	0 (0.0)	3 (23.1)	9 (33.3)	2 (7.4)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	3.86	3.36	3.86	3.36	3.63	3.04
SD	1.23	1.01	1.23	1.01	1.28	1.06

Table 7.24 - Contacting an independent organisation post-task perceived ease of use responses

Statement 5b and 5d: I could locate the information required to answer question five quickly.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	1 (7.1)	0 (0.0)	1 (7.7)	1 (7.7)	2 (7.4)	1 (3.7)
D	2 (14.3)	2 (14.3)	5 (38.5)	3 (23.1)	5 (18.5)	7 (25.9)
N	1 (7.1)	5 (35.7)	5 (38.5)	3 (23.1)	4 (14.8)	10 (37.0)
A	4 (28.6)	4 (28.6)	2 (15.4)	4 (30.8)	8 (29.6)	6 (22.2)
St A	6 (42.9)	3 (21.4)	0 (0.0)	2 (15.4)	8 (29.6)	3 (11.1)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	3.86	3.57	2.62	3.23	3.56	3.11
SD	1.35	1.02	0.87	1.24	1.31	1.05

Table 7.25 - Contacting an independent organisation post-task perceived efficiency responses

7.4.6 Cumulative Task Accuracy

The total number of correct answers for individual participants was calculated. Table 7.26 shows that over half (51.9%) of the participants answered all five questions correctly for both policies. The mean number of accurate responses was slightly higher for the standardised prototype policy (4.41) compared to the typical policy (4.26). A paired samples t-test determined that the mean difference (0.15; 95% CI -0.16 to 0.45) between policies was not statistically significant (t=1.00; df= 26; p=0.33). An independent t-test determined that the mean difference between groups one and two (0.19; 95% CI -0.36 to 0.75) for the prototype policy was not statistically significant (t=0.71; df=25; p=0.48). Similarly, the mean difference between groups one and two (0.83; 95% CI -0.56 to 0.97) for the typical policy was not statistically significant (t=0.55; df=25; p=0.57). This indicated that the order in which participants viewed the policy did not have a significant effect on the mean number of correct responses.

Cumulative correct	SP (%)	T (%)
1	0 (0.0)	0 (0.0)
2	0 (0.0)	2 (7.4)
3	3 (11.1)	3 (11.1)
4	10 (37.0)	8 (29.6)
5	14 (51.9)	14 (51.9)
Total	27 (100.0)	27 (100.0)
Mean	4.41	4.26
SD	0.70	0.94

Table 7.26 - Cumulative accuracy

7.5 Post-Study Responses

After completing tasks one to five participants responded to eleven post-study statements. For each statement participants provided separate responses for the standardised prototype policy and the typical format policy. The same five-point Likert statement used to record post-task responses was used to record post-study responses. Post-study statements relating to perceived ease of use are presented first followed by post-study statements about perceived efficiency. The response tables for each statement are presented in the same format as the post-task responses. A paired samples t-test was performed to determine whether there was a statistically significant mean difference between policy formats for each post-study statement relating to perceived ease of use and perceived efficiency. The final part of this section presents the findings for statements relating to the standardisation of privacy policies.

7.5.1 Perceived Ease of Use

Table 7.27 shows that over 85% of participants agreed to some extent that the standardised prototype was easy to use. In comparison, just under 60% of individuals felt the same way about the typical format. On average participants felt that the standardised prototype (mean: 3.93; SD 0.62) allowed them to locate the information with more ease than the typical format (mean: 3.41; SD 0.80). A paired t-test determined that the mean difference between formats (0.52; 95% CI 0.15 – 0.89) was statistically significant (t=2.881; df=26; p=0.008).

Statement six: The privacy policy was easy to use.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
D	0 (0.0)	2 (14.3)	3 (23.1)	1 (7.7)	1 (3.7)	5 (18.5)
N	2 (14.3)	3 (21.4)	3 (23.1)	1 (7.7)	3 (11.1)	6 (22.2)
A	10 (71.4)	9 (64.3)	7 (53.8)	10 (76.9)	20 (74.1)	16 (59.3)
St A	2 (14.3)	0 (0.0)	0 (0.0)	1 (7.7)	3 (11.1)	0 (0.0)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	4.00	3.50	3.31	3.85	3.93	3.41
SD	0.56	0.76	0.86	0.69	0.62	0.80

Table 7.27 - Easy to use post study responses

Table 7.28 highlights that almost 90% of participants agreed to some extent that the prototype layout was uncomplicated compared to just over 40% for the typical format. On average participants felt that the layout of the typical format (mean: 3.26; SD 1.06) was not as straightforward as the standardised prototype (mean: 4.30; SD: 0.91). A paired samples t-test determined that the mean difference between formats (1.04; 95% CI 0.47 – 1.60) was statistically significant (t=3.776; df=26; p=0.001).

Statement eight: The privacy policy layout was straightforward.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	1 (7.1)	0 (0.0)	2 (15.4)	0 (0.0)	1 (3.7)	2 (7.4)
D	0 (0.0)	2 (14.3)	1 (7.7)	0 (0.0)	0 (0.0)	3 (11.1)
N	1 (7.1)	3 (21.4)	8 (61.5)	1 (7.7)	2 (7.4)	11 (40.7)
A	4 (28.6)	7 (50.0)	1 (7.7)	7 (53.8)	11 (40.7)	8 (29.6)
St A	8 (57.1)	2 (14.3)	1 (7.7)	5 (38.5)	13 (48.1)	3 (11.1)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	4.29	3.64	2.85	4.31	4.30	3.26
SD	1.14	0.93	1.07	0.63	0.91	1.06

Table 7.28 – Layout was straightforward post study responses

Table 7.29 shows that almost 90% of participants agreed to some extent that the headings were signposted clearly for the prototype while just over 50% of individuals responded the same way for the typical format. In comparison five (18.5%) participants felt that they disagreed to some extent that the typical format headings were signposted clearly while only one (3.7%) participant felt the same way about the standardised prototype. On average participants felt that the headings were more clearly signposted for the standardised prototype (mean: 4.44; SD: 0.80) compared to the typical format (mean: 3.52; SD 1.22). A paired samples t-test determine that the mean difference between formats (0.93; 95% CI 0.36 – 1.50) was statistically significant (t=3.343; df=26; p=0.003).

Statement ten: The privacy policy headings were signposted clearly.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	2 (15.4)	0 (0.0)	0 (0.0)	2 (7.4)
D	1 (7.1)	0 (0.0)	3 (23.1)	0 (0.0)	1 (3.7)	3 (11.1)
N	1 (7.1)	5 (35.7)	3 (23.1)	1 (7.7)	2 (7.4)	8 (29.6)
A	3 (21.4)	5 (35.7)	2 (15.4)	5 (38.5)	8 (29.6)	7 (25.9)
St A	9 (64.3)	4 (28.6)	3 (23.1)	7 (53.8)	16 (59.3)	7 (25.9)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	4.43	3.93	3.08	4.46	4.44	3.52
SD	0.94	0.83	1.44	0.66	0.80	1.22

Table 7.29 – Headings were signposted clearly post study responses

Findings in table 7.30 show that almost three quarters of individuals agreed to some extent that the standardised prototype was simple to use compared to just under 45% for the typical policy. Overall 37% of participants neither agreed or disagreed that the typical format was simple to use while just under 19% of individuals felt the same about the standardised prototype. On average participants felt that the standardised prototype (mean: 3.89; SD: 0.97) was simpler to use compared to the typical format (mean: 3.30; SD: 1.17). A paired samples t-test determined that the mean difference between formats (0.59; 95% CI 0.21 – 0.98) was statistically significant (t=3.171; df=26; p=0.004).

Statement twelve: The privacy policy was simple to use.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	1 (7.1)	2 (15.4)	1 (7.7)	1 (3.7)	3 (11.1)
D	1 (7.1)	0 (0.0)	2 (15.4)	0 (0.0)	1 (3.7)	2 (7.4)
N	2 (14.3)	5 (35.7)	5 (38.5)	3 (23.1)	5 (18.5)	10 (37.0)
A	5 (35.7)	5 (35.7)	3 (23.1)	8 (61.5)	13 (48.1)	8 (29.6)
St A	6 (42.9)	3 (21.4)	1 (7.7)	1 (7.7)	7 (25.9)	4 (14.8)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	4.14	3.64	2.92	3.62	3.89	3.30
SD	0.95	1.08	1.19	0.96	0.97	1.17

Table 7.30 – Policy was simple to use post study responses

7.5.2 Perceived Efficiency

Table 7.31 highlights that over 80% of participants agreed to some extent that the standardised prototype allowed them to locate the information quickly. On the other hand, just over 55% of individuals responded in the same way for the typical format. Participants felt that the standardised prototype (mean: 3.96; SD 0.81) allowed them to locate information quicker than the typical format (mean: 3.41; SD 0.75). A paired samples t-test determined that the mean difference between formats (0.56; 95% CI 0.07 – 1.04) was statistically significant (t=2.367; df=26; p=0.026).

Statement seven: The privacy policy could be used to find information quickly.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
D	1 (7.1)	0 (0.0)	4 (30.8)	1 (7.7)	2 (7.4)	4 (14.8)
N	2 (14.3)	5 (35.7)	3 (23.1)	1 (7.7)	3 (11.1)	8 (29.6)
A	9 (64.3)	9 (64.3)	6 (46.2)	7 (53.8)	16 (59.3)	15 (55.6)
St A	2 (14.3)	0 (0.0)	0 (0.0)	4 (30.8)	6 (22.2)	0 (0.0)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	3.86	3.64	3.15	4.08	3.96	3.41
SD	0.77	0.50	0.90	0.86	0.81	0.75

Table 7.31 - Locating information quickly post study responses

Findings presented in table 7.32 show that over 85% of participants agreed to some extent that they understood where to find the answers for questions one to five when using the standardised prototype while approximately 55% of individuals felt the same way when using the typical format. In contrast, six (22.2%) participants disagreed to some extent that they understood where to look to locate the answer to questions one to five when using the typical format while zero individuals provided the same type of response for the standardised prototype. On average participants felt that they understood where they needed to look to locate the answers to questions one to five more so using the standardised prototype (mean: 4.15; SD: 0.66) than the typical format (mean: 3.33; SD: 0.96). A paired samples t-test determined that the mean difference between formats (0.82; 95% CI 0.47 – 1.16) was statistically significant (t=4.818; df=26; p<0.001).

Statement nine: I understood where I needed to look to find information when answering questions one to five.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	1 (7.7)	0 (0.0)	0 (0.0)	1 (3.7)
D	0 (0.0)	2 (14.3)	3 (23.1)	0 (0.0)	0 (0.0)	5 (18.5)
N	2 (14.3)	2 (14.3)	4 (30.8)	2 (15.4)	4 (14.8)	6 (22.2)
A	7 (50.0)	9 (64.3)	5 (38.5)	8 (61.5)	15 (55.6)	14 (51.9)
St A	5 (35.7)	1 (7.1)	0 (0.0)	3 (23.1)	8 (29.6)	1 (3.7)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	4.21	3.64	3.00	4.08	4.15	3.33
SD	0.70	0.84	1.00	0.64	0.66	0.96

Table 7.32 - Understood where I needed to look post study responses

Similar proportions of participants agreed that they could answer questions one to five efficiently using both the standardised prototype (44.4%) and the typical format (40.7%). This is shown in table 7.33. However, the results from the user study show that almost 35% of individuals strongly agreed that questions one to five could be answered efficiently using the standardised prototype while just under 15% of participants felt the same way about the typical format. On average participants felt that they could answer questions one to five with more efficiency using the standardised prototype (mean: 4.04; SD: 0.90) compared to the typical format (mean: 3.52; SD: 1.01). A paired samples t-test determined that the mean difference between formats (0.52; 95% CI 0.15 – 0.89) was statistically significant (t=2.881; df=26; p=0.008).

Statement eleven: I could use the privacy policy efficiently to answer questions one to five.						
	Group					
	1		2		Overall	
Ans.	SP (%)	T (%)	T (%)	SP (%)	SP (%)	T (%)
St D	0 (0.0)	0 (0.0)	1 (7.7)	0 (0.0)	0 (0.0)	1 (3.7)
D	1 (7.1)	1 (7.1)	2 (15.4)	1 (7.7)	2 (7.4)	3 (11.1)
N	2 (14.3)	4 (28.6)	4 (30.8)	2 (15.4)	4 (14.8)	8 (29.6)
A	6 (42.9)	6 (42.9)	5 (38.5)	6 (46.2)	12 (44.4)	11 (40.7)
St A	5 (35.7)	3 (21.4)	1 (7.7)	4 (30.8)	9 (33.3)	4 (14.8)
Total	14 (100.0)	14 (100.0)	13 (100.0)	13 (100.0)	27 (100.0)	27 (100.0)
Mean	4.07	3.79	3.23	4.00	4.04	3.52
SD	0.92	0.89	1.09	0.91	0.90	1.01

Table 7.33 - I could use the privacy policy efficiently post study responses

7.5.3 Standardisation

Findings in table 7.34 revealed over four fifths (81.4%) of individuals either agreed or strongly agreed that it was a good idea to have a summary privacy policy on all websites while zero participants disagreed. Moreover, almost 50% of individuals stated that they strongly agreed that it is a good idea to have a consistent summary page across websites and just over 40% agreed with the same statement. The results also show than zero participants disagreed that it was a good idea to have a summary page with a similar look and feel across websites.

Statement 13: It would be a good idea to have a summary policy page on all websites.			
	Group		
Ans.	1 (%)	2 (%)	Overall (%)
St D	0 (0.0)	0 (0.0)	0 (0.0)
D	0 (0.0)	0 (0.0)	0 (0.0)
N	3 (21.4)	2 (15.4)	5 (18.5)
A	7 (50.0)	6 (46.2)	13 (48.1)
St A	4 (28.6)	5 (38.5)	9 (33.3)
Total	14 (100.0)	13 (100.0)	27 (100.0)
Mean	4.07	4.23	4.15
SD	0.73	0.73	0.72
Statement 14: It would be a good idea to have a summary policy page that has a consistent look and feel across all websites.			
St D	0 (0.0)	0 (0.0)	0 (0.0)
D	0 (0.0)	0 (0.0)	0 (0.0)
N	1 (7.1)	2 (15.4)	3 (11.1)
A	6 (42.9)	5 (38.5)	11 (40.7)
St A	7 (50.0)	6 (46.2)	13 (48.1)
Total	14 (100.0)	13 (100.0)	27 (100.0)
Mean	4.43	4.31	4.37
SD	0.65	0.75	0.69

Table 7.34 - Summary standardisation post study responses

Table 7.35 shows that over 70% of the twenty-seven participants strongly agreed that privacy policies should have a consistent look and feel them and just under 30% of individuals agreed. In addition, seventeen (62.9%) out of the twenty-seven user study participants either disagreed or strongly disagreed that websites should publish privacy policies that are presented differently. In contrast eight individuals agreed to some extent that websites should offer variety in the way they publish their privacy policies.

Statement 15: It would be a good idea to have privacy policies that have a consistent look and feel across all websites.			
	Group		
Ans.	1 (%)	2 (%)	Overall (%)
St D	0 (0.0)	0 (0.0)	0 (0.0)
D	0 (0.0)	0 (0.0)	0 (0.0)
N	0 (0.0)	0 (0.0)	0 (0.0)
A	3 (21.4)	5 (38.5)	8 (29.6)
St A	11 (78.6)	8 (61.5)	19 (70.4)
Total	14 (100.0)	13 (100.0)	27 (100.0)
Mean	4.79	4.62	4.70
SD	0.43	0.51	0.47
Statement 16: I would like websites to offer variety in the way in which they present their privacy policies.			
St D	1 (7.1)	5 (38.5)	6 (22.2)
D	7 (50.0)	4 (30.8)	11 (40.7)
N	1 (7.1)	1 (7.7)	2 (7.4)
A	1 (7.1)	3 (23.1)	4 (14.8)
St A	4 (28.6)	0 (0.0)	4 (14.8)
Total	14 (100.0)	13 (100.0)	27 (100.0)
Mean	3.00	2.15	2.59
SD	1.47	1.21	1.39

Table 7.35 - Privacy policy standardisation responses

7.6 Summary

This chapter presented the findings of a usability study involving twenty-seven participants. Research results are summarised in table 7.36. The purpose of the usability study was to address research questions six, seven and eight. Research question six was: **do users feel the standardised prototype privacy policy is easier to use than a typical privacy policy?** Post-task data showed that users believed that they could locate information with more ease when using the standardised prototype for all tasks with tasks one, two and three revealing significantly better findings. Post-study results followed the same trend. Findings revealed that participants felt that the standardised prototype privacy policy was easier to use that the typical privacy policy. Furthermore, users agreed that the layout was more straightforward for the prototype and the standardised prototype was simpler to use.

Research question seven was: **do users feel the standardised prototype privacy policy can be used to retrieve information more efficiently than a typical privacy policy?** Post-task findings highlighted that participants felt that information could be located more quickly using the prototype compared to the typical format for all tasks. Tasks one, two and three proved to be significantly better for the prototype compared to the typical privacy policy when considering how quickly users felt they could locate information. In addition, post-study data showed that participants felt that the prototype could be used to locate information more quickly and efficiently than the typical policy and that the headings were signposted more clearly within the standardised prototype.

Finally, research question eight was: **do users support the idea of a standardised format privacy policy like the standardised prototype design?** Users showed strong support for the publication of a consistent privacy policy summary page. Participants also felt that privacy policies should have a consistent look and feel across websites.

		Mean		Difference
	Statement	SP	T	P<0.05(✓) P<0.01(✓✓)
1a 1c	I could locate the information required to answer question one with ease.	3.96	3.52	✓
1b 1d	I could locate the information required to answer question one quickly.	3.78	3.26	✓
2a 2c	I could locate the information required to answer question two with ease.	4.07	3.22	✓
2b 2d	I could locate the information required to answer question two quickly.	4.11	3.00	✓✓
3a 3c	I could locate the information required to answer question three with ease.	4.19	3.52	✓✓
3b 3d	I could locate the information required to answer question three quickly.	4.19	3.26	✓✓
4a 4c	I could locate the information required to answer question four with ease.	4.37	4.22	✘
4b 4d	I could locate the information required to answer question four quickly.	4.41	4.19	✘
5a 5c	I could locate the information required to answer question five with ease.	3.63	3.04	✘
5b 5d	I could locate the information required to answer question five quickly.	3.56	3.11	✘
6	The privacy policy was easy to use.	3.93	3.41	✓✓
7	The privacy policy could be used to find information quickly.	3.96	3.41	✓
8	The privacy policy layout was straightforward.	4.30	3.26	✓✓
9	I understood where I needed to look to find information when answering questions 1 to 5.	4.15	3.33	✓✓
10	The privacy policy headings were signposted clearly.	4.44	3.52	✓✓
11	I could use the privacy policy efficiently to answer questions 1 to 5.	4.04	3.52	✓✓
12	The privacy policy was simple to use.	3.89	3.30	✓✓

Table 7.36 - Summary of format statements

Chapter 8 - Discussion

8.1 Introduction

The aim of this research was to explore how UK e-commerce privacy policies could be improved. In this chapter the findings from phases one to four are synthesised to identify how UK e-commerce privacy policies could be improved. The first section in this chapter reflects on UK e-commerce privacy policies based on the evidence presented in this research. In this section findings from this study are compared with existing studies. The second section of this chapter takes the evidence gathered in this study and explores how UK e-commerce privacy policies could be improved. In this section, evidence presented in phases one to four are integrated to identify practical changes that could improve UK e-commerce privacy policies in the short, medium and long term.

8.2 The As Is: Reflections on UK e-commerce Privacy Policies

The purpose of this section is to review the findings of this research in relation to existing knowledge. Barriers to readership are analysed along with cues that individuals use to infer fair processing. Compliance with good practice and third-party data sharing descriptions are reviewed considering findings from previous studies and more recent changes in the personal data processing environment.

8.2.1 Readership Blockers

This study found several barriers that indicate why UK e-commerce privacy policies are ignored. Privacy policies take a long time to read (McDonald and Cranor, 2008). Consistent with the literature review, users were critical of privacy policy length. It was evident that the convenient nature of e-commerce and the desire for quick transactions would be compromised because of the perceived amount of time it would take users to read a privacy policy. Regulators have called for privacy policies to be made shorter (Federal Trade Commission, 2012) and Article 12 of the GDPR (European Parliament and Council, 2012) states that information provided to the data subject should be concise in nature. That said, policy length and comprehensiveness were points of contention in this study. Some users considered the longer privacy policy viewed in phase two to be more comprehensive. The longer privacy policy also disclosed more information considered as good practice. The perception from some users was that the comprehensive nature of the privacy policy invoked feelings of perceived subject knowledgeability, competence and trust. This was in direct contrast to the shortest privacy policy reviewed in phase two. Some users questioned the legitimacy of the organisation producing the shorter policy while others debated whether personal data would be held securely or whether the organisation publishing the policy was trustworthy.

On the one hand, the findings support Lauer and Deng's (2007) information privacy policy and online trust model. They found that a privacy policy publishing fair information practices increased perceptions of ability, benevolence and integrity. In this study the organisation publishing the privacy policy that disclosed more information considered as good practice was perceived to be more competent. Furthermore, the organisation publishing the policy that disclosed less information considered as good practice was perceived as being less trustworthy. On the other hand, the findings raise an important point in relation to the guidance that privacy policies should be shorter in length (Federal Trade Commission, 2012). While it is not possible to distinguish whether the perceptions of comprehensiveness were determined by the length of the policy or by the number of good practice guidelines disclosed within the privacy policy, organisations that publish a shorter privacy policy without considering good practice risk being perceived as untrustworthy and incompetent. Trust is an important concept in e-commerce because it is strongly associated with behavioural intention (McKnight, Choudhury and Kacmar, 2002). Companies need to strike a balance between publishing a privacy policy that discloses all the relevant information in a comprehensive way while considering that a lengthy privacy policy may well reduce consumer desire to read the policy.

Some users cited that they felt privacy policies are the same across websites. Burbules (1998, p. 109) coined the term: "levelling effect". He believed that the behaviour of the mainstream media and quantity of information available on the internet would create a level playing field where authors have the same level of credibility. Doing so, Burbules (1998) contends, discouraged reflection on the credibility of information. The "levelling effect" might go some way towards explaining some consumer beliefs that privacy policies "are all the same." The repeatability and familiarity of e-commerce processes probably influence attitudes in this area. Perhaps customers have become so familiar with the *same purchasing process* across websites, they feel that the privacy policies are also likely to be *the same* across websites. Breaking down the purchasing process also provokes thought. Focus group findings showed privacy policies are synonymous with “that tick box”. If consumers are familiar with the same square tick box to indicate consent across websites and the same wording to ask them to “consent” to the privacy policy across websites, it could also be logical for them to believe that the privacy policy is indeed the same across websites.

The consistency heuristic (Metzger, Flanagin and Medders 2010) might also offer insight. The consistency heuristic posits that consumers will seek to verify the believability of a source by checking the consistency of a message across websites. If consumers perceive messages to be consistent across websites, they may believe that the privacy policies are, on the face of it, the same. Consumers following the same process consistently on different websites and only ever seeing the term “privacy policy” (and not the contents of the privacy policy) when they are asked to agree to the processing practices the organisation could underpin the perception that privacy statements are the same. This finding has implications for improvements to privacy policies and is discussed more in section 8.3.2.6.

The format of privacy policies is also a barrier to readership. Privacy policies in small text appear to deter consumers from wanting the read a privacy policy. Searching for and retrieving information was perceived to be more difficult with the privacy policy that did not include headings. In addition, there was a perception that the privacy policy with no subheadings was unprofessional. Locating information was considered to be easier in those policies that provided headings.

8.2.2 My Right to Be Informed or Your Responsibility to Inform?

Phase two showed that there is a perception among some consumers that privacy policies serve the needs of organisations. Several consumers believed that the reason organisations publish a privacy policy is to protect corporate interests and fulfil legal obligations. In one sense, the observation that there is an obligation on organisations to inform consumers about personal data processing is correct. On the other hand, there was little evidence to suggest that consumers believe policies are published to inform them, the consumer, about personal data processing. This was a surprising finding that perhaps goes some way to explain low levels of privacy policy readership. The timing of data collection could have influenced this finding. The GDPR has placed the spotlight on data subject rights and now the collective requirements under Articles 12, 13 and 14 of the GDPR are recognised as the “right to be informed”. While 52% of people living in the UK state that they are aware of the right to be informed (Harris Interactive, 2018), it is not clear how consumers operationalise this belief. Do consumers know that organisations publish privacy policies to inform them about personal data processing practices? This study would suggest the contrary applies for some individuals. Instead, privacy policies are seen by some as the responsibility of the organisation and not necessarily a source of information for the user.

8.2.3 Privacy (Probably): Cues Outside the Policy

In complex situations humans will simplify the decision-making process by using heuristics (Acquisti et al 2017). Chapter five introduced the concept of privacy proxies. Privacy proxies are synonymous with cues in the environment that consumers use to infer fairness. Acquisti, Brandimarte and Loewenstein (2015, p. 509) state that: “because people are often “at sea” when it comes to the consequence of, and their feelings about, privacy, they cast around for cues to guide their behaviour.” Evidence in this study highlighted that cues influence user beliefs about fairness, legitimacy and security. The cues found in this research can be linked to heuristics. Heuristics are signals that consumers use to estimate the probability of an event. For example, participants used website reviews to infer that a website was legitimate, and this could be explained by the endorsement heuristic. Table 8.1 shows which heuristic is offered as an explanation of each cue found in this study.

Fairness, legitimacy and security cues	Heuristic (Metzger, Flanagin and Medders, 2010)
Perceived professionalism of the website design	Expectation violation heuristic
The media	N/A
Website reviews	Endorsement heuristic
Website familiarity	Reputation heuristic
Brand awareness	
Website popularity	

Table 8.1 – Heuristics used to explain fairness, legitimacy and security cues.

Research has shown that the visual appeal of a website influences perceptions of privacy assurance. Lowry et al (2012) found that increases in the perceived quality of a website increases the perception that customers feel that personal data is protected. In this research some users stated they inferred website legitimacy from the look and feel of a website. It could be that users feel that considerable resource and emphasis has been placed on the development of a visually appealing and professional looking website and therefore the same amount of effort is also placed on ensuring that personal data is processed fairly (Lowry et al 2012). However, this cue is open to exploitation. The visual cues that appear to represent credibility on a website can be subject to deception, particularly in the case of phishing where websites are purposely designed to mimic credible resources (Dhamija, Tygar and Hearst, 2006).

Some users expected to be notified of a privacy or security breach. With this in mind some users will (a) rely on information being pushed to them about breaches of privacy or security and (b) use this information to make an inference about a website. User reliance on this cue could be potentially damaging. Users might see or hear media reports of a privacy or security breach after transacting with a website. In this case, personal data may have already been processed by an organisation in a way the user deemed unfair. On the other hand, seeing or hearing a media report of a breach prior to purchasing goods or services could influence future purchasing decisions. Lowry et al (2012) found that perceived privacy assurance decreases after a user is exposed to negative media coverage.

Website reviews were also a cue that users rely on to guide privacy related behaviour. Consumers felt that comments left by other shoppers on comparison websites help to determine perceived legitimacy. The endorsement heuristic posits that: “people are inclined to believe information and sources if others do so, without much scrutiny of the site content or source” (Metzger and Flanigan, 2013, p. 215). For consumers, the time saved reading a review in comparison to reading a privacy policy is consistent with the desire for convenience and speed. Consumers find that reviews are helpful up to a threshold of 144 words (Huang et al, 2015). In this sense, it would be much quicker to read several reviews than it would be to read a privacy policy with an average word length of one thousand seven hundred words (Fabian, Ermakova and Lentz 2017).

It is interesting to note the involvement of people when considering website reviews. When consumers are looking at website reviews, they are reviewing content that someone else has produced. This suggests there could be a social element to privacy cues. Moreover, collective responses about the behaviour of others appeared elsewhere in this study. For example, one user described her experience of using clothing retailer ASOS. She said: “millions of people use them, why would they not have a secure policy?”. She was implying that ASOS would provide appropriate security measures because millions of other people use the website to purchase clothes. In addition, when discussing privacy policy readership, there was a collective element to several responses noting that “people don’t want to read them” and “no one reads them”. Participants appeared to be guiding their beliefs on the perceived actions of others.

Website familiarity, brand awareness and website popularity were other cues that were evident in participant responses. An organisation that was perceived to be “bigger” was considered by one participant as having more resource available to protect security. Furthermore, because some brand names were recognised and considered “high street names”, they were perceived as more trustworthy. The reputation heuristic offers further insight on these perceptions. Where users are familiar with a website or brand, they avoid the: “effortful processing of online sources of information” (Metzger and Flangin 2013, p. 214). Consumers may well perceive that the risk of a privacy breach following the disclosure of personal data to a familiar or recognised website to be small. That said, the assumption that popular retailers provide a more secure platform does not always prove true. Telecommunications organisation TalkTalk received a £400,000 fine from the Information Commissioner’s Office (2016c) in 2016 after the organisation were deemed to have abdicated their security obligations. British Airways (BBC News, 2018) and Tesco Bank (Financial Conduct Authority, 2018) have also been the subject of recent personal data breaches.

8.2.4 Information Disclosure: (Non) Compliance

Organisations should be transparent about the processing of personal data (Information Commissioner’s Office, 2018c). Information disclosure is a dimension of transparency (Schnackenberg and Tomlinson, 2016). Phase one of this study measured disclosure of good practice.

8.2.4.1 Data Controller Identity and Purposes for Processing

Most organisations that publish a privacy policy tend to describe why personal data is processed (Schwaig, Kane and Storey, 2006; Hooper and Vos, 2009; Cha, 2011). UK B2C e-commerce privacy polices followed this trend. Over 95% of policies in this study stated the purpose or purposes for which personal data will be processed.

Furthermore, over 95% of privacy policies in 2012 and 2015 described a purpose or purposes for using cookies. The amendments to the Privacy and Electronic Communications (EC Directive) Regulations 2003 in 2012 would likely have prompted organisations to review cookie disclosures. This would appear an explanation to the high proportion of privacy policies describing why cookies are used.

This research adopted two ways of accepting that a privacy policy stated the identity of a data controller. The first was methodologically strong; policies were reviewed to understand whether the data controller was *explicitly* identified. In most cases, that involved the policy stating the terms “data controller”. The second way of identifying the data controller was methodologically weaker and involves inferring the identity of the data controller based on the named organisations stated in the policy. Almost 30% of privacy policies explicitly identified that controller in 2015 (a statistically significant increase from approximately 20% in 2012). An explicit description of data controller identity is a clearer way to inform a reader about whom the data controller is. Recent research seems to complement the need for a change in this area. L’Hoiry and Norris (2015) reported that in 71% of cases it took researchers in the UK over five minutes or more to locate the identity of the data controller when reviewing websites. As the authors of the study describe, content can be buried deep inside privacy policies adding complexity and time to locate the data controller identity. An explicit statement would go some way towards addressing this issue.

8.2.4.2 Data Subject Rights

The disclosure of information about the right to view a copy of personal data was higher than reported in the literature. Over 60% of websites from the United States (Cha, 2011) and New Zealand (Tjhin, Vos and Managanuri 2016) mentioned that users could access or review personal data. This study found that 72% of privacy policies stated that it was possible to view personal data in 2015. That said, the explicit communication of the existence of data subject rights was poor in UK e-commerce privacy policies. Findings evidenced some significant improvement between 2012 and 2015 however explicit disclosure of the existence of rights, particularly the right to amend inaccurate personal data, remove inaccurate personal data and prevent personal data being used for direct marketing, was very low.

User awareness of data subject rights is mixed. Over half of people living in the UK state that they know about the right to access personal data (Harris Interactive, 2018), however, not all consumers will understand their rights in relation to personal data, neither will they necessarily know how to put them into practice. The Annual Track survey published by the Information Commissioner in 2018 shows that almost two thirds of people living in the UK disagree that it is easy for them to find out how personal information is stored and used by organisations (Harris Interactive, 2018). Informing data subjects that they can access personal data being processed or telling data subjects that it is their right to access personal data being processed is different from describing *how* a data subject could go about exercising the right to access personal data. The Article 29 Working Party (2018b, p. 39) recognise this; they state that the information provided to the data subject should describe: “what the right involves and how the data subject can take steps to exercise it.” In 2015, almost 40% of privacy policies did not outline how personal data could be accessed or amended. The same logic, albeit to a lesser extent, applied to the communication of the right to prevent personal data being used for direct marketing; just under one quarter of UK e-commerce privacy policies did not highlight how to exercise this right. The lack of clearly signposted procedures for exercising subject access rights may well increase the time taken for a data subject to understand how rights can be exercised, leading to frustration and ultimately the abandonment of requests (L’Hoiry and Norris (2015).

8.2.4.3 Placing the Obligation on the Data Subject

This study found three areas of information disclosure where privacy policies performed very poorly. In 2015 there was no evidence of organisations informing data subjects that they could contact the ICO to complain about the processing of personal data. Furthermore, in the same year, under 5% of privacy policies described a specific length of time for which personal data will be retained; this is a considerably lower proportion compared to previous work (Mundy 2006; Beldad, De Jong and Steehouder, 2009). Along with this, only one in five UK e-commerce privacy policies mentioned when the privacy policy was last updated. The lack of disclosure in these areas places the obligation on the data subject to take further steps to obtain the desired policy information. Even though consumers may seek information about the currency of information online on an occasional basis (Flanagin and Metzger, 2000; Metzger, 2007) it is still important to state when the policy became effective or was last updated. Without this information, it is only the organisation that knows when the privacy policy was last updated. If personal data handling processes had changed between two points in time, a data subject would be forced to contact an organisation to understand if and perhaps more importantly what had changed since previously transacting with a business. The effort invested in seeking out this information could lead to the individual abandoning any attempt to do so.

8.2.4.4 Data Sharing Descriptions

Terms such as “may”, “might”, “from time to time” and “occasionally” can be found extensively in privacy policies (Pollach, 2005; Bhatia et al, 2016). Findings showed that users associated these terms with dishonesty. There was a sense that organisations were not being truthful about their personal data sharing intentions. On the one hand, using modal verbs such as “may” and “might” offers the organisation flexibility. In one sense, the organisation has disclosed that they could potentially share personal data with a third party. If, at the time of publishing the privacy policy, the organisation does not share personal data, they could potentially do so in the future without informing the data subject. The benefit for the organisation is that they would not have to reach out to the data subject each time the policy changed. That said, as Pollach (2005) rightly described, terms such as “may” and “might” provide little assurance to the data subject. Data subjects can only be left with uncertainty about whether personal data will be shared. At the time of disclosing personal data users will not know whether personal data will be shared. Furthermore, at any point beyond the disclosure of personal data, users will be in the same position. This has been recognised by the Article 29 Working Party (2018b, p. 8); they state that information provided to the data subject: “should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations.” One user felt that the use of modal verbs provided little trust. This should be important to organisations given the clearly evidenced association between trust and behavioural intention.

The uncertainly around personal data sharing is confounded further by the names of organisations that are published within privacy policies. The content analysis of privacy policies showed that the most common terms used to describe data sharing recipients were: “select third parties”, “carefully selected third parties”, “third parties” and “carefully selected companies”. In phase two, users pointed out the lack of clarity associated with these types of descriptions. These terms provided users with no insight into who personal data is or might be shared with. Moreover, the terms are associated with perceived deception and untrustworthiness. While the descriptions might be designed to give the impression that organisations have placed time and effort in considering who personal data is shared with, in reality, users do not believe this. The terms used, again, maximise the flexibility of organisations. The broad nature of the terms could include a host of organisations, some of which the user may object to if he or she were to become aware that disclosure was going to occur. The obligation, again, is placed on the data subject to seek information. Should the data subject wish to understand the name of the organisation that personal data is shared with, they have no choice but contact the organisation to obtain this information.

The Data Sharing Code of Practice published by the Information Commissioner stated that organisations could state the names of organisations that personal data is shared with or the “types of organisation” (Information Commissioner’s Office, 2011). The important distinction is that organisations should do one *or* the other. Only a small handful of organisations (three in 2012 and 2015) chose to state the name of an organisation. The introduction of the GDPR has changed the responsibility of organisations in relation to these descriptions. Article 13 of the GDPR (European Parliament and Council, p.41) states that organisations must now state the “recipients or categories of recipients” of personal data. The *or* distinction is still present, however the Information Commissioner’s Office (2018) has advised that organisations should be as specific as possible while the Article 29 Working Party (2018b, p. 37) has said that “in practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data.” In light of these changes, this is an area that organisations will have to address.

8.2.4.5 Policy Format

Consistent with the findings of Langhorne (2014), no evidence of layered privacy policies was found in 2012 or 2015. If organisations have analytics data to show that consumers rarely visit privacy policies, they may believe that investment in designing and implementing layered privacy policies is unjustified. Additionally, organisations might be unsure about how a layered policy should be constructed or what information should go into each layer. In 2010, good practice guidelines (Information Commissioner’s Office, 2010) did show an example of a layered policy, however there was little guidance around the design approach that would shape the publication of a layered notice. Summary findings from the ICO’s consultation on privacy notices suggests that organisations would like more prescriptive layered policy guidance (Information Commissioner’s Office, 2016b). From a consumer perspective phase two of this study highlighted the importance of the visual appeal of a privacy policy. Users seek a clear structure when locating personal data processing information which can be achieved by separating content using clearly labelled headings.

8.2.4.6 The Transition of the Data Protection Act 1998 to the General Data Protection Regulation 2016

Overall findings showed that privacy policies do no consistenty follow good practice guidelines. A compliance index containing 15 good practice guidelines was developed. Privacy policies followed a mean of 6.34 guidelines in 2012 rising to a mean of 6.91 guidelines in 2015. The change between 2012 and 2015, while statistically signficant, was small. In both 2012 and 2015, privacy policies followed under 50% of good practice guidelines in the compliance index. Reviewing the legislation at the time of data collection offers further insight into the findings of this study. Schedule One of the Data Protection Act 1998 placed the obligation on data controllers to provide four information points. The first requirement was to communicate the identity of the data controller, the second was to state a nominated representative (if such a representative existed), the third was to inform the data subject about the purpose or purposes of processing and the fourth was to provide any further information necessary for fair processing. Was the description of “any further information which is necessary” (Parliament, 1998, p. 49) for fair processing too broad for organisations to interpret? Good practice guidance was clearly available (Information Commissioner’s Office, 2010), however findings from the cumulative count of good practice compliance shows the guidelines were not consistently followed. This leads to a second point of contention; were organisations aware of the good practice guidelines published by the Information Commissioner? Statistics published by the Information Commissioner showed that the *Privacy Notices Code of Practice* was not in the list of top ten requested publications in 2013 (Information Commissioner’s Office, n.d). This does bring into question whether organisations knew that such a code existed. If organisations were unaware of the guidance, the small increase in good practice compliance between 2012 and 2015 suggests that awareness of the code may not have changed between those dates.

The lack of incentivisation to follow good practice may also explain why good practice is not consistently followed. Cranor (2012) attributed the lack of incentives to the failure of P3P. Organisations may well have been aware of good practice guidelines although they may have felt insufficiently incentivised to go beyond stating the identity of the data controller and a providing a description of the purposes for processing personal data. This could be a reason why organisations performed poorly in other areas of fair processing. The incentive to follow what was recognised as good practice has now changed with the introduction of the GDPR. Explicit recognition of data subject rights and other areas of fair processing under Articles 13 and 14 of the GDPR has changed the information requirements for organisations. Compliance with GDPR is now the incentive to change and the reason why the timing of evidenced based improvements is particularly important.

8.3 How Could Privacy Policies be Improved?

This section outlines how UK e-commerce privacy policies could be improved based on the evidence gathered in this research. Short, medium and long-term improvements are described.

8.3.1 Short Term: Compliance and Nudging

In the immediate short-term organisations should focus attention on achieving GDPR compliance and they should also seek to implement the privacy nudges described.

8.3.1.1 GDPR Information Requirements

Almost three in five individuals from the UK believe that businesses are not transparent about the processing of personal data (Citizenme, 2016). Informational gaps were found that will need to be addressed to ensure GDPR compliance. On the evidence presented in this study every UK e-commerce organisation will need to review their privacy policy, however some businesses will need to address more areas than others. Along with other information requirements outlined in Articles 13 and 14 of the GDPR, organisations will have to address the following gaps to ensure GDPR compliance:

- Article 13(1)(e): The recipients or categories of recipients of personal data;
- Article 13(2)(a): Information about the personal data retention period, or details of how a retention period will be calculated;
- Article 13(2)(c): Information about data subject rights including the right to access, rectify and erase personal data along with the right to data portability and the right to object to processing;
- Article 13(2)(d): Information about the right to lodge a complaint to the supervisory authority.

In this study data sharing descriptions were inadequate and created a sense of uncertainly among participants. Organisations should focus on two areas, firstly the use of modal verbs such as “may” and “might”. Article 12 of the GDPR (European Parliament and Commission, 2016, p. 39) states that personal data information should be provided using “clear and plain” language and the Article 29 Working Party (2018b) has stated that modal verbs should be avoided. Concrete and definite language qualifiers should be used. Data sharing descriptions should outline whether personal data will or will not be shared. This approach will not provide organisations with as much flexibility as was previously available. This change will however provide more clarity for data subjects and reduce the uncertain nature of these descriptions.

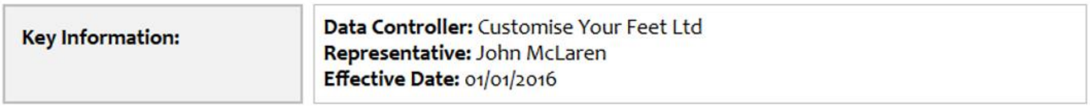
The second element of data sharing descriptions that businesses should address involves the descriptions of recipients of personal data. The name of the organisation personal data is being shared with should be provided in the first instance (Article 29 Working Party, 2018b). Where a named organisation cannot be provided, categories of recipients must be specific (Article 29 Working Party, 2018b). In consideration of this guidance, organisations will have to be more specific when describing who personal data is shared with. It would seem unlikely that the broad descriptions found in this study give any meaningful insight to end users.

8.3.1.2 Nudging Users in the Right Direction

A privacy nudge is intended to improve the design of a system by taking into account human biases that can lead to negative outcomes (Acquisti et al 2017). Presentation and information are dimensions of nudges. Acquisti et al (2017, p. 12) state that a presentational nudge: “provides necessary contextual cues in the user interface to reduce cognitive load and convey the appropriate level of risk,” while an informational nudge: “reduces information asymmetries and provides a realistic perspective of risks.” The privacy nudges presented in the following sections are a blend of presentation and informational nudges. Based on the principle of user centricity, the aim of the nudges is to help guide users into making better decisions. To that end, because the nudges are user informed they are consistent with the principle of user centricity required to achieve privacy by design. For organisations, the nudges identified are not designed to be onerous to implement. They are considered to be lightweight changes that could be implemented in the short term.

8.3.1.2.1 Explicitly Defining the Data Controller and Data Subject Rights

The Article 29 Working Party (2018) state that the right to object to processing should be *explicitly* brought to the data subjects’ attention, however explicit recognition should be extended to other information areas. The identity of the data controller and the applicable data subject rights should be explicitly outlined in a privacy policy. An extract from the proposed standardised prototype shown in figure 8.1 demonstrates how explicit recognition could be operationalised in the context of the identity of the data controller. Stating the term “data controller” should ensure that the identity of the data controller is clear to the data subject. Furthermore, privacy policies should explicitly state that it is the right of the data subject to access, rectify or erase personal data. Using the terms “you have the right to” or “it is your right” should render it more obvious to the data subject that they are legally permitted to ask the data controller to carry out certain requests regarding personal data. L’Hoiry and Norris (2015) showed the difficulties associated with identifying the data controller. This study has provided a practical suggestion to address this.



Key Information:

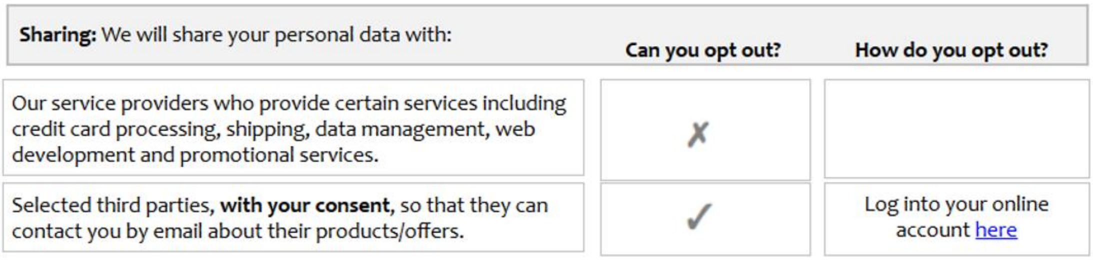
Data Controller: Customise Your Feet Ltd
Representative: John McLaren
Effective Date: 01/01/2016

Figure 8.1 - Explicit data controller identity

8.3.1.2.2 Bringing Choice and Access to the Notice

Some users believe that they do not have a choice in relation to the personal data processing practices of an organisation. However, there are elements of personal data processing where consumers do have choices, for example the sharing of personal data with third parties for direct marketing purposes. If consumers perceive they do not have a choice and therefore do not read a privacy policy, they may be unaware of any choices they do have. In light of this, choices should not be buried within a privacy policy. It should be more obvious to users that they have a choice regarding personal data processing. Not only that, but users should be able to action the choice they have from the privacy policy. Phase three showed that a graphical depiction of choice in the form of a tick or cross was a simple and effective way to indicate choice. Findings from phase four provided further support. Question one in the usability study asked users if they could prevent their personal data being used to send them information about products and services. Question three in the usability study asked users to determine if their personal data might be shared for direct marketing purposes. Both questions involve an element of choice. Users showed more agreement that they could locate the information required to answer question one and three with ease when using the policy design shown in figure 8.2 compared to a typical privacy policy. Furthermore, users perceived that they could locate the information required to answer question one and three with more efficiency when using the design in figure 8.2.

Findings suggest that the tabular design along with the use of ticks and crosses enables efficient information retrieval. The inclusion of instructions on how to log into an account within the tabular design also provides a method for users to exercise choice where they have the option to do so. Implementing this approach addresses the information gap found in phase one where some privacy policies described the right to object to processing but did not state how this right could be exercised. It is suggested that organisations adopt the approach outlined in figure 8.2 to communicate personal data processing choices.



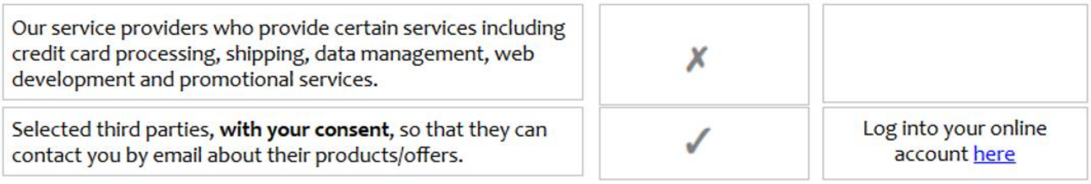
Sharing: We will share your personal data with:	**Can you opt out?**	**How do you opt out?**
Our service providers who provide certain services including credit card processing, shipping, data management, web development and promotional services.	✗	
Selected third parties, **with your consent**, so that they can contact you by email about their products/offers.	✓	Log into your online account here

Figure 8.2 - Bringing choice to the notice

The principle of ensuring that choice is made clearer to users should also be extended to personal data access. Organisations should ensure that there is a mechanism in place that will enable the data subject to know how to exercise their right to access a copy of personal data. L'Hoiry and Norris (2015) state that a standard template should be published in a privacy policy that would allow a data subject to submit a subject access request. The main point is that data subjects should be able to begin the process of subject access request from within the privacy policy. The obligation should not be placed on the data subject to perform further searches or contact the organisation by telephone (as was the case in L'Hoiry and Norris (2015)) to locate relevant information. To satisfy this, a link to an online workflow could be placed within the privacy policy. The workflow would direct the user to input the relevant personal data required to perform the request. The user should be able to progress through the workflow to complete the subject access request or come back to the request at a later point in time. Once submitted, feedback should be provided on the status of the request. An acknowledgement letter is one way to provide feedback (L'Hoiry and Norris 2015). A system status indicating the progress of the request followed by timely email updates could also be used to keep the data subject updated. Recent reports have suggested the number of subject access requests have increased following the introduction of the GDPR (Ram and Murphy, 2018). An online workflow initiated from within a privacy policy would seem to be a useful suggestion to help organise and manage these requests.

8.3.1.2.3 Emphasising Consent

Phase two showed that users feel reassured and comfortable when they are made aware that personal data will only be processed with consent. With this in mind, situations where consent is sought prior to personal data processing should be emphasised within the privacy policy. In the usability study two thirds of participants correctly noticed that personal data would be shared with another organisation with the consent of the user. It should be made clear that the emphasis on consent is not the mechanism that organisations should use to obtain consent from data subjects. Consent “must be distinguishable from other matters” (Article 29 Working Party, 2018a, p. 14) and therefore stating that consent is gained without actually obtaining consent is an ambiguous indication of the data subject’s agreement. The purpose of the emphasis within the privacy policy is to reinforce that consent will be gained prior to processing.

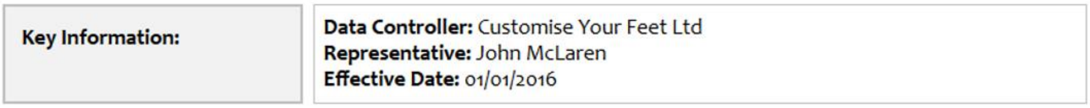


Our service providers who provide certain services including credit card processing, shipping, data management, web development and promotional services.	✗	
Selected third parties, **with your consent**, so that they can contact you by email about their products/offers.	✓	Log into your online account here

Figure 8.3 – Emphasising consent within privacy policies

8.3.1.2.4 Information About Policy Updates

All privacy policies should disclose when the privacy policy was last updated. This improvement addresses the finding that four fifths of privacy policies did not mention when the privacy policy was last updated. The date should be placed at the start of the privacy policy in a noticeable position. The summary layer of the standardised prototype privacy policy included a date as part of the key information. This is shown in figure 8.4. Furthermore, the date of last update should not be limited to the privacy policy. Organisations should also place a date of last update outside the privacy policy. The literature showed that most people do not read privacy policies. This study found the privacy policies are synonymous with “that tick box” at the end of an online transaction. Where organisations are asking data subjects to read the privacy policy, they should also state when the privacy policy was last updated. This will indicate to the data subject whether the privacy policy has been updated. Better still, organisations are likely to know the date that a product or service was last purchased from the account the consumer is using to purchase a product or service. Organisations could then calculate if the privacy policy has been updated since the last time that the user transacted. Notifying the user that the privacy policy has been updated after that previous transaction took place may well prompt the user to read the privacy policy. Providing a date of last update at the point of transaction is also in the spirit of openness and fairness. Being up front about when a privacy policy was last updated and taking steps to ensure users are made aware is consistent with the principle of transparency outlined in the GDPR and the concept of user centricity needed to achieve privacy by design.

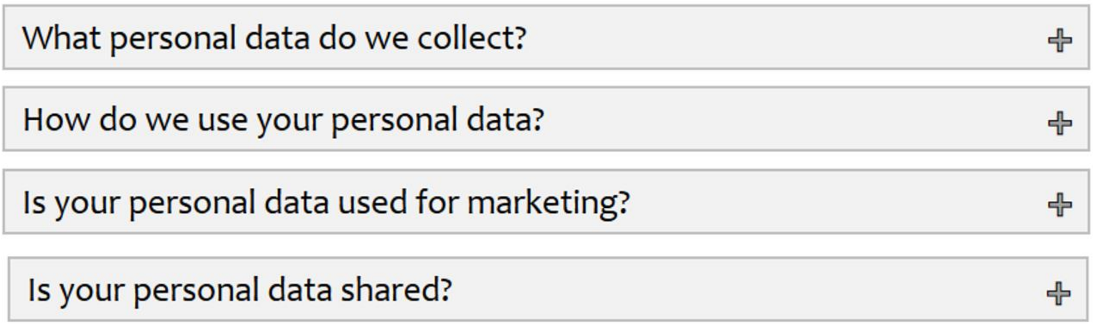


Key Information:	**Data Controller:** Customise Your Feet Ltd **Representative:** John McLaren **Effective Date:** 01/01/2016

Figure 8.4 - Date of last update

8.3.1.2.5 Making the Audience More Obvious

Evidence in this study showed that users are not necessarily aware that the purpose of a privacy policy is to inform them about organisational personal data processing practices. In consideration of this finding, efforts should be made to indicate to users that privacy policies are documents that are intended to provide information for their benefit. Phase three showed that users preferred headings framed as questions, as shown in figure 8.5. Consistent with guidance from the Article 29 Working Party (2018b) organisations should provide headings in the form of natural language questions. Natural language headings are perceived as being friendlier and more inviting. Moreover, Lauer and Deng (2007) showed that perceptions of trust increase where organisations are perceived as showing benevolence. Question two of the usability study asked users if the privacy policies provided any links to external websites about cookies. Participants would have had to use the full cookie policy with the natural language headings to locate the answer to this question. The same proportion of participants answered the question correctly for the typical privacy policy and the standardised layered prototype privacy policy. However, perceptions of locating the answer to this question were significantly different. Participants felt that it was easier to locate the information required to answer this question and that they could locate the answer more efficiently with the standardised prototype. In addition, users in phase four agreed that natural language headings were signposted clearly. Given that users in phase three pointed out the perceived benefits of natural language questions and participants in phase four would have had to use these questions to retrieve information, it would be logical to suggest that that natural language headings contributed towards perceptions of ease of use and efficiency. With this in mind natural language question headings not only play a role in altering perceptions of the policy audience but also perceptions of policy ease of use and efficiency.



What personal data do we collect? +

How do we use your personal data? +

Is your personal data used for marketing? +

Is your personal data shared? +

Figure 8.5 - Natural language question headings

8.3.2 Medium Term: Format Standardisation

In the medium-term efforts should focus on the development of a standard format privacy policy. In this study, a prototype layered privacy policy has been developed that could be standardised. Cranor (2012) states that the format of a standardised privacy policy should be uniform. There may be some scope for customisation although the aim of a standardised privacy policy should be to prevent format inconsistency. This study adds to the calls for standardisation by showing that e-commerce consumers support privacy policy format standardisation. Findings from phase four demonstrated that consumers agreed that privacy policies should be consistently formatted across websites. Moreover, consumers felt that both a summary and full privacy policy should also have a consistent look and feel.

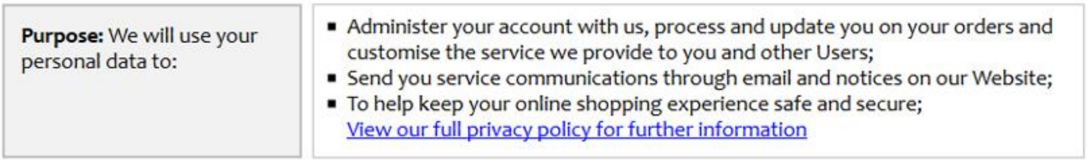
During phase three a standardised prototype layered privacy policy was developed. Results from phase four showed that the layered prototype privacy policy was considered easier to use than a typical UK e-commerce privacy policy. Moreover, phase four findings demonstrated that users believed that they could locate information with more efficiency when using the layered prototype privacy policy compared to a typical UK e-commerce privacy policy. The presentation format of the prototype privacy policy could be adopted as a standard form. This section summarises the guiding principles of the standardised layered prototype privacy policy.

8.3.2.1 Consistent Format

The consistent presentation of information underpins the principle of privacy policy standardisation. The layered approach developed in this study could be adopted across UK e-commerce websites. The Hunton and Williams (2006) layered privacy policy was criticised for being too flexible (Cranor, 2006; Kelley et al, 2010). The standardised layered prototype developed in this study is more prescriptive than the Hunton and Williams (2006) layered privacy policy and therefore does not offer the same level of flexibility. The presentation format of the summary layer would remain identical across UK e-commerce websites. The same eight categories of information would be provided in the summary layer; these categories are: key information, purpose, marketing, sharing, transferring personal data outside the EEA, security, cookies and questions. Each information container should provide no more than five bullet points of information. Container widths are fixed to limit the amount of information that can be presented in the summary layer. Each information container should provide a link to the full privacy or cookie policy. The format of the full privacy and full cookie policies would also remain the same across websites. Accordion controls would be used to show or hide policy information. UK e-commerce organisations would have some autonomy to change the headings in the full privacy and full cookie layer should they wish. Any amendments to the headings should follow the natural language questioning style.

8.3.2.2 Signposting Information

Phase two showed that consumers desire convenience and speed when making e-commerce purchasing decisions and therefore it is important that users feel that they can retrieve policy information quickly. Consistent with research showing that users spend more time looking at the left-hand side of a webpage (Fessenden, 2017), headings in the summary layer are placed on the left-hand side and encapsulated in containers, as shown in figure 8.6. This structured approach is beneficial for users; phase four showed that users felt that information could be located more quickly using the prototype privacy policy compared to the typical privacy policy. Furthermore, users perceived that the headings in the prototype privacy policy were more clearly signposted compared to the headings in the typical privacy policy.

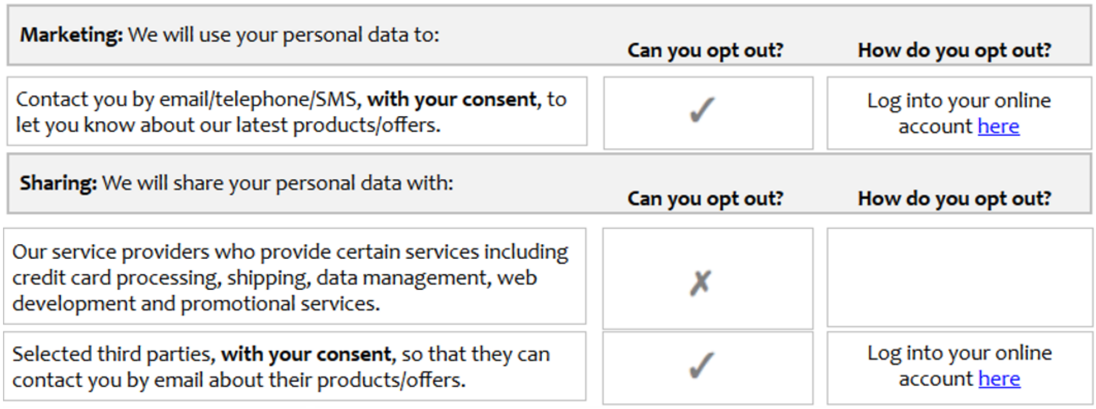


Purpose: We will use your personal data to:	▪ Administer your account with us, process and update you on your orders and customise the service we provide to you and other Users; ▪ Send you service communications through email and notices on our Website; ▪ To help keep your online shopping experience safe and secure; View our full privacy policy for further information

Figure 8.6 - Encapsulated headings

8.3.2.3 Retrieval and Action in the Summary Layer

The summary layer is important in a layered privacy policy because it is the first point at which a user will have the opportunity to view personal data processing information. Beyond providing meaningful information, the layout of the summary in the prototype privacy policy facilitates choice, as shown in figure 8.7. In instances where personal data is shared with another organisation, or where personal data is used for direct marketing, users can retrieve relevant information and act accordingly based on their beliefs. This is advantageous when compared to a typical UK e-commerce privacy policy because in a typical UK e-commerce privacy policy a user would have to search the full privacy policy to locate the appropriate information. In phase two users stated their willingness not to have to read considerable amounts of text. E-commerce users should not only view the layered prototype as a source of information; it should be viewed as an area where choices and decisions can be made.

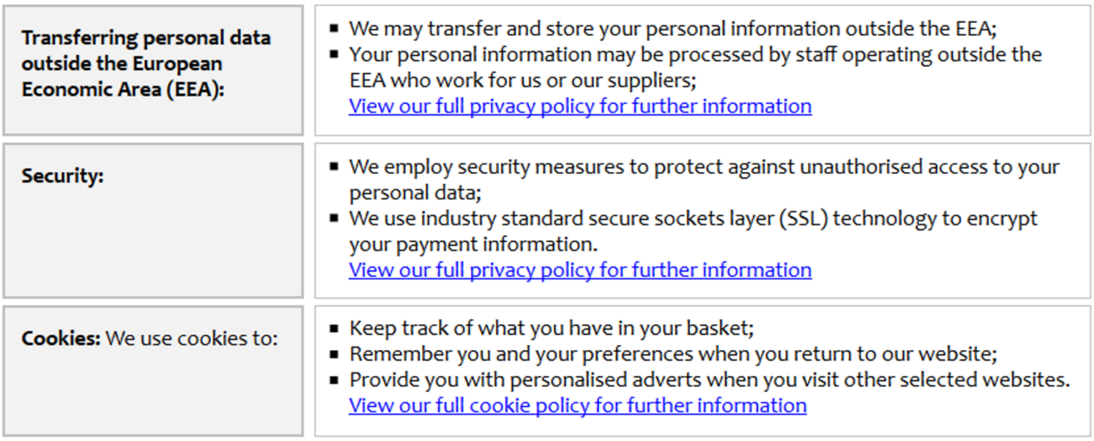


Marketing: We will use your personal data to:	**Can you opt out?**	**How do you opt out?**
Contact you by email/telephone/SMS, **with your consent**, to let you know about our latest products/offers.	✓	Log into your online account here
Sharing: We will share your personal data with:	**Can you opt out?**	**How do you opt out?**
Our service providers who provide certain services including credit card processing, shipping, data management, web development and promotional services.	✗	
Selected third parties, **with your consent**, so that they can contact you by email about their products/offers.	✓	Log into your online account here

Figure 8.7 - Retrieval and action in the summary layer

8.3.2.4 Providing Relevant Information

The summary layer is useful to users because it provides meaningful information. The data controller identity is obvious addressing the calls outlined in L'Hoiry and Norris (2015). Almost 80% of individuals living in Great Britain are concerned about organisations using personal data without permission (Bartlett, 2012). A similar proportion of individuals stated they were worried about personal data being sold to third parties (Bartlett, 2012). To that end, the reasons for personal data processing are outlined along with how personal data is shared. The transfer of personal data outside the EEA and information about cookies are described in the summary layer. Phase two and three showed that users were unaware that personal data may be processed outside the EEA. Phase three also showed that users were not aware about cookie usage. The purpose of including information about EEA transfers and cookies is to bring to light information that users do not know about. Rao et al (2016) found that user beliefs about personal data processing practices were not always reflected in privacy policies. It is hoped that highlighting those practices that users do not know about will begin to broaden awareness of the range of personal data handling practices and ultimately inform decision making. The theft of personal data was found to be the most prominent processing concern of people living in the UK in 2018 (Harris Interactive, 2018). For that reason, security information was included within the summary layer, as shown in figure 8.8. The full privacy and cookie layers should disclose the relevant information outlined in Articles 13 and 14 of the GDPR and Article 6 of the Privacy and Electronic Communications (EC Directive) Regulations.



Transferring personal data outside the European Economic Area (EEA):	▪ We may transfer and store your personal information outside the EEA; ▪ Your personal information may be processed by staff operating outside the EEA who work for us or our suppliers; View our full privacy policy for further information
Security:	▪ We employ security measures to protect against unauthorised access to your personal data; ▪ We use industry standard secure sockets layer (SSL) technology to encrypt your payment information. View our full privacy policy for further information
Cookies: We use cookies to:	▪ Keep track of what you have in your basket; ▪ Remember you and your preferences when you return to our website; ▪ Provide you with personalised adverts when you visit other selected websites. View our full cookie policy for further information

Figure 8.8 - Meaningful information in the summary layer

8.3.2.5 Simplicity and Device Neutrality

While the layered prototype offers simplicity for users, it should also be simple for organisations to implement. Developing and testing the HTML and CSS files that are required to display the prototype layered privacy policy should not be onerous. HTML and CSS are widely recognised languages that are used to develop web pages. Furthermore, making changes to the summary or full privacy or cookie policies should not be time consuming. For example, should future research demonstrate that user personal data processing expectations change, the information within the summary layer could be easily amended. In this study the layered prototype privacy policy was developed and tested on a desktop machine. The summary and full layers could be adapted for use on mobile devices. This however, would require further research with the aim of testing a standardised layered privacy policy that was device neutral.

8.3.2.6 What Next for Format Standardisation? Some Considerations for Further Research

Findings from the usability study in phase four showed that the prototype layered privacy policy performed well across several different usability metrics. Although the standardised layered format was perceived by participants to facilitate efficient information retrieval, significant differences were only found in three of the five post task questions users responded to. In question four participants were asked whether personal data might be sent outside the European Economic Area. In the standardised layered prototype policy, the information required to answer this question was in the summary layer. For that reason, it was expected that participants would feel that locating the answer to this question would be easier and quicker using the standardised prototype compared to the typical privacy policy, however the findings were not statistically significant. In phases two and three individuals expressed some concern about the practice of transferring personal data outside the EEA. It could be that users' non-significant levels of perceived ease of use and efficiency were observed because the answer to the question was in the first sentence of the "Transfers Outside of the European Economic Area" section in the typical privacy policy. Therefore, participants may have believed that locating the answer to question four was just as easy using the typical UK e-commerce privacy policy.

For question five, participants were asked: based on the policies can you contact an independent organisation and complain about the processing of your personal data? Perceived ease of use and perceived efficiency differences were not statistically significant. One might have expected a difference between policies because the answer to the question five could be found in the summary layer of the prototype layered privacy policy. The typical privacy policy did not provide the option to contact the Information Commissioner and therefore participants would have had to spend more time searching for the relevant information. The finding could be explained by fatigue. This was the final question in the usability study where users were expected to seek information from the policy.

At this stage, the policy designed in this study is considered a prototype. The findings do suggest that further research should be carried out to explore how participants use the layered prototype privacy policy. More specifically further knowledge efforts should be dedicated towards evaluating the standardised prototype in light of the concepts of clarity, accessibility and conciseness that are outlined in Article 12 of the GDPR. Focusing research efforts in this area will further determine the suitability of the proposed layered privacy policy considering the requirements of the GDPR. In addition, assessing the degree to which data subjects can successfully compare policy information between different websites using the same standardised format will add data to refute or support the effectiveness of the proposed format.

The principles outlined in the consistency heuristic (Metzeger and Flanagin, 2013) should also be considered. Phase two highlighted that some individuals feel that privacy policies are the same across websites. A consistently presented privacy policy may further reinforce the perceptions that privacy policies are the same. An educational program should be developed to highlight any changes in format and why such changes are necessary. The Information Commissioner could play a central role in disseminating information about format standardisation to data subjects.

Edwards and Abel (2014) and Cranor (2012) point out that to achieve critical mass organisations need an incentive to adopt the standardised format privacy policy. The introduction of the GDPR and the principle of transparency are important factors here. The GDPR has placed much more emphasis on personal data processing transparency. In some respects, we are at a critical point. Both the European Data Protection Board (formally the Article 29 Working Party) and the Information Commissioner's Office support the publication of layered privacy policies and advise organisations to publish privacy notices using a layered format. If it could be demonstrated that the standardised layered privacy policy developed in this study provided better transparency than a typical privacy policy, then organisations would be incentivised to publish the layered privacy policy to demonstrate GDPR compliance. The same logic applies to trust. If the layered prototype privacy policy was considered to be more trustworthy than a typical privacy policy, organisations may well be incentivised to implement the notice format. The European Data Protection Board (formally the Article 29 Working Party) and the Information Commissioner's Office will need to assess the suitability of the standardised prototype.

8.3.3 Long Term: Measuring Policy Effectiveness

In this research a methodology has been developed to evaluate the content of UK e-commerce privacy policies. The methodology provides researchers with tools to investigate the degree to which privacy policies comply with GDPR information requirements. However, the approach taken is labour intensive and based on human annotation of privacy policies. While the current research has been taking place, efforts have focused on natural language processing of privacy policies. Polisis (2017) and The Usage Privacy Project (2017) are examples of these developments. These natural language engines automate the annotation of privacy policies significantly reducing the amount of time taken to highlight and group statements that are of interest. Harkous et al (2018) have already pointed out the potential application of Polisis to the GDPR. Natural language processing could be applied to UK e-commerce privacy policies with a view to assessing privacy policies using the content analysis questions developed in phase one. Asking the specific questions of privacy policies, like, 'does the privacy policy explicitly mention the identity of the data controller?' and automating responses could provide benefits for regulators and organisations.

Organisations could receive feedback highlighting areas of compliance weakness and or an overall compliance score. This specific and personalised feedback for each privacy policy could result in good practice guidance being provided to organisations based on the findings highlighted by the natural language processor. Providing actionable feedback could incentivise organisations to make changes to privacy policies. Regulators would also benefit from such an approach. Data could be more easily gathered about privacy policies with a view to identifying compliance trends. Comparisons can be made between and within industry sectors and general or specific guidance could be provided. Moreover, changes over time can be measured. That said, the role that organisations play in provision of meaningful privacy policy information should not be overlooked. While artificial intelligence solutions hold promise for the future this research has shown a simple and effective means of disclosing relevant information without the need to rely on complex and expensive machine learning solutions.

8.4 Summary

This chapter has outlined how UK e-commerce privacy policies could be improved based on the integration of findings from research phases one to four. In the first section of the chapter, the characteristics of UK e-commerce privacy policies found in this study were compared to existing knowledge. Barriers to readership are described and cognitive heuristics are shown to be a possible explanation for inferences made about personal data processing fairness. Information gaps in UK e-commerce privacy policies are highlighted and compared to previous studies. In the second section of this chapter, short, medium and long-term suggestions for improvement to privacy policies were made. In the short term it is suggested that UK e-commerce organisations focus efforts on achieving compliance with the GDPR. In addition, several easy to implement privacy nudges were described. In the medium term, attention should shift towards the privacy policy format standardisation. The prototype layered privacy policy developed in this study could be standardised across UK e-commerce websites. Findings demonstrate perceived ease of use and perceived efficiency were significantly better for the prototype layered privacy policy in comparison to a typical UK e-commerce privacy policy. In the longer term, efforts should turn towards measuring policy effectiveness using artificial intelligence solutions.

Chapter 9 - Conclusion and Recommendations

9.1 Introduction

The aim of this research was to **explore how UK e-commerce privacy policies could be improved.** A multiphase mixed method approach was used to address the research aim. Seven research questions were devised. Four research phases were carried out with each phase addressing one or more research questions. Below, each research question is revisited, and the findings of each question are summarised. Following this, recommendations for improvement are made based on the outcomes from research phases one to four. This chapter concludes by outlining contributions of this research and the potential direction of future work.

9.2 Addressing the Research Questions

Research question one was: to what extent do UK e-commerce privacy policies follow good practice guidelines?

Findings from two content analysis studies showed that UK e-commerce privacy policies do not consistently follow good practice guidelines. A good practice index was created. An average of 6.34 guidelines out of fifteen were followed in 2012. The average number of guidelines followed by organisations increased to 6.91 in 2015. While the increase between 2012 and 2015 proved statistically significant, policies were found to follow under half of the fifteen good practice guidelines measured in the index. Findings highlighted specific informational requirements that now need to be addressed following the introduction of the GDPR in May 2018. The inconsistent publication of good practice guidelines places an increased obligation on the user to seek out further information. In this sense, more effort is required to uncover the personal data processing practices of an organisation.

Research question two was: why do e-commerce users ignore UK e-commerce privacy policies?

Focus group findings described in section 5.3 showed eight reasons why privacy policies are ignored. Evidence suggested that some consumers do not feel that they will be able to understand privacy policies (1). In addition, when purchasing products online there is an overwhelming desire for convenience and for many users the weight of this desire was greater than the perceived need to read a privacy policy (2). Policy length (3), policy format (4) and language (5) were all barriers to readership. Moreover, evidence shows that some users do not feel privacy policies are aimed at them (6) and that they feel they have a limited choice in respect of privacy policies (7). Finally some participants felt that privacy policies are the same across websites (8). The results of the focus groups also highlighted the presence of “privacy proxies”. Privacy proxies are sources other than the privacy policy that users rely on to infer that personal data will be processed fairly. These cognitive shortcuts are utilised when information processing becomes complex. Users infer trust and legitimacy from the perceived size of an organisation, familiarity with a website, customer reviews, media reports and the perceived professionalism of the website design.

Research question three was: what do e-commerce users feel are the positive and negative characteristics of UK e-commerce privacy policies?

Users have different perceptions about the comprehensiveness of privacy policies. Comprehensive privacy policies are perceived by some as being more helpful than incomprehensive statements. A comprehensive privacy policy was considered by some to be more trustworthy and legitimate than a privacy policy that did not follow good practice guidelines. The organisation publishing a privacy policy that did not follow good practice guidelines was perceived to be less competent. References to legislation were viewed as a signal of professionalism and legitimacy. Typical personal data sharing descriptions were associated with dishonesty. The processing of personal data outside the EEA was treated with some suspicion. Moreover, evidence suggested that users felt frustrated where the onus was placed on them to opt out of personal data sharing. The positive and negative characteristics of privacy policies were used to generate prototype design objectives in phase three.

Research question four was: how useful is the standardised prototype?

In phase three, a prototype layered privacy policy was produced using design objectives extracted from the findings of phase two. The first iteration prototype was reviewed by the researcher. The second iteration prototype was evaluated by e-commerce users. Focus group findings underpinned the changes made to the second iteration prototype. Users preferred policy headings to be framed as natural language questions. Furthermore, accordion controls were considered to be an effective way to present information. A third iteration prototype was examined in phase four.

Research question five was: do users feel the standardised prototype privacy policy is easier to use than a typical privacy policy?

Usability study results showed statistically significant ease of use differences between the prototype layered privacy policy and a typical privacy policy. Policy information could be located with more ease with the prototype layered privacy policy. Furthermore, the prototype privacy policy layout was considered simpler to use and the layout was perceived to be more straightforward.

Research question six was: do users feel the standardised prototype privacy policy can be used to retrieve information more efficiently than a typical privacy policy?

Usability study findings revealed that users felt that retrieving information was quicker using the prototype privacy policy. In addition, results showed that users believed the headings within the prototype privacy policy were more clearly signposted and users believed that information could be located more effectively using the prototype policy.

Research question seven was: do users support the idea of a standardised format privacy policy like the standardised prototype design?

Post task usability study results showed that users were in support of a consistent looking privacy policy summary page. E-commerce users also supported the publication of privacy policies in a consistent format.

9.3 Recommendations for Improvement

In chapter eight the outcomes of each research question were synthesised to suggest how privacy policies could be improved. Based on the suggestions, nine recommendations are made. The recommendations should be used by practitioners seeking to improve existing privacy policies. In addition, the recommendations should also be used by organisations seeking to achieve privacy by design. The practical guidance sets out steps that organisations can take to improve the transparency and user centricity of privacy policies.

9.3.1 Organisations should review privacy policies to ensure compliance with information requirements of the GDPR

This research has shown that UK e-commerce privacy policies do not consistently follow good practice guidelines. These information gaps have become more important because of the increased transparency obligations placed on organisations following the introduction of the GDPR. For that reason, organisations should review privacy policies to ensure that the information requirements outlined in Articles 13 and 14 of the GDPR are disclosed to users. Based on the evidence found in this study, careful attention needs to be paid to data sharing descriptions, the communication of data subject rights, personal data retention periods and the right to contact a supervisory authority.

9.3.2 Data sharing descriptions should be more specific

Data sharing descriptions are very broad. Terms such as “carefully selected third parties” offer the organisation disclosing personal data flexibility at the expense of the user because it is impossible to determine who personal data is shared with. Similar descriptions were found across the spectrum of UK e-commerce privacy policies. Furthermore, modal verbs such as “may” or “might” that can be found extensively in privacy policies (Pollach 2005; Bhatia et al 2016) leave the consumer with much uncertainty and are associated with perceived dishonesty. To that end, organisations should be more specific about who personal data is shared with. Privacy policies should state the names of the organisations that personal data is shared with (Article 29 Working Party, 2018). This will be an ongoing process. Privacy policies should be updated accordingly as and when changes to data practices occur or if the names of partner organisations change over time. The use of modal verbs creates uncertainty and should also be avoided.

9.3.3 Privacy policies should explicitly state (a) the identity of the data controller and (b) the rights of the data subject

Previous work has highlighted that privacy policies are unclear (Bhatia et al 2016) and more recently L’Hoiry and Norris (2015) showed the practical challenges associated with obtaining the identity of the data controller. Very few privacy policies in this study explicitly stated that identity of the data controller. To ensure that identifying the data controller is straightforward, privacy policies should explicitly state the name of the data controller. Explicit statements of data subject rights should also be included within privacy policies.

9.3.4 Privacy policies should include mechanisms to achieve choice and access

Two in five UK e-commerce privacy policies did not state how users can access a copy of personal data. Additionally, just under one quarter of UK e-commerce privacy policies did not describe how to prevent personal data being used for direct marketing. Users highlighted that they felt they did not have a choice in respect to privacy policies. To help overcome this and address the informational gap in relation to exercising data subject rights, privacy policies should ensure that choice and access can be achieved from within the privacy policy. The use of ticks and crosses within a tabular design is an easy to digest mechanism that highlights choice is possible. Furthermore, links that enable users to opt out of personal data processing from within the privacy policy should be provided. The same principle applies to accessing personal data. A link to start an online subject access request workflow is the preferable option.

9.3.5 Emphasis should be used to highlight consent

Users want to know about their choices. Evidence showed users take comfort knowing that personal data is processed with consent. Positive perceptions of trust were evident where privacy policies stated that personal data would not be shared unless consent was provided. In consideration of user perception, privacy policies should use emphasis to draw attention to statements describing that consent is obtained prior to personal data processing.

9.3.6 Every privacy policy should include a date to indicate the point in time that the policy becomes effective

Four in five UK e-commerce privacy policies did not state when the policy was last updated or became effective. Where this is the case users have no way of determining if the privacy policy has changed since the last time they transacted with the website unless the organisation has informed them directly about changes. That said, such a situation should not excuse not outlining when a privacy policy was updated. Organisations should go further than the basic requirement of disclosing when the policy was last updated within the privacy policy. Businesses should also specify when the privacy policy was last updated outside of the privacy policy. Doing so increases that chance that the user will become aware, at the point of transaction, that a change in personal data processing practices has occurred. Such a change could be inconsistent with their privacy beliefs and therefore the date that the privacy policy became effective should be published within the privacy policy and outside the privacy policy. Data Protection Officers could play an important role here. Article 39 of the GDPR outlines that tasks of a Data Protection Officer. One responsibility is to monitor compliance with the GDPR. This could include ensuing that, amongst other things, the provisions outlined in this research (such as ensuring the date of last update is included within privacy policy) are implement and monitored over time.

9.3.7 Privacy policies should be published in such a way that users perceive they are directed at them

Some users do not feel that privacy policies are aimed at them. This study found that natural language headings (Article 29 Working Party, 2018) was an effective method to help address this perception. For that reason, it should be more obvious to users of online services that a privacy policy is published to provide them with information about personal data processing. Natural language questions as policy headings are recommended to bridge the gap between the privacy policy and the intended audience.

9.3.8 The prototype privacy policy developed in this study should be used as a vehicle to explore the feasibility of privacy policy format standardisation

The prototype privacy policy developed in this study has shown encouraging findings. Users believed that they could locate the information needed to answer five personal data processing questions with more ease and more efficiency using the standardised prototype layered privacy policy. Three of these questions proved to be statistically significant in favour of the prototype layered privacy policy. In addition, post task data revealed consistently encouraging results and therefore further work should be carried out to explore whether the prototype privacy policy developed in this study could be standardised and adopted at scale.

9.3.9 Further studies should be carried out aimed at measuring the effectiveness of UK e-commerce privacy policy disclosures using natural language processing

Natural language processing of privacy policies is now being performed facilitating the annotation and visualisation of natural language privacy policies. The coding scheme developed in this study could underpin a metrics system that organisations might use to test their privacy policies using a natural language processing system.

Such a system could output a score that would determine how well privacy policies communicate the requirements of Articles 12, 13 and 14 of the GDPR. Work has already started but is at an early stage.

9.4 Outlining Research Contributions

UK e-commerce privacy policies had received little attention within the privacy policy literature prior to this study. This research has uncovered new ground in understanding the quality of information disclosed in UK e-commerce privacy policies. This knowledge is particularly useful for the regulator of personal data in the UK, the Information Commissioner's Office, and UK e-commerce organisations because it sheds light on the transparency of UK e-commerce privacy policies. From a practical standpoint this research has made a series of evidenced based recommendations that will help to improve the format and quality of information disclosed and start to address perceived shortcomings identified in this study and the literature. The findings will also be of interest to practitioners seeking to achieve privacy by design. The recommendations made offer practical, evidence based steps to help organisations produce more user centric privacy policies.

From a methodological viewpoint, this research has developed and tested a coding scheme that could be used to measure the degree to which privacy policies comply with GDPR information principles. Importantly, data has been presented that sets the foundation for future work. Findings from future UK e-commerce content analysis studies can be directly compared to the data presented in this study. This allows for an objective comparison of privacy policy content over time. Furthermore, the coding scheme can used and applied across a range of contexts, not just e-commerce.

9.5 Opportunities for Future Work

Further research should seek to establish whether a positive relationship exists between transparency in the context of personal data processing and trust. A significant positive relationship between transparency and trust may incentivise organisations to improve transparency.

Work is already under way to examine the impact of the introduction of the GDPR on privacy policies. Degeling et al (2018) found an increase in the number of websites publishing a privacy policy after the implementation of the GDPR. Following this, there also exists an opportunity post GDPR implementation to add to the data collected in this study. This study has paved the way for a third analysis of the privacy policies of those organisations included within the 2015 sample. Examination of the format and content of privacy policies using the coding scheme presented in this study would provide important insight that could be used to evaluate the impact of the GDPR. The findings of such a study could help to inform regulator policy by identifying areas of disclosure that organisations can improve.

A further set of studies should be conducted to assess the standardised prototype layered privacy policy that has been developed. Studies should aim to explore the standardised prototype in relation to the concepts outlined in Article 12 of the GDPR. A further assessment of the clarity, accessibility and conciseness of the standardised prototype will yield results that will determine the suitability of the prototype for large scale adoption. Feedback should be sought from users of varying demographic characteristics with a range of personal data processing attitudes. In addition, research exploring whether engagement with privacy policies differs according to demographic variables appears to be an under-researched area, but would be a fruitful area for further research.

Bibliography

Accenture. (2016). *The Future of Advertising*. Available at: https://www.accenture.com/us-en/~/media/Accenture/next-gen/pulse-of-media/pdf/Accenture-Future-Of-Advertising-POV.pdf. (Accessed 5 January 2019).

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Fifth ACM conference on Electronic commerce*, New York, 17-20 May, New York: ACM, pp. 21-29.

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015). Privacy and Human Behavior In the Age of Information, *Science*, 347(6221), pp. 509–514.

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y. and Wilson, S. (2017). Nudges for Privacy and Security. *ACM Computing Surveys*, 50(3), pp. 1–41.

Anthes, G. (2014). Data brokers are watching you, *Communications of the ACM*, 58(1), pp. 28–30.

Article 29 Working Party. (2004). *Opinion 10/2004 on More Harmonised Information Provisions*. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_en.pdf. (Accessed: 27 January 2019).

Article 29 Working Party. (2010). *Opinion 2/2010 on online behavioural advertising*. Available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf (Accessed: 5 August 2018).

Article 29 Working Party. (2015). *Cookie Sweep Combined Analysis*. Available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp229_en.pdf (Accessed: 7 August 2018).

Article 29 Working Party. (2018a). *Guidelines on consent under Regulation 2016/679*. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (Accessed: 5 January 2019).

Article 29 Working Party. (2018b). *Guidelines on Transparency under Regulation 2016/679*. Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (Accessed: 3 July 2018).

Bangor, A., Kortum, P. T. and Miller, J. T. (2008). An Empirical Evaluation of the System Usability Scale, *International Journal of Human-Computer Interaction*, 24(6), pp. 574–594.

Bansal, G., Zahedi, F. and Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern, *European Journal of Information Systems*, 24(6), pp. 624–644.

Barth, A. (2011). HTTP State Management Mechanism. *Internet Engineering Task Force*. Available at: https://tools.ietf.org/html/rfc6265. (Accessed 6 January 2019).

Bartlett, J. (2012). *The Data Dialogue*. Available at: https://demos.co.uk/project/the-data-dialogue/. (Accessed: 27 August 2018).

BBC News. (2018). *British Airways boss apologies for 'malicious' data breach*. Available at: https://www.bbc.co.uk/news/uk-england-london-45440850. (Access 12 January 2019).

Beldad, A. D., De Jong, M. and Steehouder, M. F. (2009). When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites, *Government Information Quarterly*, 26(4), pp. 559–566.

Berelson, B. (1952). *Content analysis in communication research*. New York: Free Press.

Bhatia, J., Breaux, T., Reidenberg, J. and Norton, T. (2016). A Theory of Vagueness and Privacy Risk Perception. *IEEE 24th International Requirements Engineering Conference (RE)*, Beijing, 12-16 September, New Jersey: IEEE, pp. 26–35.

Blaikie, N. (1993) *Approaches to Social Enquiry*. Oxford: Blackwell.

Blumer, H. (1954). What is Wrong with Social Theory? *American Sociological Review. American Sociological Association*, 19(1), pp. 3–10.

Boda, K., Foldes, A. M., Gulyas, G. G. and Imre, S. (2011). User Tracking on the Web via Cross-Browser Fingerprinting. *Sixteenth Nordic Conference on Information Security Technology for Applications*, Estonia, 26-28 October, Heidelberg: Springer, pp. 31-46.

Boerman, S. C., Kruikemeier, S. and Borgesius, F. J. Z. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda, *Journal of Advertising*, 46(3), pp. 363–376.

Borgesius, F. J. Z. (2015). *Improving privacy protection in the area of behavioural targeting*. The Hague: Kluwer Law International.

Bowker, A. H. (1948). A Test for Symmetry in Contingency Tables, *Journal of the American Statistical Association*, 43(244), pp. 572–774.

Box, G. (1979). Robustness in the strategy of scientific model building, in Launer, R. L. and Wilkinson, G. N. (eds.) *Robustness in Statistics*. London: Academic Press, pp. 201–236.

Brandeis, L. and Warren, S. (1890). The right to privacy, *Harvard Law Review*, 4(5), pp. 193–220.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology, *Qualitative Research in Psychology*, 3(2), pp. 77–101.

Brooke, J. (2013). SUS: A Retrospective, *Journal of Usability Studies*, 8(2), pp. 29–40.

Bryman, A. (2008). *Social research methods*. New York: Oxford University Press.

Burbules, N. C. (1998). Rhetorics of the Web: hyperreading and critical literacy. Snyder, I. (Ed) *Page to Screen. Taking literacy into the electronic era*. London: Routledge, pp. 102-124.

Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy, *Journal of Direct Marketing*, 11(3), pp. 44–57.

Capellini, R., Tassistro, F. and Actis-Grosso, R. (2015). Quantitative Metrics for User Experience: A Case Study, *Sixteenth International Conference on Product-Focussed Software Process Improvement*. Bolzano, 2-4 December: Switzerland: Springer International Publishing, pp. 490–496.

Case, C., King, D. and Gage, L. (2015). Online Privacy and Security at the Fortune 500: An empirical examination of practices, *American Society of Business and Behavioural Sciences*, 11(1), pp. 59–67.

Cavoukian, A. (2011). Privacy by Design. The 7 foundational principles. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. (Accessed 22 September 2019).

Cavoukian, A. (no date). Privacy by Design. The 7 foundational principles. Implementation and mapping of fair information practices. Available at: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf. (Accessed 22 September 2019).

Cha, J. (2011). Information privacy: a comprehensive analysis of information request and privacy policies of most-visited Web sites, *Asian Journal of Communication*, 21(6), pp. 613–631.

Chaffey, D. (2011). *E-Business and E-Commerce Management. Strategy, Implementation and Practice*. Harlow: Pearson.

Chowdhury, G. G. and Chowdhury, S. (2011). *Information users and usability in the digital age*. London: Facet Publishing.

Chua, H. N., Herbland, A., Wong, S. F. and Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices, *Telematics and Informatics*, 34(4), pp. 157–170.

Citizenme. (2016). *Annual Track 2016*. Available at: https://ico.org.uk/media/about-the-ico/documents/.../ico-annual-track-2016.pptx.

Cranor, L. F., Egelman, S., Sheng, S., McDonald, A. M. and Chowdhury, A. (2008). P3P deployment on websites, *Electronic Commerce Research and Applications*, 7(3), pp. 274–293.

Cranor, L. F. (2012). Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice, *Journal on Telecommunications and High Technology*, 10(2), pp. 273–208.

Cranor, L. F. (2013). Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *Presentation given at Harvard University*, Cambridge, United States, 6 May. Available at: https://crcs.seas.harvard.edu/event/lorrie-faith-cranor-necessary-not-sufficient-standardized-mechanisms-privacy-notice-and. (Accessed 13 January 2019).

Cranor, L. F., Hoke, C., Leon, P and Au, A. (2015). Are They Worth Reading? An In-Depth Analysis of Online Trackers' Privacy Policies, *I/S : a journal of law and policy for the information society*, 11(2), pp. 325–404.

Creswell, J. W. (2009). *Research design: qualitative, quantitative, and mixed methods approaches*. London: Sage Publications.

Creswell, J. W. and Plano Clark, V. L. (2011). *Designing and conducting mixed methods research*. London: Sage Publications.

Crotty, M. (1998). *The foundations of social research: meaning and perspective in the research process*. London: Sage Publications.

Culnan, M. and Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation, *Organisational Science*, 10(1), pp. 104–115.

Culnan, M. J. and Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations, *Journal of Social Issues*, 59(2), pp. 323–342.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quarterly*, 13(3), p. 319-340.

Davis, J. (2017). *Know your cookies: A guide to internet ad trackers.* Available at: https://digiday.com/media/know-cookies-guide-internet-ad-trackers/ (Accessed: 6 August 2018).

Degeling, M. Utz, C. Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T. (2018). We Value Your Privacy...Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. Prepublication: Available at: http://arxiv.org/abs/1808.05096 (Accessed: 4 November 2018).

Dhamija, R., Tygar, J. D. and Hearst, M. (2006). Why phishing works. Grinter, R., Rodden, T., Aoki, P., Cutrell, E., Jeffries, R. and Olsen, G. (Eds) *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York: ACM, pp. 581-590.

Dias, G. P., Gomes, H. and Zúquete, A. (2016). Privacy policies and practices in Portuguese local e - government, *Electronic Government, An International Journal*, 12(4), pp. 301–318.

Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce, *Information Systems Research*, 17(1), pp. 61–80.

Direct Marketing Association. (2017). *What exactly is 'profiling' under the GDPR*. Available at: https://dma.org.uk/article/what-exactly-is-profiling-under-the-gdpr (Accessed: 11 August 2018).

Dolin, C., Weinshel, B., Shan, S., Hahn, C. M., Choi, E., Mazurek, M. L. and Ur, B. (2018). Unpacking Perceptions of Data-Driven Inferences Underlying Online

Targeting and Personalization. *CHI Conference on Human Factors in Computing Systems,* Montreal, April 21-26, New York: ACM Press, pp. 1–12.

Doyle, T. (2018). Privacy, obfuscation, and propertization, *IFLA Journal*, 44(3), pp. 229–239.

Earp, J. B., Anton, A. I., Aiman-Smith, L. and Stufflebeam W. H. (2005). Examining Internet Privacy Policies Within the Context of User Privacy Values, *IEEE Transactions on Engineering Management*, 52(2), pp. 227–237.

Eckersley, P. (2010). *How Unique Is Your Web Browser?* Available at: https://panopticlick.eff.org. (Accessed: 31 July 2018).

Edwards, L. (2018a). Data Protection and ePrivacy: From Spam and Cookies to Big Data, Machine Learning and Profiling, in Edwards, L (ed) *Law, Policy and the Internet*. Oxford: Hart Publishing.

Edwards, L. (2018b) ‘Privacy and Data Protection 1: What is Privacy? Human Right, National Law, Global Problem’, in Edwards, L. (ed) *Law, Policy and the Internet*, Oxford: Hart Publishing.

Edwards, L. and Abel, W. (2014). *The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services*. Available at: http://www.create.ac.uk/publications/the-use-of-privacy-icons-and-standard-contract-terms-for-generating-consumer-trust-and-confidence-in-digital-services. (Accessed: 15 April 2018).

European Commission. (2011). *How to write clearly*. Available at: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5/language-en (Accessed: 5 July 2018).

European Commission. (2015). *Special Eurobarometer 431: Data Protection*. Available at: https://data.europa.eu/euodp/data/dataset/S2075_83_1_431_ENG. (Accessed 5 January 2019).

European Commission. (2016). *Flash Eurobarometer 443: ePrivacy*. Available at: http://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG. (Accessed 10 December 2018).

European Commission. (2017). *Internet Purchases by Individuals*. Available at: http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do (Accessed: 21 December 2017).

European Parliament and Council. (2016). 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). *Official Journal*, L119, pp. 1-88.

EuroStat. (2019). E-commerce (isoc_iec). Available at: https://ec.europa.eu/eurostat/data/database. (Accessed 28 September 2019).

Experian. (2017). *ConsumerView*. Available at: https://www.experian.co.uk/assets/marketingservices/documents/FS_ConsumerView.pdf.

Fabian, B., Ermakova, T. and Lentz, T. (2017). Large-scale readability analysis of privacy policies, *International Conference on Web Intelligence*. New York, August 23 – 26, New York: ACM Press, pp. 18–25.

Featherman, M. S., Miyazaki, A. D. and Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility, *Journal of Services Marketing*, 24(3), pp. 219–229.

Federal Trade Commission. (1998). *Privacy Online: A report to Congress*. Available at: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (Accessed: 14 March 2018).

Federal Trade Commission. (2000). *FTC Recommends Congressional Action To Protect Consumer Privacy Online*. Available at: https://www.ftc.gov/news-events/press-releases/2000/05/ftc-recommends-congressional-action-protect-consumer-privacy (Accessed: 20 November 2018).

Federal Trade Commission. (2012). *Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Policymakers*. Available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (Accessed: 22 March 2018).

Fessenden, T. (2017). *Horizontal Attention Leans Left*. Available at: https://www.nngroup.com/articles/horizontal-attention-leans-left/. (Accessed 13 January 2019).

Financial Conduct Authority. (2018). *FCA fines Tesco Bank £16.4m for failures in 2016 cyber-attack*. Available at: https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack. (Accessed 12 January 2019).

Flesch, R. (1948). A new readability yardstick, *Journal of Applied Psychology*, 32(3), pp. 221–233.

Flesch, R. (1979). *How to write plain English*. New York: Harper and Row.

Floridi, L. (2005). The Ontological Interpretation of Informational Privacy, *Ethics and Information Technology*, 7(4), pp. 185–200.

Fortune. (2018). Available at: http://fortune.com/ (Accessed: 25 November 2018).

Frey, L. R., Botan, C. H. and Kreps, G. L. (2000). *Investigating communication: an introduction to research methods*. Needham Heights, MA: Allyn and Bacon.

Fried, C. (1984). Privacy (a moral analysis), in Schoeman, F. (ed) *Philosophical Dimensions of Privacy*. Cambridge University Press: London, pp. 203-222.

Garica, A. C., McDonnell N. N., Troncoso, C., Le Metayer, D., Kroener, I., Wright, D., Del Alamo, J. M. and Maertin, Y. S. (2015). Pripare. Privacy and security by design methodology handbook. Available at: http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf. (Accessed 1 September 2019).

Gavison, R., 1984. Privacy and the limits of the law. *In:* Schoeman, F. D. (ed.) *Philosophical dimensions of privacy: An anthology*. Cambridge: Cambridge University Press, pp. 245-264.

Gefen, D., Karahanna, E. and Sttraub, D. W. (2003). Trust and TAM in online shopping: an integrated model, *MIS Quarterly*, 27(1), pp. 51–90.

Gray, D. E. (2009). *Doing Research in the Real World*. London: Sage Publications.

Guba, E. and Lincoln, Y. (1994). Competing paradigms in qualitative research, in Denzin, N. and Lincoln, Y. (eds) *Handbook of qualitative research*, California: Sage Publications, pp. 105–117.

Gurung, A. and Raja, M. K. (2016). Online privacy and security concerns of consumers, *Information and Computer Security*, 24(4), pp. 348–371.

Harkous, H., Fawaz, K., Lebret, R., Schaub F., Shin, K. G., Aberer, K. (2018). Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep

Learning. *Twenty Seventh USENIX Security Symposium*, Baltimore, August 15-17, New York: USENIX Association, pp. 531 – 548.

Harris Interactive. (2018). *Information Rights Strategic Plan: Trust and Confidence*. Available at: https://ico.org.uk/media/about-the-ico/documents/2259732/annual-track-2018.pdf. (Accessed 12 January 2019).

Holsti, O. R. (1969). *Content analysis for the social sciences and humanities*. Boston: Addison-Wesley Pub. Co.

Holtz, L.-E., Nocun, K. and Hansen, M. (2011). Towards Displaying Privacy Information with Icons, in Fischer-Hubner, S., Duquenoy, P., Hansen, M., Leenes, R. and Zhang, G. (eds) *Privacy and Identity Management for Life*, Heidelberg: Springer, pp. 338–348.

Hooper, T. and Vos, M. (2009). Establishing business integrity in an online environment: An examination of New Zealand web site privacy notices, *Online Information Review,* 33(2), pp. 343-361.

Howitt, D. and Cramer, D. (2011). *Introduction to research methods in psychology*. London: Pearson/Prentice Hall.

Huang, A. H., Chen, K., Yen, D. C., & Tran, T. P. (2015). A study of factors that contribute to online review helpfulness. *Computers in Human Behavior*, 48, 17–27.

Hunton and Williams. (2006). *Ten steps to develop a multi-layered privacy notice*. Available at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2012/07/Centre-10-Steps-to-Multilayered-Privacy-Notice.pdf. (Accessed 22 December 2018).

Information Commissioner's Office. (n.d.) *ICO Publication Statistics*. Available at: https://ico.org.uk/media/about-the-ico/documents/1042394/ico-publication-stats.pdf. (Accessed 26 January 2019).

Information Commissioner's Office. (2010). *Privacy Notices Code of Practice*. Available at: http://webarchive.nationalarchives.gov.uk/20130102180945/http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_notices.aspx. (Accessed 5 Jan 2019).

Information Commissioner's Office. (2011). *Data Sharing Code of Practice*. Availbale at: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf. (Accessed 26 January 2019).

Information Commissioner's Office. (2015). *Online Pharmacy Fined for Selling Customer Details.* Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/online-pharmacy-fined-for-selling-customer-details/ (Accessed: 17 November 2018).

Information Commissioner's Office. (2016a). *Privacy notices, Transparency and Control. A code of practice on communicating privacy information to individuals*. Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf (Accessed: 21 March 2018).

Information Commissioner's Office. (2016b). *Consultation on ICO's privacy notices code of practice: summary of responses*. Available at: https://ico.org.uk/media/about-the-ico/consultations/1625139/ico-privacy-notices-code-of-practice-consultation-summary-20161006.pdf. (Accessed 19 December 2018).

Information Commissioner's Office. (2016c). *TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/. (Accessed: 18 December 2018).

Information Commissioner's Office. (2017). *Supervisory Powers of the Information Commissioner's Office. Monetary Penalty Notice*. Available at: https://ico.org.uk/media/action-weve-taken/mpns/2172671/verso-group-uk-limited-mpn-20171017.pdf. (Accessed 12 November 2018).

Information Commissioner's Office. (2018a). *Guide to the General Data Protection Regulation*. Available at: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. (Accessed 9 January 2019).

Information Commissioner's Office. (2018b). *Supervisory Powers of the Information Commissioner's Office. Monetary Penalty Notice*. Available at: https://ico.org.uk/media/action-weve-taken/mpns/2259583/lifecycle-marketing-mother-and-baby-ltd-mpn-8-august-2018.pdf. (Accessed 12 November 2018).

Information Commissioner’s Office. (2018c). *The right to be informed*. Available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/ (Accessed: 2 July 2018).

Information Commissioner’s Office. (2019). *Data protection by design and default*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/. (Accessed 1 September 2019).

Interactive Advertising Bureau. (2016). *IAB Mobile Location Data Guide for Publishers*. Available at: https://www.iab.com/guidelines/iab-mobile-location-data-guide-publishers/ (Accessed: 6 July 2018).

International Organisation for Standardization. (2010). *ISO 9241-210:2010 - Ergonomics of human-system interaction*. Available at: https://www.iso.org/standard/52075.html (Accessed: 13 November 2017).

Jensen, C. and Potts, C. (2004). Privacy policies as decision-making tools, *The 2004 conference on Human factors in computing systems*, Austria, April 24-29, New York: ACM Press, pp. 471–478.

Johnson, R. B. and Onwuegbuzie, A. J. (2004). *Mixed Methods Research: A Research Paradigm Whose Time Has Come*. California: Sage Publications, 33(7), pp. 14–26.

Kelley, P. G., Breese, J., Cranor, L. F. and Reeder, R. W. (2009). A Nutrition label for privacy. *Fifth Symposium on Usable Privacy and Security*, California, July 15-17, New York: ACM, Article 4.

Kelley, P. G., Cesca, L., Bresse, J. and Cranor, L. F. (2010). Standardising Privacy Notices. An Online Study of the Nutrition Label Approach. *The SIGCHI Conference on Human Factors In Computing Systems*, Atlanta, April 10-15, New York: ACM, pp. 1573 – 1582.

Kincaid, P. J., Fishburne, R. P., Rogers, R. L. and Chissom, B. S. (1975). *Derivation Of New Readability Formulas (Automated Readability Index, Fog Count And Flesch Reading Ease Formula) for Navy Enlisted Personnel*. Institute for Simulation and Training.

Kirakowski, J. and Cierlik, B. (1998). Measuring the Usability of Web Sites, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 42(4), pp. 424–428.

Kleen, B. A. and Heinrichs, L. (2007). Are privacy policies more clear and conspicuous in 2006 than in 2001? A longitudinal study of the Fortune 100, *Issues in Information Systems*, 8(2), pp. 348–354.

Kleinmann Communication Group. (2006). *Evolution of a Prototype Financial Privacy Notice: A Report on the Form Development Project*. Available at: https://www.ftc.gov/reports/evolution-prototype-financial-privacy-notice-report-form-development-project (Accessed: 17 September 2018).

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, *Computers & Security*, 64, pp. 122–134.

Krippendorff, K. (2013). *Content analysis: an introduction to its methodology*. London: Sage Publications.

Kristol, D. M. (2001). HTTP Cookies: Standards, privacy, and politics, *ACM Transactions on Internet Technology*, 1(2), pp. 151–198.

Krueger, R. A. and Casey, M. A. (2009). *Focus groups: a practical guide for applied research*. California: Sage Publications.

Kuhn, T. S. (1962). *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press.

Kumaraguru, P. and Cranor, L. F. (2005). *Privacy Indexes: A Survey of Westin's Studies*. Available at: http://www.pandab.org/RptOrderForm.pdf (Accessed: 19 August 2018).

Kuniavsky, M., Goodman, E. and Moed, A. (2012). *Observing the user experience: a practitioner's guide to user research*. Waltham: Morgan Kaufmann.

Langhorne, A. L. (2014). Web Privacy Policies in Higher Education: How Are Content and Design Used to Provide Notice (Or a Lack Thereof) to Users? *Second International Conference on Human Aspects of Information Security, Privacy and Trust*, Crete, June 22 – 27, New York: Springer-Verlag, pp. 422–432.

Lauer, T. W. and Deng, X. (2007). Building online trust through privacy practices, *International Journal of Information Security*, 6(5), pp. 323–331.

Lee, S. and French, N. (2011). The readability of academic papers in the Journal of Property Investment and Finance, *Journal of Property Investment and Finance*, 29(6), pp. 693–704.

Lewis, J. R. (1995). IBM computer usability satisfaction questionnaires: Psychometric evaluation and instructions for use, *International Journal of Human-Computer Interaction*, 7(1), pp. 57–78.

Li, S. and Zhang, C. (2009). An Analysis of Online Privacy Policies of Fortune 100 Companies, in Chen, K. and Fadlalla, A. (eds) *Online Consumer Protection: Theories of Human Relativism*. London: Information Science Reference, pp. 269–283.

Li, Y., Stweart, W., Zhu, J. and Ni, A. (2012). Online Privacy Policy of the Thirty Dow Jones Corporations: Compliance with FTC Fair Information Practice Principles and Readability Assessment, *Communications of the IIMA*, 12(3), pp. 65–89.

Likert, R. (1932). A technique for the measurement of attitudes, *Archives of Psychology*, 140, pp. 1–55.

L'Hoiry, X. D., & Norris, C. (2015). The honest data protection officer's guide to enable citizens to exercise their subject access rights: lessons from a ten-country European study. *International Data Privacy Law*, 5(3), 190–204

Lincoln, Y. S. and Guba, E. G. (1985). *Naturalistic Inquiry*. London: Sage Publications.

Liu, C., Marchewka, J. T., Lu, J. and Yu, C-S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce, *Information and Management*, 42(2), pp. 289–304.

Lo, B. W. N. and Sedhain, R. S. (2006). How reliable are website rankings? Implications for e-business advertising and internet search, *Issues in Information Systems*, 7(2), pp. 233-238.

Loughborough University. (2017). Code of Practice on Investigations Involving Human Participants. Available at: http://www.lboro.ac.uk/media/wwwlboroacuk/content/universitycommittees/ethicsapprovalshumanparticipantssub-committee/Code_of_Practice_HumanInvest.pdf (Accessed: 22 December 2017).

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., & Wells, T. (2012). Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the American Society for Information Science and Technology*, 63(4), 755–776.

Lund, A. M. (2001). Measuring Usability with the USE Questionnaire, *Usability Interface*, 8(2), pp. 3–6.

Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, *Information Systems Research*, 15(4), pp. 336–355.

Martin, K. (2015). Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online, *Journal of Public Policy & Marketing*, 34(2), pp. 210–227.

Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995). An Integrative Model of Organizational Trust, *The Academy of Management Review*, 20(3), p. 709.

McDonald, A. M. and Cranor, L. F. (2008). The Cost of Reading Privacy Policies, *I/S: A Journal of Law and Policy for the Information Society*, 4(3), pp. 543–568.

McDonald, A. M., Reeder, R. W., Kelley, P. G. and Cranor, L. F. (2009). A Comparative Study of Online Privacy Policies and Formats. Goldberg, I. and Atallah, M. J. (eds) *Ninth International Symposium on Privacy Enhancing Technologies*, Berlin: Springer, pp. 37-55.

Mcknight, D. H., Choudhury, V. and Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model, *Journal of Strategic Information Systems*, 11, pp. 297–323.

Mclaughlin, G. H. (1968). Proposals for British Readability Measures. Brown, A. L and Downing, J. A (eds) *Third International Reading Symposium*, London: Cassell, pp. 186–205.

McNemar, Q. (1947). Note on the sampling error of the difference between correlated proportions or percentages, *Psychometrika*, 12(2), pp. 153–157.

McRobb, S. (2006). Let's agree to differ: varying interpretations of online privacy policies', Journal of Information, *Communication and Ethics in Society*, 4(4), pp. 215–228.

McRobb, S. and Rogerson, S. (2004). Are they really listening? *Information Technology & People*, 17(4), pp. 442–461.

McStay, A. (2016). *Digital advertising*. London: Palgrave.

Metzger, M. J. (2007). Making sense of credibility on the Web: Models for evaluating online information and recommendations for future research. *Journal of the American Society for Information Science and Technology*, 58(13), 2078–2091.

Metzger, M. J., & Flanagin, A. J. (2013). Credibility and trust of information in online environments: The use of cognitive heuristics. *Journal of Pragmatics*, 59, 210–220.

Metzger, M. J., Flanagin, A. J. and Medders, R. B. (2010). Social and Heuristic Approaches to Credibility Evaluation Online. *Journal of Communication*, 60(3), pp. 413-439.

Miles, M. B. and Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook*. London: Sage Publications.

Milne, G. R., Culnan, M. J. and Greene, H. (2006). A Longitudinal Assessment of Online Privacy Notice Readability, *Journal of Public Policy & Marketing*, 25(2), pp. 238–249.

Moore, R., Moore, M. L., Shanahan, K. J., Horky, A. and Mack, B. (2015). Creepy Marketing: Three Dimensions of Perceived Excessive Online Privacy Violation, *Marketing Management Journal*, 25(1), pp. 42–53.

Morgan, D. L. (1997). *Focus groups as qualitative research*. London: Sage Publications.

Morgan, D. L. (1998). *Planning Focus Groups*. London: Sage Publications.

Morgan, D. L. (2007). Paradigms Lost and Pragmatism Regained, *Journal of Mixed Methods Research*, 1(1), pp. 48–76.

Mundy, D. P. (2006). Customer privacy on UK healthcare websites*, Medical Informatics and the Internet in Medicine*, 31(3), pp. 175–193.

Neuendorf, K. A. (2002). *The content analysis guidebook*. London: Sage Publications.

Neuendorf, K. A. (2016). *The content analysis guidebook*. London: Sage Publications.

Nielson, J. (2010). *Horizontal Attention Leans Left (Early Research)*. Available at: https://www.nngroup.com/articles/horizontal-attention-original-research/. (Accessed 13 January 2019).

Nikiforakis, N., Kapravelos, A., Joosen, W., Kruegel, C., Piessens, F and Vigna, G. (2014). On the Workings and Current Practices of Web-Based Device Fingerprinting, *IEEE Security & Privacy*, 12(3), pp. 28–36.

Nissenbaum, H. (2010). *Privacy in Context: Technology, policy and the Integrity of Social Life*. California: Stanford University Press.

Norman, G. (2010). Likert scales, levels of measurement and the “laws” of statistics’, *Advances in Health Sciences Education*, 15(5), pp. 625–632.

Obar, J. A. and Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, *Information, Communication & Society*, pp. 1–20.

Office for National Statistics. (2017a). *E-commerce and ICT activity, UK: 2016*. Available at: https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/ecommerceandictactivity/2016. (Accessed: 29 September 2019).

Office for National Statistics. (2017b). *Internet access - households and individuals: 2017*. Available at: http://doc.ukdataservice.ac.uk/doc/8299/mrdoc/pdf/8299_statistical_bulletin.pdf. (Accessed: 28 September 2019).

Office for National Statistics. (2017c). *Internet access - households and individuals*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/datasets/internetaccesshouseholdsandindividualsreferencetables (Accessed: 21 December 2017).

Office for National Statistics. (2018). Comparing “bricks and mortar” store sales with online retail sales: August 2018. Available at: https://www.ons.gov.uk/businessindustryandtrade/retailindustry/articles/comparingbricksandmortarstoresalestoonlineretailsales/august2018. (Accessed 28 September 2019).

Office of the Federal Register. (2009). Final Model Privacy Form under the Gramm-Leach-Bliley Act, *Federal Register*, 74(229), pp. 62890 – 62994.

Onwuegbuzie, A. J., Johnson, R. B. and Collins, K. M. (2009). Call for mixed analysis: A philosophical framework for combining qualitative and quantitative approaches, *International Journal of Multiple Research Approaches*, 3(2), pp. 114–139.

Outlaw, (2016). *Record £400, 000 fine for TalkTalk following data breach*. Available at: https://www.out-law.com/en/articles/2016/october/record-400000-fine-for-talktalk-following-data-breach/. (Accessed 12 January 2019).

Oxford University Press (2018) *Oxford English Dictionary*.

Parliament (1998). *Data Protection Act 1998*. Available at: https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf. (Accessed 9 January 2019).

Parliament. (2003). *Privacy and Electronic Communications (EC Directive) Regulations 2003* (SI 2426). Available at: http://www.legislation.gov.uk/uksi/2003/2426/pdfs/uksi_20032426_en.pdf. (Accessed 9 January 2019).

Patton, M. Q. (2015). *Qualitative research and evaluation methods: integrating theory and practice.* London: Sage Publications.

Peslak, A. R., & Jurkiewicz, N. (2008). Internet Privacy Policies of the Largest International Companies in 2004 and 2006. In Khosrow-Pour (ed) *Web Technologies for Commerce and Services Online*, Hershey: IGI Global, pp. 77-94.

Polisis. (2017). Available at: https://pribot.org/. (Accessed 26 January 2019).

Pollach, I. (2005). A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent, *Journal of Business Ethics*, 62(3), pp. 221–235.

Pollach, I. (2007), What's wrong with online privacy policies? *Communications of the ACM*, 50(9), pp. 103–108.

Proctor, R. W., Ali, M. A. and Vu, K.-P. L. (2008). Examining Usability of Web Privacy Policies, *International Journal of Human-Computer Interaction,* 24(3), pp. 307–328.

Rains, S. A. and Bosch, L. A. (2009). Privacy and Health in the Information Age: A Content Analysis of Health Web Site Privacy Policy Statements, *Health Communication*, 24(5), pp. 435–446.

Ram, A. and Murphy, H. (2018). Companies under strain from GDPR requests. *Financial Times.* Available at: https://www.ft.com/content/31d9286a-7bac-11e8-8e67-1e1a0846c475. (Accessed 26 January 2019).

Rao, A., Schaub, F., Sadeh, N., Acquisti, A. and Kang, R. (2016). Expecting the Unexpected: Understanding mismatched privacy expectations online, *Twelfth USENIX Conference on Usable Privacy and Security*, Denver, June 22-24, Berkeley: USENIX Association, pp. 77-96.

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J., Lui, F., McDonald, A., Norton, T., Ramanath, R., Russell, C. N., Sadeh, N. and Schaub, F. (2015). Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding, *Berkeley Technology Law Journal*, 30(1), pp. 39-68.

Rohrer, C. (2014). *When to Use Which User-Experience Research Methods*. Available at: https://www.nngroup.com/articles/which-ux-research-methods/ (Accessed: 3 December 2017).

Sadeh, N., Acquisti, A., Breaux, T., Cranor, L. F., McDonald, A., Reidenberg, J., Smith, N. A., Liu, F., Russell, N. C., Schaub, F., Wilson, S., Graves, J. T., Leon, P. G., Ramanath, R., Rao, A. (2014). Towards Usable Privacy Policies: Semi Automatically Extracting Data Practices from Websites' Privacy Policies. *Symposium on Usable Privacy and Security*, California, July 9-11. Available at: https://cups.cs.cmu.edu/soups/2014/posters/soups2014_posters-paper20.pdf. (Accessed 13 January 2019).

Salesforce. (2018). *Digital Advertising 2020 Insights into a new era of advertising and media buying*. Available at: https://www.salesforce.com/content/dam/web/en_us/www/assets/pdf/datasheets/digital-advertising-2020.pdf. (Accessed: 5 August 2018).

Sawyer, A. G., Laran, J. and Xu, J. (2008). The Readability of Marketing Journals: Are Award-Winning Articles Better Written? *Journal of Marketing*, 72(1), pp. 108–117.

Schnackenberg, A. K. and Tomlinson, E. C. (2016). Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships, *Journal of Management*, 42(7), pp. 1784–1810.

Schwaig, K. S., Kane, G. C., and Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & Management*, 43(7), 805–820.

Schwaig, K. S., Segars, A. H., Grover, V. and Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy, *Information & Management*, 50(1), pp. 1–12.

Schwandt, T. A. (2015). *The SAGE Dictionary of Qualitative Inquiry*. London: Sage Publications.

Singh, R. I., Sumeeth, M. and Miller, J. (2011). A user-centric evaluation of the readability of privacy policies in popular web sites, *Information Systems Frontiers*, 13(4), pp. 501–514.

Smith, H. J., Milberg, S. J. and Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices, *MIS Quarterly*, 20(2), p. 167.

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Son, Y. and Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological, *MIS Quarterly*, 32(3), pp. 503-529.

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment', *Computers in Human Behavior*, 55(Part B), pp. 992–1000.

Sumeeth, M., Singh, R. I. and Miller, J. (2010). Are Online Privacy Policies Readable? *International Journal of Information Security and Privacy*, 4(1), pp. 93–116.

Tavani, H. T. (2007). Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy, *Metaphilosophy*, 38(1), pp. 1–22.

Teddlie, C. and Tashakkori, A. (2009). *Foundations of mixed methods research: integrating quantitative and qualitative approaches in the social and behavioral sciences*. London: Sage Publications.

The Economist. (2017). *The world's most valuable resource is no longer oil, but data*. Available at: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. (Accessed: 5 January 2019).

The Usable Privacy Project. (2018). Available at: https://www.usableprivacy.org/. (Accessed 26 January 2019).

Tjhin, I., Vos, M. and Munaganuri, S. (2016). Privacy Governance Online: Privacy Policy Practices on New Zealand Websites, *Twentieth Pacific Asia Conference on Information Systems*, Taiwan, June 27 – Jul 1. Available at: https://aisel.aisnet.org/pacis2016/. (Accessed 6 January 2019).

Tsai, J. Y., Egelman, S., Cranor, L. and Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, *Information Systems Research*, 22(2), pp. 254–268.

Tullis, T. and Albert, B. (2008). *Measuring the user experience: collecting, analyzing, and presenting usability metrics*. Massachusetts: Morgan Kaufmann.

UK Government. (n.d). *Companies House*. Available at: https://www.gov.uk/government/organisations/companies-house (Accessed: 13 November 2017).

United States Government Accountability Office. (2013). *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*. Available at: https://www.gao.gov/products/GAO-13-663 (Accessed: 11 November 2018).

Upathilake, R., Li, Y. and Matrawy, A. (2015). A classification of web browser fingerprinting techniques, *Seventh International Conference on New Technologies, Mobility and Security*, Paris, July 27-29, pp. 1–5. doi: 10.1109/NTMS.2015.7266460.

Ur, B., Leon, P. G., Cranor, L. F., Shay, R. and Wang, Y. (2012). Smart, useful, scary, creepy, *Eighth Symposium on Usable Privacy and Security*. Washington, June 11-13, New York: ACM Press, Article 4.

Van den Hoonaard, W. C. (1997). *Working with sensitizing concepts: analytical field research*. Thousand Oaks: Sage Publications.

Venkatesh, V. and Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies, *Management Science*, 46(2), pp. 186–204.

Walker, J. (2013). Data mining to recruit sick people, *Wall Street Journal*. Available at: https://www.wsj.com/articles/data-mining-to-recruit-sick-people-1387237952.

Webb, L. M. and Wang, Y. (2014). Techniques for Sampling Online Text-Based Data Sets, in Hu, W.-C. and Kaabouch, N. (eds) *Big Data Management, Technologies, and Applications*. Hershey: IGI Global, pp. 95–114.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

Westin, A. F. (2003). Social and Political Dimensions of Privacy, *Journal of Social Issues*, 59(2), pp. 431-453.

White, M. D. and Marsh, E. E. (2006). Content Analysis: A Flexible Methodology, *Library Trends*, 55(1), pp. 22–45.

Williams, T. L., Agarwal, N. and Wigand, R. T. (2014). Protecting private information: Current attitudes concerning privacy policies. The 2014 ASE BigData/SocialInformatics/PASSAT/BioMedCom, Harvard University, December 14-16. Available at: https://www.researchgate.net/publication/279980732_Protecting_Private_Information_Current_Attitudes_Concerning_Privacy_Policies. (Accessed: 25 August 2019)

Zaeem, R. N. and Barber, K. S. (2017). A study of web privacy policies across industries, *Journal of Information Privacy and Security*, 13(4), pp. 169–185.

Appendices

Appendix A: Phase One Variable Metadata

No.	**A priori/ Induction**	**Recording unit**	**Reliability Pre/Post (Cohen's Kappa)**

Section 1: Format			
1.1	Is the privacy policy presented in a layered format?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100

Section 2: Effective Date			
2.1	Does the privacy policy state when the policy was last updated?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100

Section 3: Data Controller Identity and Purposes for Processing			
3.1	Does the privacy policy explicitly mention the identity of the data controller?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100
3.2	If no to 3.1, is it possible to infer who the data controller is from the privacy policy?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 95 2015: 100/ 100
3.3	Does the privacy policy identify the purpose or purposes for which personal data will be processed?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100
3.4	Does the privacy policy identify a named individual to contact regarding personal data processing?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100

Section 4: Personal Data Sharing for Direct Marketing Purposes			
4.1	Does the privacy policy mention that personal data is or might be shared for direct marketing purposes (with or without the consent of the user)?		
	No; Yes; Open to interpretation		
	Induction	Privacy policy	2012: 100/ 100 2015: 100/ 100
4.2	If yes to 4.1, does the privacy policy mention with whom personal data will be shared?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100

No.	**A priori/ Induction**	**Recording unit**	**Reliability Pre/Post (Cohen’s Kappa)**
4.3	If yes to 4.2, with whom is personal data shared?		
	Names:		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100
4.4	If yes to 4.2, are any names of organisations mentioned?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100
Section 5: Accessing and Amending			
5.1	Does the privacy policy mention that it is possible to view or amend personal data?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100
5.2	Does the privacy policy mention anything about how personal data being processed by the organisation can be viewed or amended?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 95 2015: 100/ 100
5.3	Does the privacy policy mention that it is the right of the user to request a copy of the personal data being processed?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100
5.4	Does the privacy policy mention that it is the right of the user to amend inaccurate personal data being processed?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 95
5.5	Does the privacy policy mention that it is the right of the user to remove inaccurate personal data being processed?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100
Section 6: Direct Marketing Preferences			
6.1	Does the privacy policy mention that it is possible to prevent personal data being used for direct marketing?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 95 2015: 100/ 100
6.2	Does the privacy policy mention how to prevent personal data being used for direct marketing purposes?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 89 2015: 100/ 100
6.3	Does the privacy policy mention that it is the right of the user to prevent personal data being processed for direct marketing purposes?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100

No.	**A priori/ Induction**	**Recording unit**	**Reliability Pre/Post (Cohen's Kappa)**

Section 7: Accountability			
7.1	Does the privacy policy mention that the user has the option to contact the Information Commissioner's Office should a dispute arise?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100
7.2	Does the privacy policy mention any contact details for the organisation?		
	No; Yes		
	A priori	Privacy policy	2012: 95/ 95 2015: 100/ 100

Section 8: Retention			
8.1	Does the privacy policy mention a specific length of time personal data will be retained for?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 100 2015: 100/ 100

Section 9: Security			
9.1	Does the privacy policy mention anything about the technology or technologies used to keep personal data secure?		
	No; Yes		
	A priori	Privacy policy	2012: 100/ 81 2015: 100/ 100
9.2	Does the website publish information on the security of personal data separately to the privacy policy?		
	No; Yes		
	Induction	U.K. B2C e-commerce website	2012: 100/ 100 2015: 100/ 100
9.3	If yes to either 9.2, does the separate security information mention anything about the technology or technologies used to keep personal data secure?		
	No; Yes		
	A priori	Security policy	2012: 100/ 100 2015: 100/ 100

Section 10: Cookies			
10.1	Does the website publish a cookie policy?		
	No; Yes		
	A priori	U.K. B2C e-commerce website	2012: 100/ 100 2015: 100/ 100
10.2	If yes to 10.1, does the website publish a cookie policy separately to the privacy policy?		
	No; Yes		
	Induction	U.K. B2C e-commerce website	2012: 100/ 100 2015: 100/ 100
10.3	If yes to 10.1, does the cookie policy describe the purpose or purposes for which cookies are used?		
	No; Yes		
	A priori	Privacy/cookie policy	2012: 100/ 100 2015: 100/ 100

Appendix B: Phase One Sampling Frame

Highlighted grey: Included within the sample (200 websites)

	Website	Unique visitors	Reach (%)	Rejection code
1	amazon.co.uk	18,000,000	35.30%	1
2	tesco.com	7,400,000	14.70%	
3	argos.co.uk	7,400,000	14.60%	
4	stores.ebay.co.uk	4,600,000	9.20%	
5	myworld.ebay.co.uk	4,600,000	9.20%	
6	marksandspencer.com	4,600,000	9.20%	
7	next.co.uk	4,600,000	9.10%	
8	amazon.com	3,800,000	7.70%	
9	play.com	3,200,000	6.30%	
10	johnlewis.com	3,500,000	6.90%	
11	skydrive.live.com	2,900,000	5.80%	2
12	debenhams.com	2,900,000	5.70%	
13	secure.tesco.com	2,400,000	4.70%	3
14	sainsburys.co.uk	2,100,000	4.30%	
15	photobucket.com	1,800,000	3.60%	
16	littlewoods.com	1,800,000	3.60%	
17	newlook.com	1,800,000	3.60%	
18	lovefilm.com	1,600,000	3.30%	
19	very.co.uk	1,600,000	3.20%	
20	comet.co.uk	1,600,000	3.20%	
21	fashion.ebay.co.uk	1,500,000	3.00%	2
22	sportsdirect.com	1,400,000	2.70%	
23	riverisland.com	1,300,000	2.70%	
24	hmv.com	1,200,000	2.40%	
25	houseoffraser.co.uk	1,200,000	2.40%	
26	lego.com	1,100,000	2.20%	
27	261atalan.co.uk	1,100,000	2.20%	
28	save-clever.co.uk	1,100,000	2.20%	
29	topshop.com	1,200,000	2.40%	
30	toysrus.co.uk	1,000,000	2.00%	
31	clothingattesco.com	920,000	1.80%	5
32	hm.com	840,000	1.70%	1
33	dorothyperkins.com	830,000	1.60%	
34	s3.amazonaws.com	760,000	1.50%	1
35	qvcuk.com	750,000	1.50%	
36	bhs.co.uk	750,000	1.50%	
37	mandmdirect.com	750,000	1.50%	
38	jdsports.co.uk	630,000	1.30%	
39	universe.lego.com	630,000	1.30%	
40	boden.co.uk	620,000	1.20%	
41	moonpig.com	620,000	1.20%	
42	clarks.co.uk	620,000	1.20%	
43	kandco.com	620,000	1.20%	
44	phone-shop.tesco.com	570,000	1.10%	
45	uk.shopping.com	520,000	1.00%	
46	boohoo.com	570,000	1.10%	
47	waterstones.com	570,000	1.10%	
48	money.marksandspencer.com	560,000	1.10%	
49	shopwiki.co.uk	520,000	1.00%	
50	jjbsports.com	520,000	1.00%	

51	24studio.co.uk	520,000	1.00%	
52	tkmaxx.com	510,000	1.00%	
53	gap.eu	480,000	0.90%	
54	hst.tradedoubler.com	470,000	0.90%	
55	photobox.co.uk	470,000	0.90%	
56	sellercentral.amazon.co.uk	470,000	0.90%	
57	homeshopping.24studio.co.uk	470,000	0.90%	
58	snapfish.co.uk	430,000	0.90%	
59	simplybe.co.uk	430,000	0.90%	
60	etsy.com	390,000	0.80%	
61	laredoute.co.uk	430,000	0.90%	
62	office.co.uk	430,000	0.90%	
63	schuh.co.uk	390,000	0.80%	
64	lauraashley.com	420,000	0.80%	
65	monsoon.co.uk	420,000	0.80%	
66	uk.westfield.com	390,000	0.80%	
67	missselfridge.com	390,000	0.80%	
68	community.ebay.co.uk	390,000	0.80%	
69	wallis.co.uk	350,000	0.70%	
70	republic.co.uk	390,000	0.80%	
71	shutterstock.com	380,000	0.80%	1
72	westfield.com	380,000	0.80%	2
73	nike.com	380,000	0.80%	1
74	gooutdoors.co.uk	360,000	0.70%	
75	elc.co.uk	350,000	0.70%	
76	zalando.co.uk	350,000	0.70%	
77	topman.com	350,000	0.70%	
78	peacocks.co.uk	350,000	0.70%	
79	zara.com	350,000	0.70%	
80	opticalexpress.co.uk	350,000	0.70%	
81	marisota.co.uk	350,000	0.70%	
82	evans.co.uk	290,000	0.60%	5
83	warehouse.co.uk	290,000	0.60%	
84	cafepress.co.uk	320,000	0.60%	
85	search.qvcuk.com	320,000	0.60%	
86	wiley.com	320,000	0.60%	
87	istockphoto.com	290,000	0.60%	
88	bestbuy.co.uk	320,000	0.60%	
89	oasis-stores.com	290,000	0.60%	
90	isme.com	290,000	0.60%	
91	asylum.co.uk	290,000	0.60%	2
92	blockbuster.co.uk	290,000	0.60%	
93	store.nike.com	290,000	0.60%	1
94	notonthehighstreet.com	290,000	0.60%	
95	javari.co.uk	290,000	0.60%	
96	gettingpersonal.co.uk	320,000	0.60%	
97	selfridges.com	290,000	0.60%	
98	shopstyle.co.uk	290,000	0.60%	
99	primark.co.uk	290,000	0.60%	
100	onlinelibrary.wiley.com	270,000	0.50%	
101	zazzle.co.uk	270,000	0.50%	1
102	walletpop.co.uk	270,000	0.50%	6
103	specsavers.co.uk	270,000	0.50%	1
104	bid.tv	270,000	0.50%	
105	bankfashion.co.uk	240,000	0.50%	
106	reviews.argos.co.uk	270,000	0.50%	
107	shop.lego.com	270,000	0.50%	

108	123rf.com	270,000	0.50%	
109	net-a-porter.com	270,000	0.50%	
110	smythstoys.com	260,000	0.50%	
111	mybrowserbar.com	260,000	0.50%	2
112	jacquielawson.com	260,000	0.50%	
113	uk.shop.com	240,000	0.50%	2
114	stores.ebay.com	260,000	0.50%	2
115	everything5pounds.com	260,000	0.50%	
116	list-manage1.com	240,000	0.50%	
117	bizrate.com	240,000	0.50%	
118	ulsterbank.co.uk	240,000	0.50%	
119	partydelights.co.uk	220,000	0.40%	
120	thebookpeople.co.uk	240,000	0.50%	
121	bonprixsecure.com	220,000	0.40%	
122	interflora.co.uk	220,000	0.40%	
123	abebooks.co.uk	220,000	0.40%	
124	hsamuel.co.uk	240,000	0.50%	
125	harrods.com	220,000	0.40%	
126	gallery.live.com	240,000	0.50%	
127	cottontraders.co.uk	220,000	0.40%	
128	kaleidoscope.co.uk	220,000	0.40%	
129	clker.com	220,000	0.40%	
130	vertbaudet.co.uk	200,000	0.40%	
131	myfuncards.com	220,000	0.40%	1
132	mandco.com	220,000	0.40%	
133	bookdepository.co.uk	220,000	0.40%	
134	allsaints.com	200,000	0.40%	
135	jackwills.com	180,000	0.40%	
136	ulsterbankanytimebanking.co.uk	220,000	0.40%	
137	reviews.ebay.co.uk	240,000	0.50%	
138	polyvore.com	200,000	0.40%	
139	lipsy.co.uk	210,000	0.40%	
140	overstock.com	210,000	0.40%	
141	secretsales.com	220,000	0.40%	
142	coast-stores.com	180,000	0.40%	
143	zavvi.com	220,000	0.40%	
144	jacamo.co.uk	220,000	0.40%	
145	fashionworld.co.uk	200,000	0.40%	
146	buyagift.co.uk	200,000	0.40%	
147	hottershoes.com	200,000	0.40%	
148	hollisterco.com	200,000	0.40%	
149	watchshop.com	180,000	0.40%	
150	fiftyplus.co.uk	200,000	0.40%	
151	whitestuff.com	200,000	0.40%	
152	barratts.co.uk	200,000	0.40%	
153	superdry.com	200,000	0.40%	
154	corporate.marksandspencer.com	200,000	0.40%	
155	landsend.co.uk	180,000	0.40%	
156	toyssale.com	200,000	0.40%	
157	help.next.co.uk	180,000	0.40%	
158	123greetings.com	180,000	0.40%	
159	shop.adidas.co.uk	180,000	0.40%	
160	lightinthebox.com	200,000	0.40%	
161	shopdirect.com	180,000	0.40%	2
162	karenmillen.com	160,000	0.30%	5
163	dreamstime.com	180,000	0.40%	1
164	account.lego.com	200,000	0.40%	7

165	dealtime.com	180,000	0.40%	2
166	cathkidston.co.uk	180,000	0.40%	
167	cloggs.co.uk	180,000	0.40%	
168	fatface.com	200,000	0.40%	
169	firebox.com	160,000	0.30%	
170	figleaves.com	180,000	0.40%	
171	bonmarche.co.uk	180,000	0.40%	
172	help.marksandspencer.com	180,000	0.40%	2
173	janenorman.co.uk	160,000	0.30%	
174	funkypigeon.com	180,000	0.40%	
175	264asbro.com	180,000	0.40%	
176	premierman.com	200,000	0.40%	
177	thehut.com	180,000	0.40%	
178	urbanoutfitters.co.uk	200,000	0.40%	
179	getthelabel.com	150,000	0.30%	
180	fotosearch.com	180,000	0.40%	
181	surfdome.com	170,000	0.30%	
182	discogs.com	170,000	0.30%	2
183	missguided.co.uk	170,000	0.30%	
184	adidas.co.uk	92,000	0.20%	
185	dhgate.com	170,000	0.30%	
186	sage.co.uk	150,000	0.30%	
187	secure.comet.co.uk	1,600,000	3.20%	
188	bravissimo.com	160,000	0.30%	
189	joke.co.uk	180,000	0.40%	
190	supersavvyme.co.uk	180,000	0.40%	
191	hobbs.co.uk	160,000	0.30%	
192	ernestjones.co.uk	160,000	0.30%	
193	woolworths.co.uk	160,000	0.30%	
194	ambrosewilson.com	160,000	0.30%	
195	joules.com	150,000	0.30%	
196	lasenza.co.uk	180,000	0.40%	
197	frenchconnection.com	180,000	0.40%	
198	264asbro.com	150,000	0.30%	
199	youtu.be	31,000,000	62.10%	
200	thebrilliantgiftshop.co.uk	140,000	0.30%	
201	theoutnet.com	150,000	0.30%	
202	starwars.lego.com	150,000	0.30%	2
203	musicmagpie.co.uk	150,000	0.30%	2
204	mto.lauraashley.com	150,000	0.30%	3
205	burton.co.uk	150,000	0.30%	5
206	cduniverse.com	160,000	0.30%	1
207	northernbank.co.uk	160,000	0.30%	2
208	makro.co.uk	150,000	0.30%	
209	whosay.com	150,000	0.30%	
210	phase-eight.co.uk	140,000	0.30%	
211	photobox.com	140,000	0.30%	1
212	city.lego.com	140,000	0.30%	2
213	ninjago.lego.com	140,000	0.30%	2
214	paidonresults.net	130,000	0.20%	2
215	yoursclothing.co.uk	140,000	0.30%	
216	dune.co.uk	120,000	0.20%	
217	uniformdating.com	140,000	0.30%	
218	partnershipcard.co.uk	140,000	0.30%	
219	ecards.myfuncards.com	140,000	0.30%	
220	stereoboard.com	120,000	0.20%	
221	stat.dealtime.com	140,000	0.30%	2

222	aliexpress.com	140,000	0.30%	1
223	toysrus.com	130,000	0.30%	1
224	millets.co.uk	130,000	0.30%	
225	thetoyshop.com	130,000	0.30%	
226	modelmayhem.com	130,000	0.30%	
227	uk.ebid.net	130,000	0.30%	
228	damart.co.uk	130,000	0.30%	
229	usc.co.uk	120,000	0.20%	
230	buildabear.co.uk	130,000	0.30%	
231	herofactory.lego.com	140,000	0.30%	1
232	thewatchhut.co.uk	130,000	0.20%	
233	ralphlauren.co.uk	120,000	0.20%	1
234	morelikethis.ebay.co.uk	120,000	0.20%	2
235	uniqlo.com	110,000	0.20%	
236	jlpjobs.com	120,000	0.20%	
237	shopstyle.com	110,000	0.20%	
238	tedbaker.com	120,000	0.20%	
239	grattan.co.uk	120,000	0.20%	
240	blacks.co.uk	120,000	0.20%	
241	search.next.co.uk	4,600,000	9.10%	5
242	us2.list-manage1.com	240,000	0.50%	2
243	smilebox.com	140,000	0.30%	1
244	bigtop40.com	120,000	0.20%	2
245	cotswoldoutdoor.com	120,000	0.20%	
246	my-wardrobe.com	120,000	0.20%	
246	promotionalcodes.org.uk	120,000	0.20%	
248	tiffany.co.uk	120,000	0.20%	
249	truprint.co.uk	120,000	0.20%	
250	secure.partnershipcard.co.uk	120,000	0.20%	
251	kurtgeiger.com	130,000	0.30%	
252	store.makro.co.uk	120,000	0.20%	2
253	alienconquest.lego.com	110,000	0.20%	2
254	ctshirts.co.uk	110,000	0.20%	
255	swarovski.com	94,000	0.20%	
256	yoox.com	100,000	0.20%	
257	forever21.com	100,000	0.20%	
258	affiliate-program.amazon.co.uk	110,000	0.20%	
259	walmart.com	110,000	0.20%	
260	localstore.co.uk	120,000	0.20%	
261	secure2.photobox.com	110,000	0.20%	5
262	careers.next.co.uk	110,000	0.20%	2
263	goldsmiths.co.uk	120,000	0.20%	
264	reissonline.com	110,000	0.20%	
265	thekidswindow.co.uk	110,000	0.20%	
266	costco.co.uk	110,000	0.20%	
267	hallmark.co.uk	100,000	0.20%	
268	promo.snapfish.co.uk	430,000	0.90%	
269	us1.list-manage1.com	240,000	0.50%	
270	outdoorkit.co.uk	100,000	0.20%	
271	shop.uniqlo.com	110,000	0.20%	3
272	feefo.com	94,000	0.20%	2
273	spreadshirt.co.uk	85,000	0.20%	1
274	uggaustralia.co.uk	100,000	0.20%	
275	amazon.de	100,000	0.20%	2
276	uroda.onet.pl	100,000	0.20%	2
277	redletterdays.co.uk	100,000	0.20%	
278	sparknotes.com	110,000	0.20%	

279	legoland.co.uk	93,000	0.20%	
280	gap.com	100,000	0.20%	
281	fancydress.com	110,000	0.20%	
282	mailing.tesco.com	120,000	0.20%	2
283	supsale.com	93,000	0.20%	2
284	greenfingers.com	92,000	0.20%	
285	watchfinder.co.uk	92,000	0.20%	
286	plana.marksandspencer.com	100,000	0.20%	
287	shiply.com	100,000	0.20%	
288	bearville.com	110,000	0.20%	
289	vivaladiva.com	92,000	0.20%	
290	creator.lego.com	92,000	0.20%	
291	uk.supsale.com	92,000	0.20%	2
292	fantasticfiction.co.uk	100,000	0.20%	2
293	johnlewisgiftlist.com	100,000	0.20%	5
294	266andora.net	100,000	0.20%	2
295	kodakgallery.co.uk	110,000	0.20%	1
296	astore.amazon.com	110,000	0.20%	1
297	louisvuitton.com	94,000	0.20%	1
298	folksy.com	85,000	0.20%	2
299	find-me-a-gift.co.uk	93,000	0.20%	
300	youtubedownloader.mybrowserbar.com	84,000	0.20%	2
301	francisfrith.com	93,000	0.20%	1
302	tmlewin.co.uk	84,000	0.20%	
303	aldoshoes.com	84,000	0.20%	7
304	adidas.com	92,000	0.20%	1
305	joebrowns.co.uk	100,000	0.20%	
306	harveynichols.com	92,000	0.20%	
307	pauls-boutique.com	91,000	0.20%	
308	266etflix.com	83,000	0.20%	
309	quizclothing.co.uk	86,000	0.20%	
310	hyperpromote.com	71,000	0.10%	
311	ecrater.co.uk	85,000	0.20%	2
312	poundland.co.uk	85,000	0.20%	
313	gb.com	77,000	0.20%	
314	foot-locker.co.uk	85,000	0.20%	
315	blogs.qvcuk.com	94,000	0.20%	
316	clintoncards.co.uk	85,000	0.20%	
317	dltk-kids.com	85,000	0.20%	
318	digital-photography-school.com	70,000	0.10%	
319	size.co.uk	77,000	0.20%	
320	kingdoms.lego.com	85,000	0.20%	
321	the-saleroom.com	93,000	0.20%	2
322	barnesandnoble.com	77,000	0.20%	1
323	mulberry.com	84,000	0.20%	
324	linksoflondon.com	77,000	0.20%	
325	moviease.com	84,000	0.20%	
326	jaeger.co.uk	84,000	0.20%	
327	brantano.co.uk	76,000	0.20%	
328	worthpoint.com	84,000	0.20%	
329	drjays.com	84,000	0.20%	
330	services.amazon.co.uk	84,000	0.20%	
331	fashionunion.com	84,000	0.20%	
332	nextflowers.co.uk	84,000	0.20%	5
333	24ace.co.uk	84,000	0.20%	5
334	mountainwarehouse.com	84,000	0.20%	
335	jojomamanbebe.co.uk	84,000	0.20%	

336	haringey.gov.uk	84,000	0.20%	
337	heroica.lego.com	76,000	0.20%	
338	royalcollection.org.uk	92,000	0.20%	
339	mainlinemenswear.co.uk	84,000	0.20%	
340	look.co.uk	84,000	0.20%	
341	fotolia.com	92,000	0.20%	1
342	gltc.co.uk	76,000	0.20%	
343	barbourbymail.co.uk	83,000	0.20%	
344	movielush.com	83,000	0.20%	
345	shoe-shop.com	91,000	0.20%	
346	signup.netflix.com	83,000	0.20%	
347	womanandhome.com	78,000	0.20%	
348	fashionfinder.asos.com	70,000	0.10%	
349	mail.inbox.lv	85,000	0.20%	
350	invaluable.com	77,000	0.20%	
351	cards.hallmark.co.uk	70,000	0.10%	
352	getpark.co.uk	77,000	0.20%	
353	allfancydress.com	70,000	0.10%	
354	johngreedjewellery.com	70,000	0.10%	
355	partyrama.co.uk	85,000	0.20%	
356	zenfolio.com	70,000	0.10%	
357	uk.thenorthface.com	84,000	0.20%	
358	radley.co.uk	77,000	0.20%	
359	reelvidz.com	77,000	0.20%	
360	bbcshop.com	69,000	0.10%	
361	thenorthface.com	84,000	0.20%	1
362	crewclothing.co.uk	76,000	0.20%	
363	jonesbootmaker.com	76,000	0.20%	
364	bonhams.com	76,000	0.20%	
365	fancydressball.co.uk	69,000	0.10%	
366	youandyourwedding.co.uk	69,000	0.10%	
367	mattel.com	76,000	0.20%	
368	search2.lego.com	83,000	0.20%	
369	shop.cafepress.co.uk	76,000	0.20%	
370	tescophoto.com	76,000	0.20%	
371	filmlush.com	83,000	0.20%	2
372	wynsors.com	83,000	0.20%	
373	sportsshoes.com	68,000	0.10%	
374	amazon.fr	75,000	0.10%	
375	search.shoe-shop.com	75,000	0.10%	
376	curvissa.co.uk	71,000	0.10%	
377	routeone.co.uk	78,000	0.20%	
378	sendit.com	71,000	0.10%	
379	shoetailor.com	71,000	0.10%	
380	lkbennett.com	70,000	0.10%	
381	partypieces.co.uk	85,000	0.20%	
382	catalink.com	70,000	0.10%	2
383	astore.amazon.co.uk	77,000	0.20%	1
384	affiliate-program.amazon.com	70,000	0.10%	1
385	bananarepublic.gap.co.uk	64,000	0.10%	
386	sxc.hu	77,000	0.20%	
387	bonusprint.co.uk	63,000	0.10%	
388	item.taobao.com	70,000	0.10%	
389	zazzle.com	77,000	0.20%	
390	lovell-rugby.co.uk	70,000	0.10%	
391	api.mybrowserbar.com	76,000	0.20%	2
392	thorntons.co.uk	69,000	0.10%	

393	hugoboss.com	76,000	0.20%	1
394	rubbersole.co.uk	63,000	0.10%	1
395	videogames.lego.com	76,000	0.20%	2
396	minifigures.lego.com	63,000	0.10%	2
397	jigsaw-online.com	69,000	0.10%	
398	reviews.marksandspencer.com	63,000	0.10%	
399	grayandosbourn.co.uk	69,000	0.10%	
400	matchesfashion.com	62,000	0.10%	
401	tescodvdrental.com	68,000	0.10%	5
402	photoboxgallery.com	75,000	0.10%	2
403	simplyyours.co.uk	71,000	0.10%	5
404	city-listings.co.uk	59,000	0.10%	2
405	store-uk.hugoboss.com	58,000	0.10%	1
406	pumpkinpatch.co.uk	58,000	0.10%	
407	snowandrock.com	64,000	0.10%	
408	icanbe.barbie.com	58,000	0.10%	
409	daxon.co.uk	58,000	0.10%	
410	nikerunning.nike.com	64,000	0.10%	
411	sarenza.co.uk	64,000	0.10%	1
412	shoezone.com	64,000	0.10%	
413	latasca.co.uk	70,000	0.10%	2
414	reelhd.com	58,000	0.10%	1
415	gems.tv	63,000	0.10%	
416	orvis.co.uk	63,000	0.10%	
417	pure.hmv.com	63,000	0.10%	
418	arco.co.uk	70,000	0.10%	
419	ralphlauren.com	57,000	0.10%	
420	shop.hm.com	--	0.00%	
421	purecollection.com	57,000	0.10%	
422	beaverbrooks.co.uk	69,000	0.10%	
423	robinsonsequestrian.com	69,000	0.10%	
424	harrypotter.lego.com	63,000	0.10%	
425	medion.com	69,000	0.10%	
426	shopalike.co.uk	57,000	0.10%	
427	eharmony.com	69,000	0.10%	
428	partypacks.co.uk	63,000	0.10%	
429	footasylum.com	62,000	0.10%	
430	timberlandonline.co.uk	62,000	0.10%	
431	longtallsally.com	57,000	0.10%	
432	serenataflowers.com	59,000	0.10%	
433	268ondon.londinium.com	58,000	0.10%	
434	newitts.com	58,000	0.10%	
435	pricelessshoes.co.uk	64,000	0.10%	
436	royalmint.com	53,000	0.10%	
437	victoriassecret.com	53,000	0.10%	
438	shortlist.com	58,000	0.10%	
439	images.littlewoods.com	53,000	0.10%	
440	traffordcentre.co.uk	58,000	0.10%	
441	ulsterbank.com	58,000	0.10%	1
442	blu-ray.com	58,000	0.10%	1
443	macys.com	58,000	0.10%	1
444	hotelchocolat.co.uk	64,000	0.10%	
445	jjshouse.com	53,000	0.10%	1
446	selectfashion.co.uk	64,000	0.10%	
447	depositphotos.com	64,000	0.10%	
448	aldi.com	64,000	0.10%	
449	competitions.argos.co.uk	7,400,000	14.60%	

450	lookbook.nu	58,000	0.10%	
451	alibris.co.uk	58,000	0.10%	1
452	price-drop.tv	58,000	0.10%	5
453	en.fotolia.com	52,000	0.10%	1
454	dwsports.com	52,000	0.10%	
455	vente-privee.com	63,000	0.10%	1
456	club.lego.com	57,000	0.10%	2
457	shop.ebay.ie	52,000	0.10%	2
458	gamestop.co.uk	47,000	0.10%	1
459	adnxs.com	57,000	0.10%	2
460	levi.com	57,000	0.10%	1
461	gonedigging.co.uk	57,000	0.10%	
462	rideaway.co.uk	57,000	0.10%	
463	converse.co.uk	57,000	0.10%	1
464	visionexpress.com	57,000	0.10%	
465	cdwow.com	52,000	0.10%	
466	paperchase.co.uk	57,000	0.10%	
467	bradford.co.uk	57,000	0.10%	
468	hamleys.com	68,000	0.10%	
469	homeshoppingdirect.com	48,000	0.10%	
470	zappos.com	53,000	0.10%	
471	megashare.info	58,000	0.10%	2
472	finance.debenhams.com	53,000	0.10%	6
473	trekwear.co.uk	53,000	0.10%	
474	axparis.co.uk	53,000	0.10%	
475	zinio.com	58,000	0.10%	
476	pixlr.com	48,000	0.10%	
477	exlibrisgroup.com	48,000	0.10%	
478	bullionvault.com	58,000	0.10%	
479	easylifegroup.com	53,000	0.10%	
480	dancedirect.com	53,000	0.10%	
481	shop.sage.co.uk	53,000	0.10%	2
482	walmartstores.com	58,000	0.10%	2
483	email.boden.co.uk	48,000	0.10%	2
484	thisisexeter.co.uk	6,800,000	13.50%	2
485	liberty.co.uk	58,000	0.10%	
486	conrad-uk.com	58,000	0.10%	
487	reviews.ebay.com	48,000	0.10%	
488	jparkers.co.uk	52,000	0.10%	
489	amazon.co.jp	48,000	0.10%	
490	onlinepictureproof.com	52,000	0.10%	
492	theimagefile.com	52,000	0.10%	2
492	fieldandtrek.com	52,000	0.10%	5
493	forums.preloved.co.uk	1,200,000	2.40%	2
494	barbour.com	52,000	0.10%	5
495	firemansamonline.com	52,000	0.10%	6
496	adele.tv	52,000	0.10%	2
497	fashion.ebay.com	52,000	0.10%	2
498	pasttimes.com	52,000	0.10%	
499	rugbystore.co.uk	47,000	0.10%	
500	julesb.co.uk	52,000	0.10%	
501	truffleshuffle.co.uk	52,000	0.10%	
502	lynxtrack.com	47,000	0.10%	7
503	jobs.walmartstores.com	57,000	0.10%	2
504	rceltickets.com	43,000	0.10%	6
505	serialssolutions.com	52,000	0.10%	2
506	ib.adnxs.com	57,000	0.10%	2

507	fitflop.com	47,000	0.10%	
508	sweatybetty.com	51,000	0.10%	
509	jibjab.com	62,000	0.10%	
510	chanel.com	57,000	0.10%	
511	chums.co.uk	44,000	0.10%	
512	photos.truprint.co.uk	48,000	0.10%	1
513	daily.newlook.com	48,000	0.10%	3
514	claires.com	48,000	0.10%	1
515	buildabear.com	48,000	0.10%	4
516	clifford-james.co.uk	48,000	0.10%	
517	shopmania.co.uk	44,000	0.10%	
518	cgi.ebay.ie	48,000	0.10%	
519	esprit.co.uk	48,000	0.10%	
520	ecards.co.uk	44,000	0.10%	
521	threadless.com	48,000	0.10%	1
522	sellingantiques.co.uk	43,000	0.10%	2
523	hive4business.com	53,000	0.10%	7
524	verses4cards.co.uk	43,000	0.10%	2
525	everybodysmile.biz	53,000	0.10%	2
526	ccfashion.co.uk	43,000	0.10%	
527	charlesclinkard.co.uk	48,000	0.10%	4
528	clothing.boden.co.uk	48,000	0.10%	8
529	dealtastic.co.uk	43,000	0.10%	1
530	duoboots.com	48,000	0.10%	
531	farfetch.com	43,000	0.10%	
532	mrporter.com	48,000	0.10%	5
533	fisher-price.com	48,000	0.10%	1
534	knittingpatterncentral.com	48,000	0.10%	2
535	anniversaryideas.co.uk	48,000	0.10%	
536	toast.co.uk	47,000	0.10%	
537	diesel.com	43,000	0.10%	
538	johnnorris.co.uk	43,000	0.10%	
539	samuel-windsor.co.uk	47,000	0.10%	
540	herorecon.lego.com	47,000	0.10%	
541	craghoppers.com	47,000	0.10%	
542	stellaartois.com	47,000	0.10%	2
543	whatculture.com	47,000	0.10%	2
544	arkclothing.com	47,000	0.10%	
545	cult.co.uk	47,000	0.10%	
546	sendables.jibjab.com	52,000	0.10%	
547	whistles.co.uk	47,000	0.10%	
548	rolex.com	43,000	0.10%	
549	ingentaconnect.com	47,000	0.10%	
550	guardianbookshop.co.uk	47,000	0.10%	
551	virginexperiencedays.co.uk	47,000	0.10%	
552	weareelectricals.com	47,000	0.10%	
553	westfieldstratfordcity2011.com	47,000	0.10%	
554	bluemountain.com	43,000	0.10%	
555	createsend1.com	52,000	0.10%	
556	eu.levi.com	52,000	0.10%	
557	support.sage.co.uk	43,000	0.10%	
558	woolovers.com	52,000	0.10%	
559	treds.co.uk	51,000	0.10%	
560	en.vente-privee.com	47,000	0.10%	
561	shop.mattel.com	44,000	0.10%	1
562	adams.co.uk	44,000	0.10%	
563	store.americanapparel.co.uk	44,000	0.10%	1

564	acefancydress.co.uk	44,000	0.10%	
565	diyaonline.com	40,000	0.10%	
566	preview.next.co.uk	4,600,000	9.10%	
567	cafepress.com	44,000	0.10%	
568	awooh.com	44,000	0.10%	
569	jimmychoo.com	40,000	0.10%	
570	vans.com	48,000	0.10%	
571	photography.nationalgeographic.com	44,000	0.10%	2
572	mayflower.org.uk	44,000	0.10%	2
573	guess.eu	44,000	0.10%	1
574	endclothing.co.uk	43,000	0.10%	4
575	americanapparel.co.uk	43,000	0.10%	1
576	target.com	53,000	0.10%	1
577	foreseeresults.com	43,000	0.10%	2
578	chelseamegastore.com	43,000	0.10%	
579	bullionbypost.co.uk	39,000	0.10%	
580	tescopricecheck.com	43,000	0.10%	
581	reebok.com	48,000	0.10%	
582	pricedropper.co.uk	48,000	0.10%	5
583	bench.co.uk	43,000	0.10%	
584	qvc.com	43,000	0.10%	
585	shoes.co.uk	39,000	0.10%	
586	weddingdressonlineshop.co.uk	43,000	0.10%	
587	chemical-records.co.uk	39,000	0.10%	
588	shutterfly.com	43,000	0.10%	
589	moss.co.uk	48,000	0.10%	
590	fabulousmag.co.uk	39,000	0.10%	
591	cyclestore.co.uk	39,000	0.10%	
592	dealbd.mystart.com	39,000	0.10%	2
593	sears.com	47,000	0.10%	1
594	kovideo.net	39,000	0.10%	2
595	universal-music.co.uk	39,000	0.10%	
596	stylebop.com	43,000	0.10%	
597	shopbop.com	43,000	0.10%	
598	bunches.co.uk	43,000	0.10%	
599	east.co.uk	39,000	0.10%	
600	canstockphoto.com	35,000	0.10%	
601	catalogue-connection.co.uk	39,000	0.10%	2
602	free-stuff.co.uk	47,000	0.10%	2
603	shopwiki.com	43,000	0.10%	2
604	thewholesaler.co.uk	43,000	0.10%	2
605	iobit.mybrowserbar.com	39,000	0.10%	2
606	agentprovocateur.com	47,000	0.10%	
607	photoprintit.de	39,000	0.10%	1
608	stylecompare.co.uk	43,000	0.10%	2
609	movedancewear.com	35,000	0.10%	
610	live.bullionvault.com	58,000	0.10%	
611	outdoorsmagic.com	40,000	0.10%	2
612	as.photoprintit.de	36,000	0.10%	1
613	asda-photo.co.uk	44,000	0.10%	5
614	animal.co.uk	40,000	0.10%	
615	thejewelhut.co.uk	40,000	0.10%	5
616	anthropologie.eu	36,000	0.10%	
617	dvd.stellaartois.com	40,000	0.10%	
618	tomsshoes.co.uk	40,000	0.10%	
619	citikey.co.uk	40,000	0.10%	
620	crocs.co.uk	40,000	0.10%	

621	fredperry.com	40,000	0.10%	
622	annharveyfashion.co.uk	44,000	0.10%	
623	nordstrom.com	40,000	0.10%	
624	allaboutvision.com	33,000	0.10%	
625	celtic-sheepskin.co.uk	36,000	0.10%	
626	lets-have-a-party.co.uk	36,000	0.10%	
627	resultspage.com	44,000	0.10%	
628	ellis-brigham.com	36,000	0.10%	
629	calderdale.gov.uk	44,000	0.10%	
630	goddiva.co.uk	33,000	0.10%	
631	itshd.com	48,000	0.10%	1
632	store.diesel.com	39,000	0.10%	3
633	rupalionline.com	43,000	0.10%	
634	leapfrog.com	43,000	0.10%	1
635	hawkin.com	43,000	0.10%	
636	homesandbargains.co.uk	39,000	0.10%	
637	allsaintsarchive.com	43,000	0.10%	
638	petitionbuzz.com	36,000	0.10%	
639	amazon.ca	43,000	0.10%	
640	fortnumandmason.com	32,000	0.10%	
641	sunglasses-shop.co.uk	39,000	0.10%	
642	tommy.com	39,000	0.10%	2
643	taaz.com	39,000	0.10%	2
644	indianajones.lego.com	32,000	0.10%	2
465	coggles.com	36,000	0.10%	
646	viviennewestwood.co.uk	36,000	0.10%	
647	purseblog.com	43,000	0.10%	
648	base.com	39,000	0.10%	
649	thegiftexperience.co.uk	43,000	0.10%	
650	crafterscompanion.co.uk	39,000	0.10%	
651	easy-wellies.co.uk	39,000	0.10%	
652	wonderlandparty.com	35,000	0.10%	
653	shop.nordstrom.com	39,000	0.10%	
654	sweatshop.co.uk	35,000	0.10%	
655	babble.com	43,000	0.10%	
656	ewm.co.uk	36,000	0.10%	
657	debenhamsweddings.com	36,000	0.10%	
658	choicestore.co.uk	33,000	0.10%	
659	rokit.co.uk	36,000	0.10%	
660	wisepay.co.uk	40,000	0.10%	
661	footlocker.com	40,000	0.10%	1
662	circle.supersavvyme.co.uk	40,000	0.10%	2
663	printablecolouringpages.co.uk	36,000	0.10%	2
664	creative.lego.com	40,000	0.10%	2
665	outfit.boden.co.uk	30,000	0.10%	3
666	kodakgallery.com	33,000	0.10%	1
667	bookfinder.com	36,000	0.10%	2
668	tjhughes.co.uk	36,000	0.10%	
669	piajewellery.com	36,000	0.10%	
670	deichmann.com	36,000	0.10%	
671	flannelsfashion.com	36,000	0.10%	
672	borro.com	39,000	0.10%	2
673	thatsmystyle.co.uk	36,000	0.10%	5
674	tiffany.com	33,000	0.10%	
675	store.universal-music.co.uk	39,000	0.10%	
676	bluebanana.com	36,000	0.10%	
677	272acques-vert.co.uk	33,000	0.10%	

678	localhistories.org	36,000	0.10%	
679	thedigitalfix.co.uk	30,000	0.10%	
680	sheerluxe.com	39,000	0.10%	
681	oakley.com	36,000	0.10%	
682	wholesaleclearance.co.uk	43,000	0.10%	
683	dessy.com	39,000	0.10%	
684	lookagain.co.uk	39,000	0.10%	
685	brandalley.com	33,000	0.10%	
686	legospace.com	33,000	0.10%	
687	primarkonlineshop.com	33,000	0.10%	
688	shop.animal.co.uk	36,000	0.10%	
689	taxfreegold.co.uk	36,000	0.10%	
690	spreadshirt.com	36,000	0.10%	
691	8ball.co.uk	39,000	0.10%	
692	find-dvd.co.uk	36,000	0.10%	2
693	scottsmenswear.com	32,000	0.10%	
694	kickbacksports.co.uk	32,000	0.10%	
694	storetwentyone.co.uk	39,000	0.10%	
696	pharaohsquest.lego.com	29,000	0.10%	
697	firstworldwar.com	36,000	0.10%	
698	webkinz.com	36,000	0.10%	
699	coolest-birthday-cakes.com	43,000	0.10%	
700	hotwheels.com	36,000	0.10%	
701	cachefly.net	36,000	0.10%	2
702	b2b-trade.net	29,000	0.10%	2
703	bluenile.co.uk	36,000	0.10%	1
704	gb.zinio.com	32,000	0.10%	1
705	austinreed.co.uk	39,000	0.10%	
706	argento.co.uk	32,000	0.10%	
707	poemsource.com	32,000	0.10%	
708	denby.co.uk	29,000	0.10%	
709	fancydressnation.co.uk	39,000	0.10%	
710	thebookseller.com	39,000	0.10%	
711	halfpriceperfumes.co.uk	35,000	0.10%	
712	bhsmenswear.co.uk	39,000	0.10%	
713	273ostco.com	35,000	0.10%	
714	hawesandcurtis.com	39,000	0.10%	
715	hunter-boot.com	35,000	0.10%	
716	swshoes.co.uk	47,000	0.10%	
717	acasports.co.uk	35,000	0.10%	
718	shopeezee.co.uk	35,000	0.10%	
719	choicesuk.com	35,000	0.10%	
720	modainpelle.com	35,000	0.10%	
721	img.photobucket.com	35,000	0.10%	1
722	toysdirect.com	29,000	0.10%	
723	forums.thedigitalfix.co.uk	35,000	0.10%	2
724	kew159.com	43,000	0.10%	5
725	edeandravenscroft.co.uk	39,000	0.10%	
726	langtoninfo.co.uk	36,000	0.10%	
727	regattaoutlet.co.uk	33,000	0.10%	
728	dealio.mybrowserbar.com	36,000	0.10%	
729	watches.co.uk	36,000	0.10%	
730	sqlservercentral.com	36,000	0.10%	
731	iflorist.co.uk	27,000	0.10%	
732	prezzybox.com	36,000	0.10%	
733	photoshopessentials.com	30,000	0.10%	
734	wholesaleforum.com	36,000	0.10%	

735	eu.jimmychoo.com	33,000	0.10%	
736	my.sage.co.uk	33,000	0.10%	
737	converse.com	33,000	0.10%	
738	startriteshoes.com	33,000	0.10%	
739	bigstockphoto.com	36,000	0.10%	
740	hmvdigital.com	27,000	0.10%	
741	probikekit.com	33,000	0.10%	
742	fhinds.co.uk	30,000	0.10%	
743	whypinkfloyd.com	30,000	0.10%	
744	botb.com	33,000	0.10%	
745	pdfforge.mybrowserbar.com	40,000	0.10%	
746	aspinaloflondon.com	33,000	0.10%	
747	kickers.co.uk	30,000	0.10%	
748	jewellerymaker.com	30,000	0.10%	
749	bbclothing.co.uk	36,000	0.10%	
750	store.drmartens.co.uk	33,000	0.10%	
751	cooksongold.com	39,000	0.10%	
752	drmartens.co.uk	18,000	0.00%	
753	rohan.co.uk	33,000	0.10%	
754	atlantis.lego.com	33,000	0.10%	
755	suitsmeonline.com	33,000	0.10%	
756	mydearvalentine.com	33,000	0.10%	
757	calor.co.uk	27,000	0.10%	
758	artigiano.co.uk	32,000	0.10%	
759	ulsterbank.ie	30,000	0.10%	
760	fenwick.co.uk	32,000	0.10%	
761	urbanoutfitters.com	32,000	0.10%	5
762	amstock.co.uk	36,000	0.10%	7
763	racers.lego.com	29,000	0.10%	2
764	thestir.cafemom.com	29,000	0.10%	2
765	watches2u.com	32,000	0.10%	
766	forbiddenplanet.co.uk	27,000	0.10%	
767	polo-shirts.co.uk	39,000	0.10%	
768	shop.vans.com	29,000	0.10%	
769	gaynors.co.uk	32,000	0.10%	
770	hatsandcaps.co.uk	29,000	0.10%	
771	firetrap.com	29,000	0.10%	
772	forum.purseblog.com	36,000	0.10%	2
773	about.hm.com	840,000	1.70%	1
774	artfact.com	39,000	0.10%	2
775	noelgallagher.com	29,000	0.10%	1
776	partybritain.com	35,000	0.10%	
777	catalog.aldi.com	35,000	0.10%	
778	antiques-atlas.com	35,000	0.10%	
779	flowersdirect.co.uk	32,000	0.10%	
780	megabloks.com	32,000	0.10%	
781	julipa.com	43,000	0.10%	5
782	prettygreen.com	35,000	0.10%	
783	trimsole.com	32,000	0.10%	
784	duplo.lego.com	32,000	0.10%	
785	berghaus.com	29,000	0.10%	
786	thomassabo.com	32,000	0.10%	
787	spartoo.co.uk	35,000	0.10%	
788	simonjersey.com	35,000	0.10%	
789	brooktaverner.co.uk	30,000	0.10%	
790	wpclipart.com	27,000	0.10%	
791	waterstonesmarketplace.com	30,000	0.10%	1

792	secure.dhgate.com	170,000	0.30%	1
793	marksandspencer-appliances.com	30,000	0.10%	
794	uggstore.com.au	27,000	0.10%	1
795	hattongardenmetals.com	27,000	0.10%	
796	soletrader.co.uk	30,000	0.10%	
797	a1gifts.co.uk	27,000	0.10%	
798	photographersdirect.com	33,000	0.10%	
799	hein-gericke.co.uk	30,000	0.10%	
800	starstore.com	27,000	0.10%	
801	webtogs.co.uk	27,000	0.10%	
802	imag-e-nation.com	30,000	0.10%	
803	oxendales.co.uk	33,000	0.10%	
804	swpp.co.uk	36,000	0.10%	
805	swatch.com	24,000	0.00%	
806	mytheresa.com	30,000	0.10%	
807	reviews.debenhams.com	2,900,000	5.70%	
808	dollshouse.com	24,000	0.00%	
809	urbanpath.com	30,000	0.10%	
810	bleedingcool.com	33,000	0.10%	
811	awear.com	33,000	0.10%	1
812	trespass.co.uk	30,000	0.10%	
813	gallery.hd.org	30,000	0.10%	2
814	startfitness.co.uk	30,000	0.10%	
815	wellywarehouse.co.uk	27,000	0.10%	
816	chinasearch.co.uk	24,000	0.00%	
817	soccerbible.com	27,000	0.10%	
818	flyingflowers.co.uk	27,000	0.10%	
819	omegatravel.net	32,000	0.10%	
820	urbanindustry.co.uk	27,000	0.10%	
821	sexyher.co.uk	32,000	0.10%	
822	twoseasons.co.uk	29,000	0.10%	4
823	glow.co.uk	29,000	0.10%	
824	hosted.exlibrisgroup.com	29,000	0.10%	
825	wraplondon.co.uk	29,000	0.10%	
826	countryattire.com	32,000	0.10%	
827	thejewellerychannel.tv	32,000	0.10%	
828	musicstack.com	27,000	0.10%	
829	zeeandco.co.uk	29,000	0.10%	
830	cosyfeet.com	29,000	0.10%	
831	emmabridgewater.co.uk	29,000	0.10%	
832	eil.com	29,000	0.10%	
833	shop.thomassabo.com	29,000	0.10%	
834	tributeballoon.com	29,000	0.10%	
835	russellandbromley.co.uk	27,000	0.10%	
836	johnlewispartnership.co.uk	32,000	0.10%	
837	corsets-uk.com	29,000	0.10%	
838	unrealitymag.com	32,000	0.10%	
839	musto.com	29,000	0.10%	
840	eu.wiley.com	32,000	0.10%	
841	bionicle.lego.com	24,000	0.00%	2
842	toywiz.com	29,000	0.10%	1
843	lyleandscott.com	32,000	0.10%	
844	puma.co.uk	17,000	0.00%	1
845	owntherunway.com	32,000	0.10%	4
846	landsend.com	29,000	0.10%	1
847	im.qq.com	32,000	0.10%	1
848	coins-of-the-uk.co.uk	29,000	0.10%	2

849	best-trends-for-friends.co.uk	29,000	0.10%	2
850	eflorist.co.uk	26,000	0.10%	
851	kdp.amazon.com	29,000	0.10%	1
852	tiso.com	29,000	0.10%	
853	luxuryleathergoods.com	27,000	0.10%	
854	craftsuprint.com	25,000	0.00%	
855	i18nguy.com	25,000	0.00%	
856	inthepaper.co.uk	30,000	0.10%	
857	vanmildert.com	25,000	0.00%	
858	britishinformation.com	25,000	0.00%	
859	snazal.com	27,000	0.10%	
860	blockbuster.com	30,000	0.10%	
861	americanapparel.net	30,000	0.10%	2
862	fossil.co.uk	33,000	0.10%	
863	cheshireoaksdesigneroutlet.com	27,000	0.10%	2
864	shopperhive.co.uk	30,000	0.10%	2
865	www-ssl.bestbuy.co.uk	27,000	0.10%	8
866	bonusprint.com	27,000	0.10%	1
867	greatglam.com	22,000	0.00%	1
868	pollypocket.com	27,000	0.10%	1
869	dotcomgiftshop.com	33,000	0.10%	
870	dickiesstore.co.uk	30,000	0.10%	
871	cheapestfancydress.co.uk	27,000	0.10%	
872	hardcloud.com	27,000	0.10%	
873	jamesandjames.com	27,000	0.10%	
874	weddings.about.com	25,000	0.00%	
875	londonmintoffice.org	27,000	0.10%	
876	philipmorrisdirect.co.uk	27,000	0.10%	
877	bloomindelightful.co.uk	27,000	0.10%	
878	go4awalk.com	27,000	0.10%	
879	show.qq.com	30,000	0.10%	
880	popular.ebay.com	25,000	0.00%	
881	tmall.com	33,000	0.10%	1
882	beadsdirect.co.uk	33,000	0.10%	
883	sillyjokes.co.uk	30,000	0.10%	
884	waitrosejobs.com	27,000	0.10%	
885	htcsense.com	27,000	0.10%	
886	specialized.com	30,000	0.10%	
887	asda-flowers.co.uk	27,000	0.10%	
888	free-scores.com	24,000	0.00%	
889	menswear.mainlinemenswear.co.uk	24,000	0.00%	
890	remotesupportid.sage.co.uk	27,000	0.10%	
891	theworks.co.uk	24,000	0.00%	
892	service.lego.com	30,000	0.10%	2
893	forum.blu-ray.com	22,000	0.00%	2
894	emails.houseoffraser.co.uk	24,000	0.00%	2
895	mixb.jp	24,000	0.00%	1
896	mythings.com	33,000	0.10%	1
897	partystuffonline.co.uk	22,000	0.00%	4
898	old-maps.co.uk	30,000	0.10%	2
899	planet.co.uk	27,000	0.10%	
900	newsletter.brandalley.com	27,000	0.10%	
901	brastop.com	24,000	0.00%	4
902	tower.com	24,000	0.00%	7
903	omegawatches.com	27,000	0.10%	1
904	williamsandbrown.co.uk	29,000	0.10%	5
905	createsend2.com	22,000	0.00%	7

906	lensway.co.uk	27,000	0.10%	1
907	spongebob.lego.com	24,000	0.00%	2
908	hushpuppies.com	32,000	0.10%	1
909	nicekicks.com	27,000	0.10%	1
910	qassimy.com	27,000	0.10%	1
911	surplusandoutdoors.com	27,000	0.10%	4
912	application-form.org	27,000	0.10%	2
913	activitysuperstore.com	27,000	0.10%	
914	ohsocherished.co.uk	29,000	0.10%	
915	mintvelvet.co.uk	29,000	0.10%	
916	a2z-kids.co.uk	29,000	0.10%	
917	gettyimages.com	27,000	0.10%	
918	emails.secretsales.com	24,000	0.00%	
919	123pricecheck.com	24,000	0.00%	
920	cdn3.123rf.com	24,000	0.00%	
921	stockingshq.com	27,000	0.10%	
922	myoutlets.co.uk	24,000	0.00%	2
923	watchuseek.com	27,000	0.10%	1
924	shop.puma.co.uk	29,000	0.10%	1
925	standard.co.uk	680,000	1.30%	2
926	chockersshoes.co.uk	27,000	0.10%	
927	blakeflannery.hubpages.com	22,000	0.00%	
928	forums.watchuseek.com	24,000	0.00%	
929	clikpic.com	29,000	0.10%	
930	danda.co.uk	27,000	0.10%	
931	daisytrail.com	22,000	0.00%	
932	buycostumes.com	29,000	0.10%	1
933	zanox.com	26,000	0.10%	2
934	prositehosting.co.uk	24,000	0.00%	7
935	visiondirect.co.uk	29,000	0.10%	1
936	motelrocks.com	26,000	0.10%	
937	lacoste.com	29,000	0.10%	
938	sparklingstrawberry.com	22,000	0.00%	
939	brora.co.uk	24,000	0.00%	
940	sockshop.co.uk	25,000	0.00%	
941	superherohype.com	30,000	0.10%	2
942	gillyhicks.com	25,000	0.00%	4
943	email.lauraashley.com	25,000	0.00%	2
944	mirrorreaderoffers.co.uk	27,000	0.10%	
945	garageshoes.co.uk	25,000	0.00%	
946	email.waterstones.com	22,000	0.00%	
947	surplusandadventure.com	25,000	0.00%	
948	speedo.co.uk	--	0.00%	
949	shop-uk.lacoste.com	27,000	0.10%	
950	letterbox.co.uk	22,000	0.00%	
951	prodirectrugby.com	22,000	0.00%	
952	discountcyclesdirect.co.uk	25,000	0.00%	
953	webalbum.bonusprint.com	20,000	0.00%	
954	running.sweatshop.co.uk	25,000	0.00%	
955	bountyweb.co.uk	27,000	0.10%	
956	pt-pt.facebook.com	27,000	0.10%	
957	prada.com	22,000	0.00%	
958	firebrandlive.com	22,000	0.00%	
959	convio.net	27,000	0.10%	
960	themall.co.uk	27,000	0.10%	
961	bargainplace.co.uk	25,000	0.00%	2
962	justlastseason.co.uk	25,000	0.00%	5

963	vogue.com.au	27,000	0.10%	2
964	governmentauctionsuk.com	27,000	0.10%	2
965	store.berghaus.com	29,000	0.10%	
966	coxandcox.co.uk	20,000	0.00%	
967	presentsformen.co.uk	27,000	0.10%	
968	bestofferbuy.com	24,000	0.00%	
969	278olka.pl	24,000	0.00%	
970	onestopplus.co.uk	24,000	0.00%	
971	celticsuperstore.co.uk	22,000	0.00%	5
972	stockshifters.com	24,000	0.00%	2
973	melodymaison.co.uk	22,000	0.00%	
974	prod.fadvhms.com	24,000	0.00%	2
975	thediamondstore.co.uk	24,000	0.00%	
976	wwrd.com	22,000	0.00%	
977	bca-online-auctions.co.uk	18,000	0.00%	
978	visitsouthport.com	24,000	0.00%	
979	cdn4.123rf.com	20,000	0.00%	
980	football-shirts.co.uk	22,000	0.00%	
981	isabellaoliver.com	22,000	0.00%	
982	christianlouboutin.com	24,000	0.00%	1
983	contactlenses.co.uk	27,000	0.10%	
984	optimalprint.co.uk	24,000	0.00%	
985	toyshopuk.co.uk	24,000	0.00%	
986	dare2b.com	20,000	0.00%	
987	thedogsdoodahs.com	20,000	0.00%	
988	powerminers.lego.com	27,000	0.10%	
989	s.taobao.com	24,000	0.00%	
990	drapersonline.com	24,000	0.00%	
991	shoestudio.com	24,000	0.00%	5
992	tradetang.com	24,000	0.00%	1
993	yours.co.uk	29,000	0.10%	
994	viyella.co.uk	27,000	0.10%	1
995	secure.legoland.co.uk	93,000	0.20%	2
996	berketexbride.com	24,000	0.00%	2
997	myshopping.com.au	24,000	0.00%	1
998	teds-shed.com	24,000	0.00%	5
999	woodhouseclothing.com	24,000	0.00%	
1000	backstreet-merch.com	29,000	0.10%	

Rejection Code	**Number of websites**	**Rejection Description**
1		The sampling frame URL did not link to a website that was owned or operated by an organisation incorporated within the U.K.
2		The sampling frame URL did not link to a website that conformed to e-the commerce definition
3		The sampling frame URL was a subdomain that was part of a top-level domain that had already been included within the sample
4		The sampling frame URL linked to a website where there was insufficient evidence to determine whether or not the organisation operating the website was incorporated within the U.K.
5		The sampling frame URL linked to a website that was owned or operated by an organisation or group that has already been included within the sample or had previously appeared within the sampling frame
6		The sampling frame URL did not link to a homepage
7		There was a technical error with website
8		Website had ceased trading

Appendix C: Phase One Sample

Highlighted dark grey: Excluded from 2012 sample (18 websites) leaving 182 websites

Highlighted light blue: Excluded from 2015 sample (17 websites) leaving 165 websites

Sample No	Website	Unique visitors	Date coded 2012	Date coded 2015	Rejection code
1	tesco.com	7,400,000	06/02	06/04	
2	argos.co.uk	7,400,000	06/02	06/04	
3	debenhams.com	2,900,000	06/02	06/04	
4	sainsburys.co.uk	2,100,000	06/02	06/04	
5	sportsdirect.com	1,400,000	06/02	06/04	
6	riverisland.com	1,300,000	07/02	07/04	
7	dorothyperkins.com	830,000	07/02	07/04	
8	qvcuk.com	750,000	07/02	07/04	
9	moonpig.com	620,000	07/02	07/04	
10	clarks.co.uk	620,000	07/02	07/04	
11	24studio.co.uk	520,000	08/02	08/04	
12	tkmaxx.com	510,000	08/02	08/04	
13	laredoute.co.uk	430,000	08/02	08/04	
14	office.co.uk	430,000	08/02	08/04	
15	gooutdoors.co.uk	360,000	08/02	08/04	
16	elc.co.uk	350,000	09/02	09/04	
17	marisota.co.uk	350,000	09/02	09/04	
18	warehouse.co.uk	290,000	09/02	09/04	
19	blockbuster.co.uk	290,000	09/02		1
20	notonthehighstreet.com	290,000	09/02	09/04	
21	bid.tv	270,000	10/02		1
22	jacquielawson.com	260,000	10/02	09/04	
23	everything5pounds.com	260,000			2
24	bankfashion.co.uk	240,000	10/02		1
25	bonprixsecure.com	220,000	10/02	10/04	
26	interflora.co.uk	220,000	10/02	10/04	
27	mandco.com	220,000	13/02	10/04	
28	bookdepository.co.uk	220,000	13/02	10/04	
29	secretsales.com	220,000			2
30	whitestuff.com	200,000			2
31	barratts.co.uk	200,000	13/02	10/04	
32	coast-stores.com	180,000	13/02	13/04	
33	cathkidston.co.uk	180,000	13/02	13/04	
34	cloggs.co.uk	180,000	14/02	13/04	
35	bonmarche.co.uk	180,000	14/02	13/04	
36	surfdome.com	170,000	14/02	13/04	
37	missguided.co.uk	170,000	14/02	14/04	
38	janenorman.co.uk	160,000	14/02	14/04	
39	hobbs.co.uk	160,000	15/02	14/04	
40	ernestjones.co.uk	160,000	15/02	14/04	
41	theoutnet.com	150,000	15/02	14/04	
42	makro.co.uk	150,000	15/02	15/04	
43	yoursclothing.co.uk	140,000	15/02	15/04	
44	millets.co.uk	130,000	16/02	15/04	
45	thetoyshop.com	130,000	16/02	15/04	
46	thewatchhut.co.uk	130,000	16/02		2
47	kurtgeiger.com	130,000	16/02	15/04	
48	dune.co.uk	120,000	16/02	16/04	

49	cotswoldoutdoor.com	120,000	17/02	16/04	
50	my-wardrobe.com	120,000	17/02		3
51	goldsmiths.co.uk	120,000	17/02	16/04	
52	uniqlo.com	110,000	17/02	16/04	
53	ctshirts.co.uk	110,000	17/02	16/04	
54	reissonline.com	110,000	20/02	17/04	
55	fancydress.com	110,000	20/02		2
56	uggaustralia.co.uk	100,000	20/02	17/04	
57	redletterdays.co.uk	100,000	20/02	17/03	
58	joebrowns.co.uk	100,000	20/02	17/04	
59	find-me-a-gift.co.uk	93,000	21/02	17/04	
60	greenfingers.com	92,000	21/02		4
61	harveynichols.com	92,000	21/02	20/04	
62	poundland.co.uk	85,000	21/02	20/04	
63	partypieces.co.uk	85,000	21/02	20/04	
64	tmlewin.co.uk	84,000	22/02	20/04	
65	mulberry.com	84,000	22/02	20/04	
66	fashionunion.com	84,000	22/02		5
67	mountainwarehouse.com	84,000	22/02	21/04	
68	barbourbymail.co.uk	83,000	22/02		6
69	wynsors.com	83,000	23/02	21/04	
70	gb.com	77,000	23/02	21/04	
71	linksoflondon.com	77,000	23/02	21/04	
72	getpark.co.uk	77,000	23/02	21/04	
73	gltc.co.uk	76,000	23/02	22/04	
74	crewclothing.co.uk	76,000	24/02	22/04	
75	jonesbootmaker.com	76,000	24/02	22/04	
76	cards.hallmark.co.uk	70,000	24/02	22/04	
77	thorntons.co.uk	69,000	24/02	22/04	
78	jigsaw-online.com	69,000	24/02	23/04	
79	beaverbrooks.co.uk	69,000	27/02	23/04	
80	sportsshoes.com	68,000	27/02	23/04	
81	bananarepublic.gap.co.uk	64,000	27/02	23/04	
82	snowandrock.com	64,000	27/02	23/04	
83	shoezone.com	64,000	27/02	24/04	
84	hotelchocolat.co.uk	64,000	28/02	24/04	
85	selectfashion.co.uk	64,000	28/02	24/04	
86	gems.tv	63,000	28/02		3
87	serenataflowers.com	59,000	28/02	24/04	
88	pumpkinpatch.co.uk	58,000			7
89	liberty.co.uk	58,000	28/02	24/04	
90	conrad-uk.com	58,000	29/02	27/04	
91	purecollection.com	57,000	29/02	27/04	
92	longtallsally.com	57,000	29/02	27/04	
93	gonedigging.co.uk	57,000	29/02	27/04	
94	rideaway.co.uk	57,000	29/02	27/04	
95	visionexpress.com	57,000	01/03	28/04	
96	trekwear.co.uk	53,000	01/03	28/04	
97	axparis.co.uk	53,000	01/03	28/04	
98	dwsports.com	52,000	01/03	28/04	
99	pasttimes.com	52,000	01/03		1
100	truffleshuffle.co.uk	52,000	02/03	28/04	
101	clifford-james.co.uk	48,000	02/03	29/04	
102	duoboots.com	48,000	02/03	29/04	
103	anniversaryideas.co.uk	48,000	02/03	29/04	
104	reebok.com	48,000			7
105	rugbystore.co.uk	47,000	02/03	29/04	
106	fitflop.com	47,000	05/03	29/04	

107	craghoppers.com	47,000	05/03	30/04	
108	arkclothing.com	47,000	05/03	30/04	
109	virginexperiencedays.co.uk	47,000	05/03	30/04	
110	weareelectricals.com	47,000	05/03		1
111	agentprovocateur.com	47,000			2
112	chums.co.uk	44,000	06/03	30/04	
113	adams.co.uk	44,000	06/03	30/04	
114	acefancydress.co.uk	44,000	06/03		1
115	annharveyfashion.co.uk	44,000	06/03		3
116	ccfashion.co.uk	43,000	06/03	01/05	
117	farfetch.com	43,000	07/03	01/05	
118	chelseamegastore.com	43,000	07/03	01/05	
119	bench.co.uk	43,000	07/03	01/05	
120	rupalionline.com	43,000	07/03	01/05	
121	hawkin.com	43,000	07/03	04/05	
122	wholesaleclearance.co.uk	43,000	08/03	04/05	
123	animal.co.uk	40,000	08/03	04/05	
124	fredperry.com	40,000	08/03	04/05	
125	bullionbypost.co.uk	39,000	08/03	04/05	
126	cyclestore.co.uk	39,000			2
127	universal-music.co.uk	39,000	08/03	05/05	
128	sunglasses-shop.co.uk	39,000	09/03	05/05	
129	easy-wellies.co.uk	39,000	09/03	05/05	
130	8ball.co.uk	39,000	09/03	05/05	
131	austinreed.co.uk	39,000			8
132	bhsmenswear.co.uk	39,000			8
133	edeandravenscroft.co.uk	39,000	09/03	06/05	
134	cooksongold.com	39,000	09/03	06/05	
135	anthropologie.eu	36,000	12/03	06/05	
136	coggles.com	36,000	12/03	06/05	
137	tjhughes.co.uk	36,000	12/03	06/05	
138	piajewellery.com	36,000	12/03	07/05	
139	flannelsfashion.com	36,000			2
140	oakley.com	36,000	12/03	07/05	
141	prezzybox.com	36,000	13/03	07/05	
142	movedancewear.com	35,000	13/03	07/05	
143	wonderlandparty.com	35,000	13/03	07/05	
144	halfpriceperfumes.co.uk	35,000			2
145	partybritain.com	35,000	13/03	08/05	
146	prettygreen.com	35,000	13/03	08/05	
147	tiffany.com	33,000	14/03	08/05	
148	probikekit.com	33,000	14/03	08/05	
149	fossil.co.uk	33,000	14/03	08/05	
150	dotcomgiftshop.com	33,000	14/03	11/05	
151	beadsdirect.co.uk	33,000			2
152	scottsmenswear.com	32,000			8
153	argento.co.uk	32,000	14/03	11/05	
154	watches2u.com	32,000	15/03	11/05	
155	trimsole.com	32,000			2
156	sexyher.co.uk	32,000	15/03		5
157	lyleandscott.com	32,000	15/03	11/05	
158	fhinds.co.uk	30,000	15/03	11/05	
159	marksandspencer-appliances.com	30,000	15/03		5
160	imag-e-nation.com	30,000			2
161	trespass.co.uk	30,000	16/03	12/05	
162	startfitness.co.uk	30,000	16/03	12/05	
163	sillyjokes.co.uk	30,000	16/03	12/05	

164	toysdirect.com	29,000	16/03	12/05	
165	firetrap.com	29,000			8
166	glow.co.uk	29,000	16/03	12/05	
167	emmabridgewater.co.uk	29,000	19/03	13/05	
168	eil.com	29,000			2
169	tiso.com	29,000	19/03	13/05	
170	ohsocherished.co.uk	29,000	19/03	13/05	
171	mintvelvet.co.uk	29,000	19/03	13/05	
172	a2z-kids.co.uk	29,000	19/03	13/05	
173	store.berghaus.com	29,000	20/03	14/05	
174	yours.co.uk	29,000	20/03	14/05	
175	iflorist.co.uk	27,000	20/03	14/05	
176	forbiddenplanet.co.uk	27,000	20/03	14/05	
177	hattongardenmetals.com	27,000	20/03	14/05	
178	webtogs.co.uk	27,000	21/03	15/05	
179	luxuryleathergoods.com	27,000	21/03	15/05	
180	cheapestfancydress.co.uk	27,000	21/03		5
181	hardcloud.com	27,000	21/03	15/05	
182	planet.co.uk	27,000	21/03	15/05	
183	activitysuperstore.com	27,000	22/03	15/05	
184	stockingshq.com	27,000	22/03	18/05	
185	chockersshoes.co.uk	27,000	22/03	18/05	
186	mirrorreaderoffers.co.uk	27,000	22/03	18/05	
187	contactlenses.co.uk	27,000	22/03	18/05	
188	eflorist.co.uk	26,000	23/03	18/05	
189	motelrocks.com	26,000	23/03	19/05	
190	garageshoes.co.uk	25,000	23/03	19/05	
191	discountcyclesdirect.co.uk	25,000	23/03	19/05	
192	theworks.co.uk	24,000	23/03	19/05	
193	thediamondstore.co.uk	24,000	26/03	19/05	
194	woodhouseclothing.com	24,000	26/03	20/05	
195	daisytrail.com	22,000	26/03	20/05	
196	prodirectrugby.com	22,000	26/03	20/05	
197	melodymaison.co.uk	22,000	26/03	20/05	
198	isabellaoliver.com	22,000			2
199	coxandcox.co.uk	20,000	27/03	20/05	
200	drmartens.co.uk	18,000	27/03	21/05	

Rejection Code	**Number of websites**	**Rejection Description**
1	6	The website has ceased trading
2	15	The privacy policy could not be found on the website
3	3	Website assets sold to another group
4	1	The link to the privacy policy did not work
5	3	The website was not available to view
6	1	The website has been replaced by two different websites
7	2	Collecting data under legislation of another country
8	4	Website was part of another group already included within this sample

Appendix D: Phase One Coding Scheme

Coding Instructions

Step 1: Navigate to the website specified on the sampling list. Check to see if the website has published a privacy policy. If the website has not published a privacy policy, it should be excluded from this study. If the website does have a privacy policy go to step 2.

Step 2: Open the coding framework template in Microsoft Excel.

Step 3: Complete section 1 of the coding framework.

Step 4: Copy the privacy policy and other personal data processing information, including security policy and or cookie policy into separate Microsoft Word documents for each published page.

Step 5: Complete sections 2 to 10 of the coding framework.

Step 6: Open the SPSS tab on the coding framework. Check the validation section to ensure that all variables have been entered. Copy the line of numerical values into SPSS.

Step 7: Copy the string value(s) entered for variable 4.3 into the string analysis Microsoft Excel document.

Step 8: Save and close the coding framework. Use the year, sample number and website URL as the file name, for example 2012_001_Tesco, 2012_002_Argos.

Throughout the coding exercise refer to the instructions set out below for details about how each variable is operationalised and examples of coding. The coding instructions below make reference to screenshots that can be found in appendix E.

Section 1: Format

1.1	Is the privacy policy presented in a layered format?		
	No	0	The privacy policy is not presented in a layered format.
	Yes	1	The privacy policy is presented in a layered format.
Operationalisation: In an online context, a layered privacy policy is presented over two or more pages with an incremental build-up of the amount of information presented. The first layer or page a user would encounter is considered the short notice and should contain the identity of the data controller and the purposes for processing personal data. The short layer should also contain a link to a second layer or more detailed notice or page that presents a full account of organisational personal data handling practices. This follows the guidelines published by the Information Commissioner's Office (2010) and The Article 29 Working Party (2004).			
Examples: Yes 1. Screenshots 1 and 2 provide more detail.			

Section 2: Effective Date

2.1	Does the privacy policy state when the policy was last updated?		
	No	0	The privacy policy does not mention when it was last updated.
	Yes	1	The privacy policy does mention when the policy was last updated.
Operationalisation: Yes The privacy policy must contain a date, in any format, mentioning when the policy was either last reviewed/updated or became effective.			
Examples: Yes Screenshot 3 provides more detail.			

Section 3: Data Controller Identity and Purposes for Processing

3.1	Does the privacy policy explicitly mention the identity of the data controller?		
	No	0	The privacy policy does not explicitly state the identity of the data controller.
	Yes	1	The privacy policy explicitly states the identity of the data controller.
Operationalisation: Yes A privacy policy may state: "the data controller is company A" or "for the purposes of the data protection act Company A is registered as a data controller." In each of those instances the identity of the data controller is explicitly stated within the privacy policy. Additionally, the privacy policy might state the name of an organisation under the headings of "Data Controller". In this instance, the privacy policy should also be considered as explicitly stating the identity of the data controller.			
Examples Yes 1. For the purposes of the Data Protection Act 1998 (the "Act"), the data controller is Company X of 440-450 Cob Drive, Swan Valley, Northampton, NN4 9BB, registered in England and Wales with company number 508746.			

2. For the purpose of the Data Protection Act 1998 (the Act), the data controller is Company Y of 12 Colima Avenue, Sunderland Enterprise Park, Sunderland, SR5 3XB.

3.2	If no to 3.1, is it possible to infer who the data controller is from the privacy policy?		
	No	0	It is not possible to infer the identity of the data controller from the privacy policy.
	Yes	1	It is possible to infer the identity of the data controller from the privacy policy.

Operationalisation:

Yes
A privacy policy might state: “company A uses your information as outlined below” or “company A protects your privacy”. In those two instances, it could be inferred that company A is the data controller. Additionally, a privacy policy might include a company address and this could also be used to infer who the data controller is. Ultimately, if the privacy policy includes a company name this could be inferred to be the data controller.

Examples

Yes
1. At Company Z we are committed to protecting your privacy. Company Z will only use the information that is collected about you in accordance with the Data Protection Act 1998.

2. By entering your details in the fields requested, you enable Company A Ltd and its service providers to provide you with the services you select. Whenever you provide such personal information, we will treat that information in accordance with this policy. Our services are designed to give you the information that you want to receive. Company A Ltd will act in accordance with current legislation and aim to meet current Internet best practice.

3.3	Does the privacy policy identify the purpose or purposes for which personal data will be processed?		
	No	0	The privacy policy does not state any purpose or purposes for which personal data obtained through the website is processed.
	Yes	1	The privacy policy states the purpose or purposes for which personal data is processed.

Operationalisation:

Yes
A privacy policy might state: “Company A uses your personal data to process orders, contact you about further promotions and personalise offerings to you.” In this instance, the privacy policy has stated the purposes for which personal data is processed.

Examples:

Yes
1. We confirm that your Personal Information is held in accordance with the registration We have with the Information Commissioner’s Office We only use your personal Information for the following purposes:

a) Processing your Orders;
b) For statistical purposes to improve this Website and its services to You;
c) To administer this Website;
d) Other use by Us to which You agree when asked on this Website.

2. What we do with the information we gather
We require this information to understand your needs and provide you with a better service, and in particular for the following reasons:

- Fulfillment of your orders and the provision of our services

- Internal record keeping.
- We may use the information to improve our products and services.
- We may periodically send promotional emails about new products, special offers or other information which we think you may find interesting using the email address which you have provided.

From time to time, we may also use your information to contact you for market research purposes. We may contact you by email, phone, fax or mail. We may use the information to customise the website according to your interests.

3.4	Does the privacy policy identify a named individual to contact regarding personal data processing?		
	No	0	The privacy policy does not state the name of an individual to contact regarding personal data processing.
	Yes	1	The privacy policy does state the name of an individual to contact regarding personal data processing.
Operationalisation: Yes A privacy policy might state: “Contact Mr PhD for further information about how your personal data is processed.” In this instance, the privacy policy has stated the name of an individual to contact regarding personal data processing.			
Examples Yes 1. Our nominated representative for the purpose of the Act is Bob Collins.			

Section 4: Personal Data Sharing for Direct Marketing Purposes

4.1	Does the privacy policy mention that personal data is or might be shared for direct marketing purposes (with or without the consent of the user)?		
	No	0	The privacy policy does not mention that personal data is or might be shared for direct marketing with or without the consent of the user.
	Yes	1	The privacy policy states that personal data is or might be shared with a third party for the purpose of direct marketing with or without the consent of the user.
	Open to interpretation		The privacy policy has mentioned something to suggest that personal data may be shared for direct marketing purposes but it is not entirely clear whether or not personal data is or might be shared.
Operationalisation: Yes A privacy policy might state: “we may share your personal data with third parties so they can contact you by mail about their products.” In this instance, the privacy policy has stated that personal data *might* be shared with a third party for direct marketing. Further to this, the privacy policy might state: “if you have consented, we will share your name and address with selected third parties so they can inform you about products that may interest you.” In this instance, the privacy policy has stated that personal data *will* be shared with a third party if the user has given their consent. In both of the examples stated the privacy policy has mentioned that personal data *is or might* be shared for direct marketing purposes. Open to interpretation A privacy policy may state: “we may send you information in connection with our joint marketing partners.” Does this mean that personal data is shared with these joint marketing partners? It is open to interpretation and therefore should be coded this way.			

Examples:

Yes

1. We may share your information with other organisations. We or they may contact you for marketing purposes by mail, telephone, e-mail or otherwise. If you do not wish to be contacted by other organisations for marketing purposes please write to Marketing Administration Dept.

Open to interpretation

1. Updates and Promotional offers: if you have consented in advance we send you updates and information on our promotional offers. These may include joint promotions with our business partners. If you no longer want to receive such offers, please notify us by emailing us at privacy@companyV.co.uk.

4.2	If yes to 4.1, does the privacy policy mention with whom personal data will be shared?		
	No	0	The privacy policy does not state who personal data is shared with for direct marketing purposes.
	Yes	1	The privacy policy does state who personal data is shared with for direct marketing purposes.

Operationalisation:

No

A privacy policy might state: “your personal data is disclosed for marketing purposes.” In this instance, the privacy policy does not state who personal data is shared with.

Yes

A privacy policy might state: “your personal information is shared with carefully selected third parties for marketing purposes.” In this instance, the privacy policy has mentioned who personal data is shared with, this being carefully selected third parties.

Examples:

Yes

1. Occasionally our list of customers' names and addresses is made available to other carefully screened companies whose products and services may be of interest to you. You have the ability to opt-out during the registration process.

2. We may pass your information onto one of our business partners or to other selected third parties to enable them to send you information which may be of interest to you but only if you have given us permission to do so. You can tell us to stop this at any time by sending an e-mail to customerservices@companyU.com.

4.3	If yes to 4.2, with whom is personal data shared?	
	Names:	

Operationalisation:

This is the name or names of that organisation(s) that personal data is shared with for direct marketing purposes. This is taken directly from the privacy policy.

If the same name appears more than once within the privacy policy both instances should be recorded. For example, if the privacy policy states: “Your personal data is shared with other organisations so that they can send you information about their products and services by email” and then goes on to state: “other organisations will have access to your personal data to send you marketing emails” the term “other organisations” should only be recorded twice.

4.4	If yes to 4.2, are any names of organisations mentioned?		
	No	0	The privacy policy does not mention the name of an organisation or organisations who personal data is shared with for direct marketing purposes.
	Yes	1	The privacy policy does mention the name of an organisation or organisations who personal data is shared with for direct marketing purposes.
Operationalisation: <u>No</u> A privacy policy might state: “personal data might be shared with other companies for their marketing activities.” In this instance, the privacy policy does not state the *actual name* of the organisation that personal data is shared with. <u>Yes</u> A privacy policy may state: “if you have agreed we will share your personal information with PhD Products Ltd so they can offer you services and products via email.” In this instance, the privacy policy has specified *the name* of the organisation that personal data is shared with for direct marketing purposes, in this case being PhD Products Ltd. Further examples can be found in section 7 of appendix X.			
Examples: <u>Yes</u> 1. Company Z may, from time to time, share your personal information with its affiliated company, Offspring. Offspring may contact you by post or by electronic mail services about new products, special offers or other information which we think you may find interesting using the delivery or email address which you have provided. 2. We may share your details with other members of the Company D Group and those members may contact you by mail, telephone, email or any other reasonable method. We may share your detail with our former sister companies, Company E and Company F.			

Section 5: Accessing and Amending

5.1	Does the privacy policy mention that it is possible to view or amend personal data?		
	No	0	The privacy policy does not mention that it is possible to view or amend personal data.
	Yes	1	The privacy policy mentions that it is possible to view or amend personal data.
Operationalisation: <u>Yes</u> A privacy policy may state: “You can view your personal data by logging into your online account or writing to us” or “You have the right to view your personal information”. In both instances, the privacy policy mentions that it is possible to view or amend personal data. However, the privacy policy does not have to mention how personal data is viewed or amended. This is not a consideration for this variable. To be coded as yes, the privacy policy only has to provide the user with the choice or option to access or amend personal data.			
Examples: <u>Yes</u> 1. The information we hold will be accurate and up to date. You can check the information that we hold about you by emailing sales@companyG.co.uk. If you find any inaccuracies we will delete or correct it promptly. 2. If you would like to revise the information you have provided to us, or feel that what we currently have on record is incorrect, you may update the information by emailing: info@companyJ.com.			

<table>
<tr><td rowspan="3">5.2</td><td colspan="3">Does the privacy policy mention anything about how personal data being processed by the organisation can be viewed or amended?</td></tr>
<tr><td>No</td><td>0</td><td>The privacy policy does not mention how personal data can be viewed or amended.</td></tr>
<tr><td>Yes</td><td>1</td><td>The privacy policy does mention how to view or amend personal data being processed.</td></tr>
<tr><td colspan="4">Operationalisation:

Yes
A privacy policy might state: “to view your personal data log into your account” or “to exercise the right to view your personal data please write to us at the following address”. In both instances, the privacy policy provides the user with a method to view or amend personal data.</td></tr>
<tr><td colspan="4">Examples:

Yes
1. The information we hold will be accurate and up to date. You can check the information that we hold about you by emailing us or by checking the 'My Account' section of the website. If you find any inaccuracies we will delete or correct it promptly.

2. We want to make sure that the information we hold about you is correct and up to date at all times. You can at any time amend or update your information by clicking here to log in and update your details.

You are entitled to ask for a copy of the information we hold about you (for which we may charge a small fee).</td></tr>
</table>

<table>
<tr><td rowspan="3">5.3</td><td colspan="3">Does the privacy policy mention that it is the right of the user to request a copy of the personal data being processed?</td></tr>
<tr><td>No</td><td>0</td><td>The privacy policy does not mention that it is the right of the user to request a copy of their personal data.</td></tr>
<tr><td>Yes</td><td>1</td><td>The privacy policy does mention that it is the right of the user to request a copy of their personal data.</td></tr>
<tr><td colspan="4">Operationalisation:

No
A privacy policy might state: “You can view or amend your personal data by logging into your account.” In this instance, the privacy policy has not mentioned that it is the right of the user access a copy their personal data being processed.

Yes
A privacy policy may state: “you are entitled to a copy of your personal data under the Data Protection Act 1998” or “you have to right to view your personal data”. In both instances, the privacy policy does mention that it is the right of the user to request a copy of their personal data. However, the privacy policy does not have to explicitly mention that it is the right of the user to request a copy of personal data to be coded as a yes for this variable. Statements such as “you can request a copy of your personal data” that appear under a “your rights” heading should also be coded as a yes.</td></tr>
<tr><td colspan="4">Examples:

Yes
1. You have the right to contact us (see paragraph 10 below) in order to find out what information we hold about you (please note that a small fee may be payable) or to access or correct any information we hold about you.

2. Your rights:</td></tr>
</table>

You may instruct us to provide you with any personal information we hold about you. Provision of such information may be subject to the payment of a fee (currently fixed at £10.00).

<table>
<tr><td rowspan="3">5.4</td><td colspan="3">Does the privacy policy mention that it is the right of the user to amend inaccurate personal data being processed?</td></tr>
<tr><td>No</td><td>0</td><td>The privacy policy does not mention that it is the right of the user to amend inaccurate personal data.</td></tr>
<tr><td>Yes</td><td>1</td><td>The privacy policy does mention that it is the right of the user to amend inaccurate personal data.</td></tr>
<tr><td colspan="4">Operationalisation:

<u>No</u>
A privacy policy might state: “you can view or amend your personal data by writing to us.” In this instance, the privacy policy does not mention that it is the right of the user to amend inaccurate personal data being processed.

<u>Yes</u>
A privacy policy might state: “you have the right to amend your personal information” or “you are entitled to change inaccurate personal data.” In both instances, the privacy policy states that the user is entitled to amend inaccurate personal data. However, the privacy policy does not have to explicitly state that it is the right of the user to amend inaccurate personal data to be coded as a yes for this variable. Statements such as “you can amend your personal data” that appear under a “your rights” heading should be coded as a yes for this variable.</td></tr>
<tr><td colspan="4">Examples:

<u>Yes</u>
1. You have the right to see what is held about you and correct any inaccuracies.

2. Your rights include the following:

• the right to ask us to update and correct any out-of-date or incorrect personal information that we hold about you free of charge;</td></tr>
</table>

<table>
<tr><td rowspan="3">5.5</td><td colspan="3">Does the privacy policy mention that it is the right of the user to remove inaccurate personal data being processed?</td></tr>
<tr><td>No</td><td>0</td><td>The privacy policy does not mention that it is the right of the user to delete inaccurate personal data.</td></tr>
<tr><td>Yes</td><td>1</td><td>The privacy policy does mention that it is the right of the user to delete inaccurate personal data.</td></tr>
<tr><td colspan="4">Operationalisation:

<u>No</u>
A privacy policy might state: “You can delete your personal information if you contact us.” In this instance, the privacy policy has not mentioned that it is the right of the user to delete inaccurate personal data.

<u>Yes</u>
A privacy policy might state: “you have to right to remove inaccurate personal data” or “you are entitled to delete inaccurate personal data”. In both instances, the privacy policy mentions that the user is entitled to delete inaccurate personal data. However, the privacy policy does not have to explicitly mention that it is the right of the user to delete inaccurate personal data to be coded as a yes for this variable. Statements such as “you can delete inaccurate personal data” that appear under a “your rights” headings should be coded as a yes.</td></tr>
<tr><td colspan="4">Examples:</td></tr>
</table>

Yes
1. Your Rights: You have the right to access and review your Personal Data and to request that your Personal Data be corrected, amended, deleted, or blocked.

Section 6: Direct Marketing Preferences

<table>
<tr><td rowspan="3">6.1</td><td colspan="3">Does the privacy policy mention that it is possible to prevent personal data being used for direct marketing?</td></tr>
<tr><td>No</td><td>0</td><td>The privacy policy does not mention that it is possible to prevent personal data being used for direct marketing.</td></tr>
<tr><td>Yes</td><td>1</td><td>The privacy policy does mention that it is possible to prevent personal data being used for direct marketing.</td></tr>
<tr><td colspan="4">Operationalisation:

Yes
A privacy policy might state: “you can amend your direct marketing preferences by contacting us” or “to stop receiving emails from us you can unsubscribe at any time”. In both instances, the privacy policy mentions that it is possible to prevent personal data being used for direct marketing. However, the privacy policy does not have to mention how to prevent personal data being used for direct marketing although it must mention that it is possible to do so. Recording whether or not the privacy policy mentions how to prevent personal data being used for direct marketing is considered in variable 6.2.</td></tr>
<tr><td colspan="4">Examples:

Yes
1. Email: We may from time to time send you e-mail or other communications regarding current promotions, specials and new additions to the CompanyK.com site. You may "opt-out," or unsubscribe from our newsletters by following the unsubscribe instructions in any e-mail you receive from us, or by sending an e-mail to no_news@companyK.com. After doing so, CompanyK.com users will not receive future promotional emails unless they open a new account, enter a contest, or sign up to receive newsletters or emails.

2. We will give you the chance to refuse any marketing email from us or from another trader in the future.</td></tr>
</table>

<table>
<tr><td rowspan="3">6.2</td><td colspan="3">Does the privacy policy mention how to prevent personal data being used for direct marketing purposes?</td></tr>
<tr><td>No</td><td>0</td><td>The privacy policy does not mention how to prevent personal data being used for direct marketing.</td></tr>
<tr><td>Yes</td><td>1</td><td>The privacy policy does mention how to prevent personal data being used for direct marketing.</td></tr>
<tr><td colspan="4">Operationalisation:

Yes
A privacy policy might state: “to unsubscribe from our promotional emails click the unsubscribe link at the bottom of each email” or “log into your account to change your email preferences.” In both instances, the privacy policy has mentioned how to prevent personal data being used for direct marketing purposes.</td></tr>
<tr><td colspan="4">Examples:

Yes
1. If you receive emails from us, simply click the ‘unsubscribe' link at the end of any email you receive from us. If you receive postal mailings simply email your name, address and postcode to contactus@companyR.co.uk and we will remove you from our mailing list.</td></tr>
</table>

2. If you would prefer not to receive any marketing information, please send an e-mail to customerservices@companyW.co.uk.

6.3	Does the privacy policy mention that it is the right of the user to prevent personal data being processed for direct marketing purposes?		
	No	0	The privacy policy does not mention that it is the right of the user prevent personal data being used for direct marketing purposes.
	Yes	1	The privacy policy does mention that it is the right of the user prevent personal data being used for direct marketing purposes.

Operationalisation:

Yes
A privacy policy might state: “you are entitled to prevent your personal data from being used for direct marketing” and “you have to right to ask us to stop using your personal data for direct marketing.” In both instances, the privacy policy mentions that the user is entitled to prevent the organisation using their personal data for direct marketing. However, the privacy policy does not have to explicitly mention that it is the right of the user to prevent personal data from being used for direct marketing. Statements such as “you can ask us to not use your personal data for direct marketing” that appear under a “your rights” heading should be coded as a yes for this variable.

Examples:

Yes
1. At any stage you also have the right to ask us to stop using your personal data for direct marketing purposes. You can opt-out any time by emailing our customer service team at customerservices@companyF.co.uk; or by following the instructions at www.companyF.co.uk/page/newsletterunsubscribe.

2. Your rights include the following:

• the right to ask us to update and correct any out-of-date or incorrect personal information that we hold about you free of charge; and

• the right to opt out of any marketing communications that we may send you.

Section 7: Accountability

7.1	Does the privacy policy mention that the user has the option to contact the Information Commissioner’s Office should a dispute arise?		
	No	0	The privacy policy does not mention that the user has the option to contact the Information Commissioner’s Office should a dispute arise.
	Yes	1	The privacy policy does mention that the user has the option to contact the Information Commissioner’s Office should a dispute arise.

Operationalisation:

Yes
A privacy policy might state: “you can contact the Information Commissioner’s Office should you wish to discuss a problem concerning your personal data.” In this instance, the privacy policy has provided the user with the option to contact the Information Commissioner should they require it.

Examples:

Yes
1. We aim to ensure that we have resolved any matters satisfactorily, however if you are not satisfied with our response you may contact:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

7.2	Does the privacy policy mention any contact details for the organisation?		
	No	0	The privacy policy does not provide any contact details for the organisation that operates the website.
	Yes	1	The privacy policy does provide contact details for the organisation that operates the website.
Operationalisation: Yes Privacy policies that provide a link to a contact us page should also be coded as a yes for this variable.			
Examples: Yes 1. For further information from us on data protection and privacy or any requests concerning your personal information please write to This Company Limited, 24 Britton Street, London, EC1M 111 or email us at customerservice@thiscompany.com. 2. If you have any questions, comments or requests regarding this policy please contact the Customer Service Department at: customerservice@newcompany.co.uk. You can also write to us at: New Company Customer Service Department, The New Group Limited 440-450 Drive Drive Valley Swansea NN4 234			

Section 8: Retention

8.1	Does the privacy policy mention a specific length of time personal data will be retained for?		
	No	0	The privacy policy does not provide a specific length of time personal data will be retained for.
	Yes	1	The privacy policy does provide a specific length of time personal data will be retained for.
Operationalisation: No A privacy policy might state: “we hold your personal data for as long as necessary.” In this instance, the privacy policy has not mentioned a specific length of time they retain personal data for. Yes A privacy policy might state: “we retain your personal information for 1 year after your last purchase.” In this instance, the privacy policy has provided a specific length of time personal data is retained for.			
Examples: Yes			

1. We store the encrypted version on our servers, to save you having to re-enter it when you buy from us again, after when it is automatically deleted. The encrypted information is retained for a period of 12 months, when it is automatically deleted.

Section 9: Security

9.1	Does the privacy policy mention anything about the technology or technologies used to keep personal data secure?		
	No	0	The privacy policy does not mention anything about the technology used to keep personal data secure.
	Yes	1	The privacy policy does mention something about the technology used to keep personal data secure.
Operationalisation: Yes A privacy policy might state: "we use secure socket layers (SSL) to ensure your information is kept secure" or "your personal information is stored in encrypted format". In both instances, the technical measures used to keep personal data secure have been mentioned within the privacy policy.			
Examples: No 1. We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online. 2. We take appropriate security measures in relation to the information which you provide to us. For more information on the Data Protection Act, please visit the website maintained by the Office of the Information Commissioner. Yes 1. When you shop at our Website we use a 128-bit SSL encrypted secure internet connection to protect your payment details. Your computer should automatically allow the opening of the secure connection when you place your order. This means that all the details you supply and any responses are encrypted before they are sent over the internet. 2. We take the security of your transaction very, very seriously. All online purchases take place in a safe environment using the latest security technology to protect all of our customers. We encrypt your credit card information to ensure your transactions with us are private and protected whilst online. We accept orders only from Web browsers that permit communication through Secure Socket Layer (SSL) technology - this means you cannot inadvertently place an order through an unsecured connection.			

9.2	Does the website publish information on the security of personal data separately to the privacy policy?		
	No	0	The website does not publish information on the security of personal data separately to the privacy policy.
	Yes	1	The website does publish information on the security of personal data separately to the privacy policy.
Operationalisation: This study defines separately as another webpage or a page that is different to the privacy policy where the website has used a web technology (such as CSS or JavaScript) meaning that a request for a new webpage is not required. A common example of the latter display is the use of tabs where a new webpage is not requested when the user clicks on another tab.			
Examples:			

No Screenshot 4 provides more detail. Yes Screenshot 5 provides more detail.

9.3	If yes to 9.2, does the separate security information mention anything about the technology or technologies used to keep personal data secure?		
	No	0	The security policy does not mention anything about the technology used to keep personal data secure.
	Yes	1	The security policy does mention something about the technology used to keep personal data secure.
Operationalisation: See 9.1			
Examples: See 9.1			

Section 10: Cookies

10.1	Does the website publish a cookie policy?		
	No	0	The website does not publish a cookie policy.
	Yes	1	The website does publish a cookie policy.
Operationalisation: This study defines a cookie policy as any information about cookies.			

10.2	If yes to 10.1, does the website publish a cookie policy separately to the privacy policy?		
	No	0	The website does not publish a cookie policy separately to the privacy policy.
	Yes	1	The website does publish a cookie policy separately to the privacy policy.
Operationalisation: This study defines separately as another webpage or a page that is different to the privacy policy where the website has used a web technology (such as CSS or JavaScript) meaning that a request for a new webpage is not required. A common example of the latter display is the use of tabs where a new webpage is not requested when the user clicks on another tab.			
Examples: Yes Screenshot 6 provides more detail.			

10.3	If yes to 10.1, does the cookie policy describe the purpose or purposes for which cookies are used?		
	No	0	The cookie policy does not describe the purpose or purposes for which cookies are set.
	Yes	1	The cookie policy does describe the purpose or purposes for which cookies are set.
Operationalisation: Yes			

A cookie policy might state: “Company A uses cookies to personalise your experience on our website, provide a shopping cart facility and to keep track of the pages you have visited so we can understand more about your preferences.” In this instance, the information on cookies has described the purpose for which cookies are being set.

Examples:

Yes

1. When you visit our website, we will place a session cookies called 'JSESSIONID' on your computer which enables the shopping basket and other core functions of the website to function correctly. We will also place a cookie called 'ItsUserCookie' with a 1 year expiry which enables us, for example, to remember the items that you have saved in your basket and the language and currency settings for the website. If you log in to our community site we will place either a session cookie or a 14-day cookie (depending on whether you check the 'remember me' box) which will begin with 'wordpress' to enable the forum and commenting systems to work fully. We feel these cookies are strictly necessary for the website to function fully and do not directly offer a means to opt out of them as without them the website doesn't work properly.

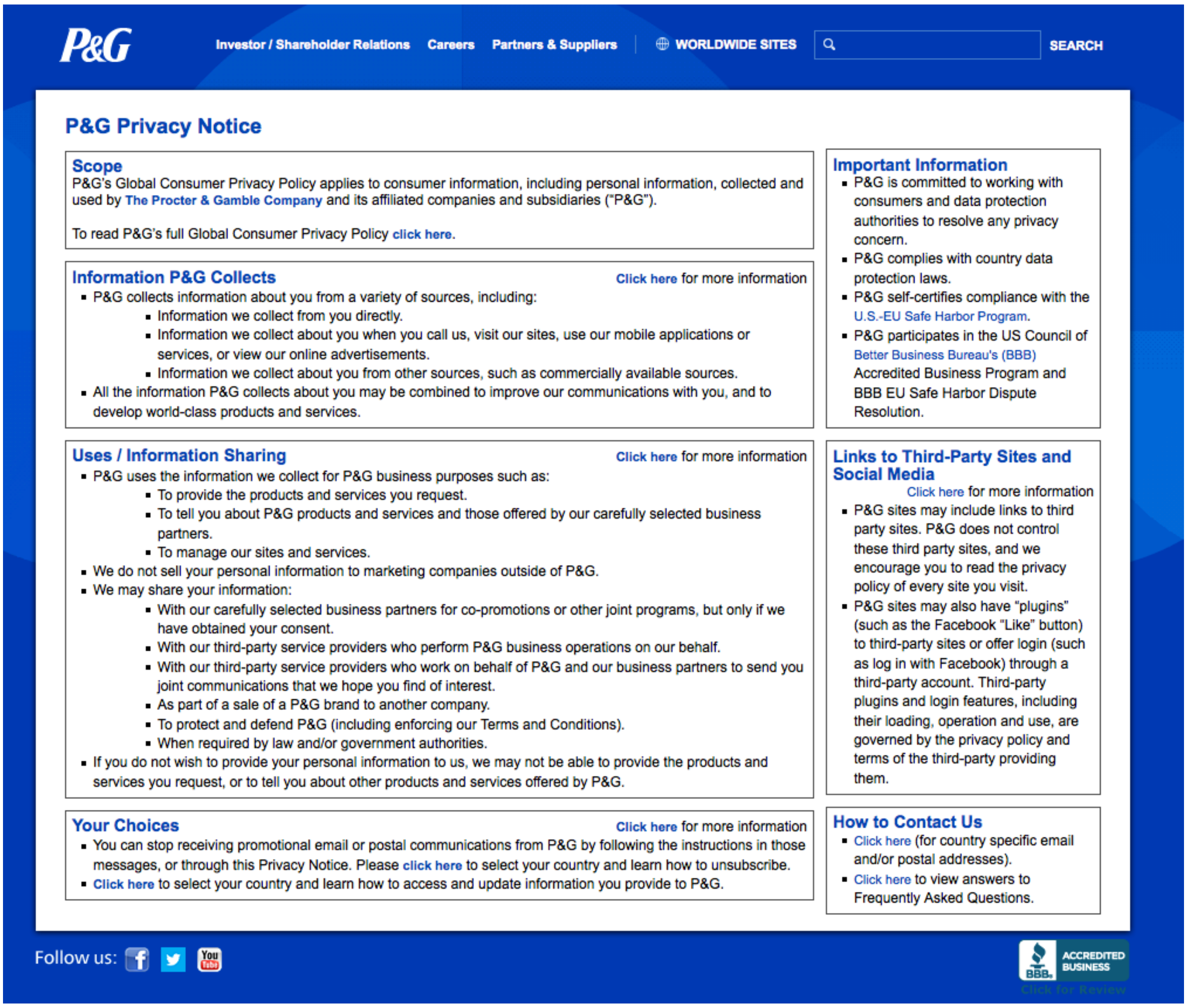
2. We use cookies for the following purposes:

- Recognise you when you return to our site
- Store information about your preferences, and so allow Us to customise Our Site and to provide you with offers that are targeted at your individual interests

Appendix E: Phase One Supporting Evidence

Screenshot 1: Variable 1.1 – Is the privacy policy presented in a layered format? Yes

The privacy policy below is presented in a layered format. The first layer shown in screenshot below provides the identity of the data controller as well as purposes for processing personal data. In this example, other information is also presented in the first layer. The first layer also contains links to the second more detailed layer shown in screenshot 2.



P&G Privacy Notice

Scope
P&G's Global Consumer Privacy Policy applies to consumer information, including personal information, collected and used by The Procter & Gamble Company and its affiliated companies and subsidiaries ("P&G").

To read P&G's full Global Consumer Privacy Policy click here.

Information P&G Collects Click here for more information

- P&G collects information about you from a variety of sources, including:
  - Information we collect from you directly.
  - Information we collect about you when you call us, visit our sites, use our mobile applications or services, or view our online advertisements.
  - Information we collect about you from other sources, such as commercially available sources.
- All the information P&G collects about you may be combined to improve our communications with you, and to develop world-class products and services.

Uses / Information Sharing Click here for more information

- P&G uses the information we collect for P&G business purposes such as:
  - To provide the products and services you request.
  - To tell you about P&G products and services and those offered by our carefully selected business partners.
  - To manage our sites and services.
- We do not sell your personal information to marketing companies outside of P&G.
- We may share your information:
  - With our carefully selected business partners for co-promotions or other joint programs, but only if we have obtained your consent.
  - With our third-party service providers who perform P&G business operations on our behalf.
  - With our third-party service providers who work on behalf of P&G and our business partners to send you joint communications that we hope you find of interest.
  - As part of a sale of a P&G brand to another company.
  - To protect and defend P&G (including enforcing our Terms and Conditions).
  - When required by law and/or government authorities.
- If you do not wish to provide your personal information to us, we may not be able to provide the products and services you request, or to tell you about other products and services offered by P&G.

Your Choices Click here for more information

- You can stop receiving promotional email or postal communications from P&G by following the instructions in those messages, or through this Privacy Notice. Please click here to select your country and learn how to unsubscribe.
- Click here to select your country and learn how to access and update information you provide to P&G.

Important Information

- P&G is committed to working with consumers and data protection authorities to resolve any privacy concern.
- P&G complies with country data protection laws.
- P&G self-certifies compliance with the U.S.-EU Safe Harbor Program.
- P&G participates in the US Council of Better Business Bureau's (BBB) Accredited Business Program and BBB EU Safe Harbor Dispute Resolution.

Links to Third-Party Sites and Social Media
Click here for more information

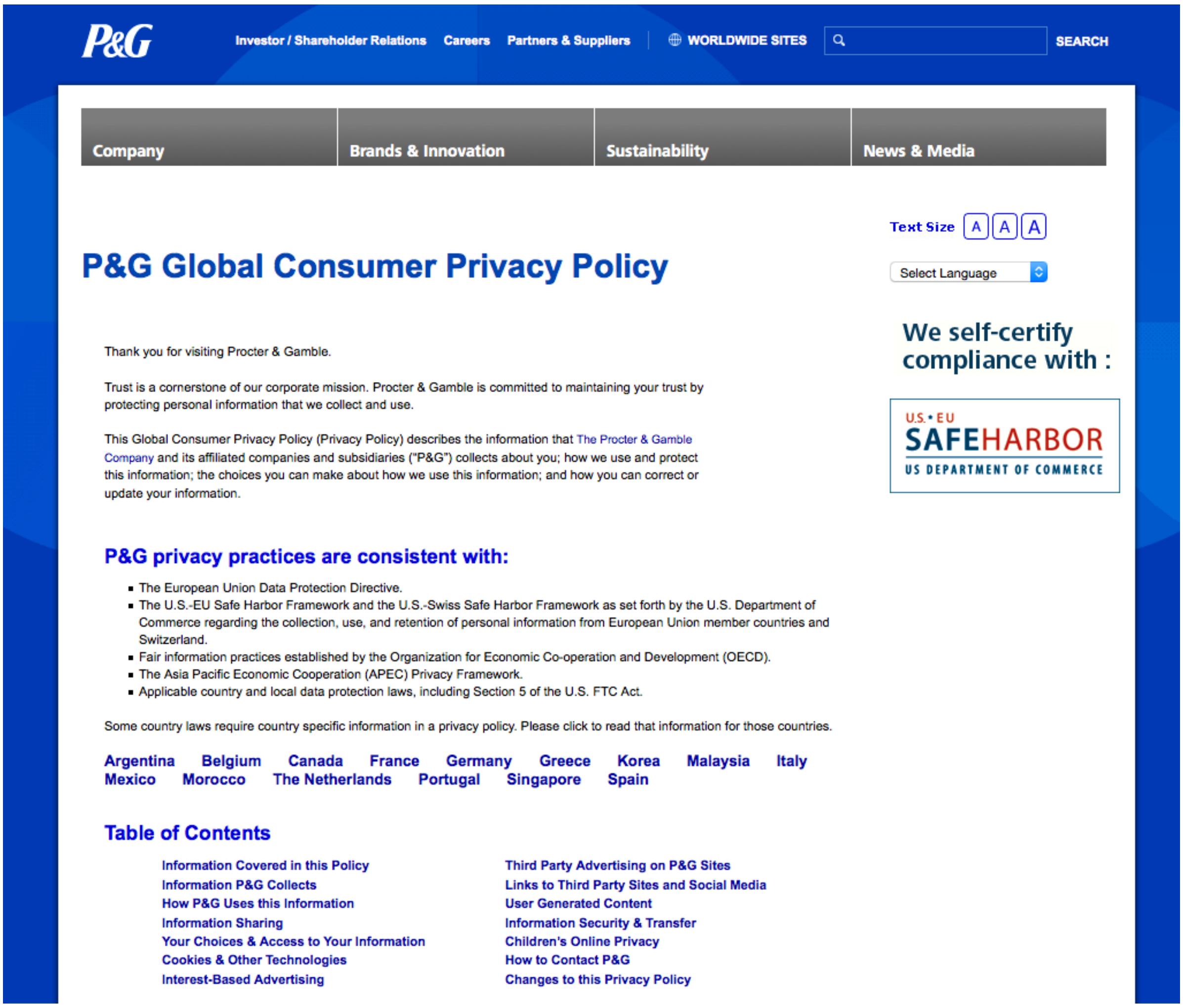
- P&G sites may include links to third party sites. P&G does not control these third party sites, and we encourage you to read the privacy policy of every site you visit.
- P&G sites may also have "plugins" (such as the Facebook "Like" button) to third-party sites or offer login (such as log in with Facebook) through a third-party account. Third-party plugins and login features, including their loading, operation and use, are governed by the privacy policy and terms of the third-party providing them.

How to Contact Us

- Click here (for country specific email and/or postal addresses).
- Click here to view answers to Frequently Asked Questions.

Screenshot 2: Variable 1.1 – Is the privacy policy presented in a layered format? Yes

The screenshot below shows the second layer of a layered privacy policy.



P&G Global Consumer Privacy Policy

Thank you for visiting Procter & Gamble.

Trust is a cornerstone of our corporate mission. Procter & Gamble is committed to maintaining your trust by protecting personal information that we collect and use.

This Global Consumer Privacy Policy (Privacy Policy) describes the information that The Procter & Gamble Company and its affiliated companies and subsidiaries ("P&G") collects about you; how we use and protect this information; the choices you can make about how we use this information; and how you can correct or update your information.

P&G privacy practices are consistent with:

- The European Union Data Protection Directive.
- The U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland.
- Fair information practices established by the Organization for Economic Co-operation and Development (OECD).
- The Asia Pacific Economic Cooperation (APEC) Privacy Framework.
- Applicable country and local data protection laws, including Section 5 of the U.S. FTC Act.

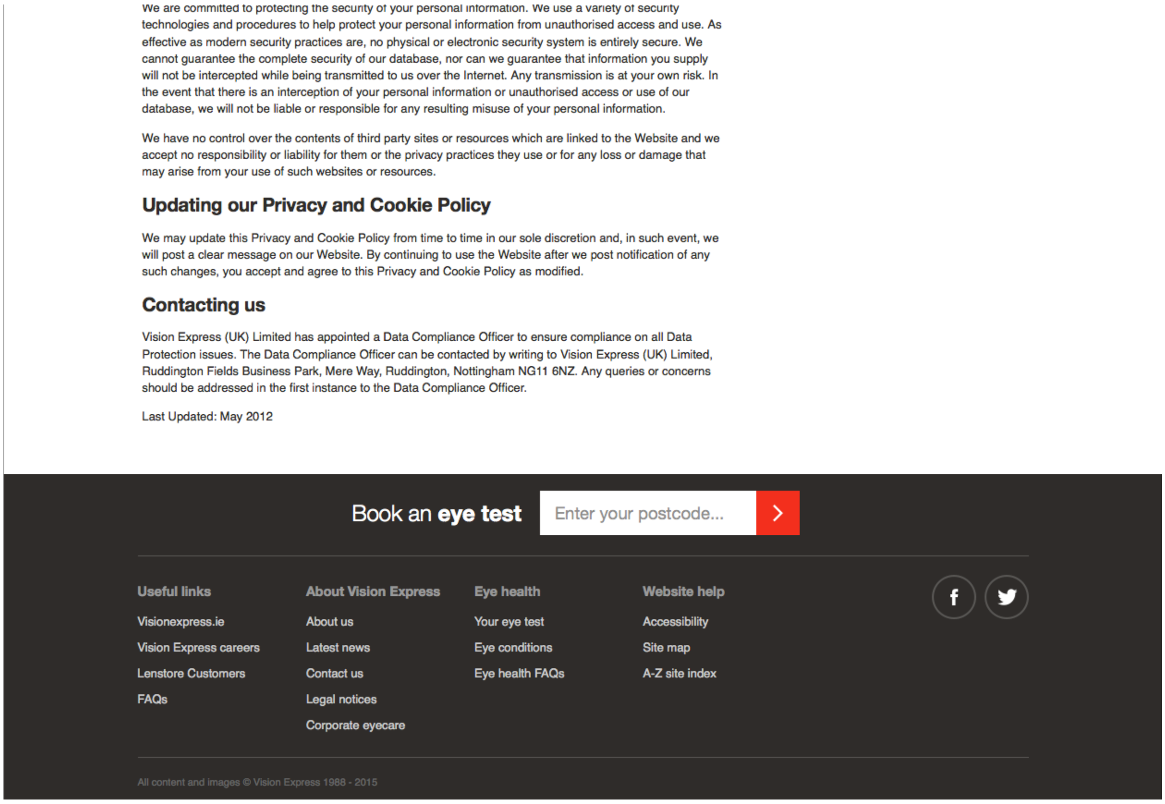
Some country laws require country specific information in a privacy policy. Please click to read that information for those countries.

Argentina Belgium Canada France Germany Greece Korea Malaysia Italy
Mexico Morocco The Netherlands Portugal Singapore Spain

Table of Contents

Screenshot 3: Variable 2.1 - Does the privacy policy mention when the policy was last updated? Yes

The screenshot below shows an example of a privacy policy that does mention when the policy was last updated.



We are committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorised access and use. As effective as modern security practices are, no physical or electronic security system is entirely secure. We cannot guarantee the complete security of our database, nor can we guarantee that information you supply will not be intercepted while being transmitted to us over the Internet. Any transmission is at your own risk. In the event that there is an interception of your personal information or unauthorised access or use of our database, we will not be liable or responsible for any resulting misuse of your personal information.

We have no control over the contents of third party sites or resources which are linked to the Website and we accept no responsibility or liability for them or the privacy practices they use or for any loss or damage that may arise from your use of such websites or resources.

Updating our Privacy and Cookie Policy

We may update this Privacy and Cookie Policy from time to time in our sole discretion and, in such event, we will post a clear message on our Website. By continuing to use the Website after we post notification of any such changes, you accept and agree to this Privacy and Cookie Policy as modified.

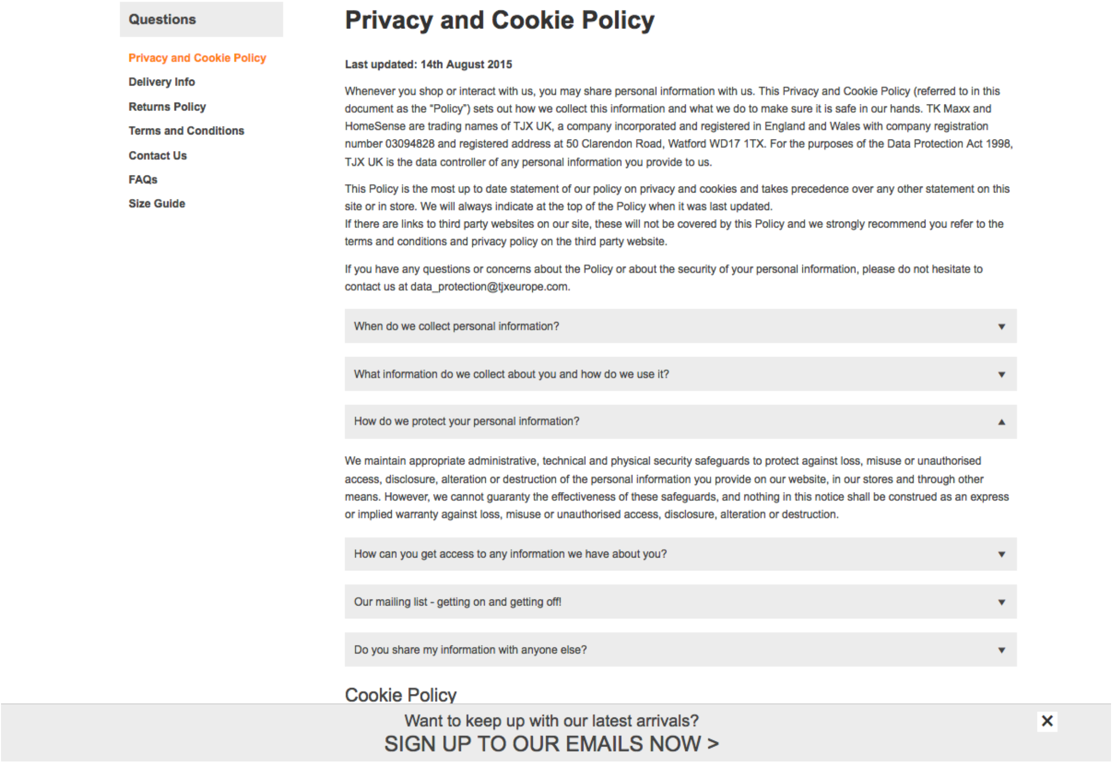
Contacting us

Vision Express (UK) Limited has appointed a Data Compliance Officer to ensure compliance on all Data Protection issues. The Data Compliance Officer can be contacted by writing to Vision Express (UK) Limited, Ruddington Fields Business Park, Mere Way, Ruddington, Nottingham NG11 6NZ. Any queries or concerns should be addressed in the first instance to the Data Compliance Officer.

Last Updated: May 2012

Screenshot 4: Variable 9.2 **-** Does the website publish information on the security of personal data separately to the privacy policy? No

The screenshot below shows an example where security information is presented on the same page as the privacy policy.


Questions
Privacy and Cookie Policy
Delivery Info
Returns Policy
Terms and Conditions
Contact Us
FAQs
Size Guide
Want to keep up with our latest arrivals?
SIGN UP TO OUR EMAILS NOW >
✕

Privacy and Cookie Policy

Last updated: 14th August 2015

Whenever you shop or interact with us, you may share personal information with us. This Privacy and Cookie Policy (referred to in this document as the "Policy") sets out how we collect this information and what we do to make sure it is safe in our hands. TK Maxx and HomeSense are trading names of TJX UK, a company incorporated and registered in England and Wales with company registration number 03094828 and registered address at 50 Clarendon Road, Watford WD17 1TX. For the purposes of the Data Protection Act 1998, TJX UK is the data controller of any personal information you provide to us.

This Policy is the most up to date statement of our policy on privacy and cookies and takes precedence over any other statement on this site or in store. We will always indicate at the top of the Policy when it was last updated.
If there are links to third party websites on our site, these will not be covered by this Policy and we strongly recommend you refer to the terms and conditions and privacy policy on the third party website.

If you have any questions or concerns about the Policy or about the security of your personal information, please do not hesitate to contact us at data_protection@tjxeurope.com.

When do we collect personal information? ▼

What information do we collect about you and how do we use it? ▼

How do we protect your personal information? ▲

We maintain appropriate administrative, technical and physical security safeguards to protect against loss, misuse or unauthorised access, disclosure, alteration or destruction of the personal information you provide on our website, in our stores and through other means. However, we cannot guaranty the effectiveness of these safeguards, and nothing in this notice shall be construed as an express or implied warranty against loss, misuse or unauthorised access, disclosure, alteration or destruction.

How can you get access to any information we have about you? ▼

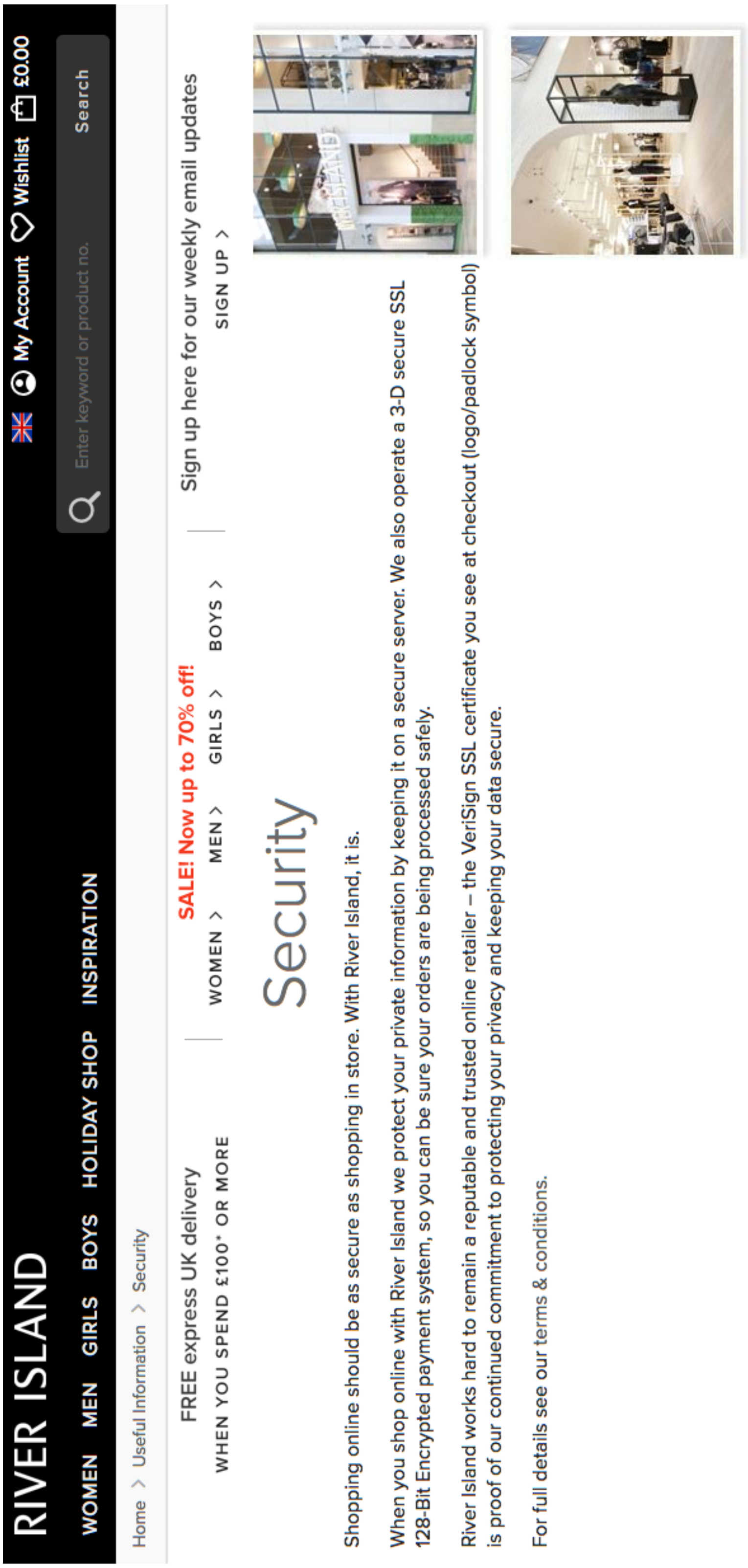
Our mailing list - getting on and getting off! ▼

Do you share my information with anyone else? ▼

Cookie Policy

Screenshot 5: Variable 9.2 **-** Does the website publish information on the security of personal data separately to the privacy policy? Yes

The screenshot below shows an example where a security policy is published on a separate page to the privacy policy.


RIVER ISLAND
WOMEN MEN GIRLS BOYS HOLIDAY SHOP INSPIRATION
My Account
Wishlist
£0.00
Enter keyword or product no.
Search
Home > Useful Information > Security
FREE express UK delivery
WHEN YOU SPEND £100* OR MORE
SALE! Now up to 70% off!
WOMEN > MEN > GIRLS > BOYS >
Sign up here for our weekly email updates
SIGN UP >

Security

Shopping online should be as secure as shopping in store. With River Island, it is.

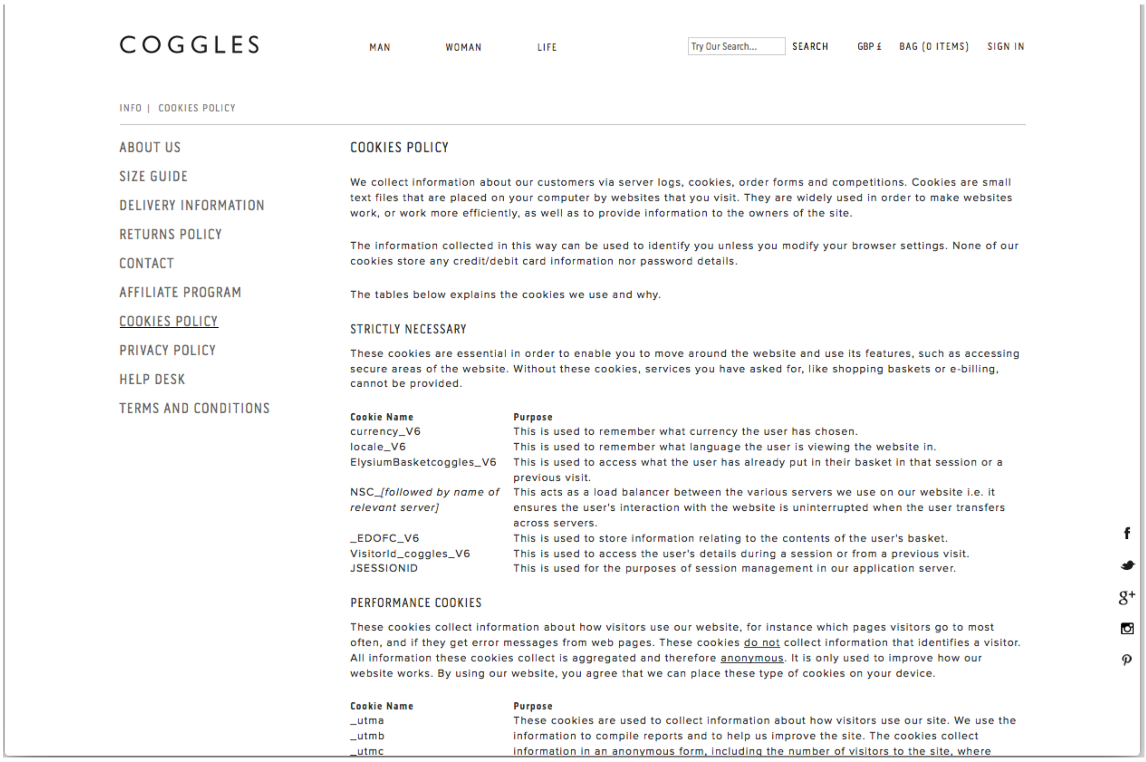
When you shop online with River Island we protect your private information by keeping it on a secure server. We also operate a 3-D secure SSL 128-Bit Encrypted payment system, so you can be sure your orders are being processed safely.

River Island works hard to remain a reputable and trusted online retailer – the VeriSign SSL certificate you see at checkout (logo/padlock symbol) is proof of our continued commitment to protecting your privacy and keeping your data secure.

For full details see our terms & conditions.

Screenshot 6: Variable 10.2 **-** If yes to 10.1, does the website publish a cookie policy separately to the privacy policy? **-** Yes

The screenshot below shows an example of a cookie policy the is published separately to the privacy policy.



COOKIES POLICY

We collect information about our customers via server logs, cookies, order forms and competitions. Cookies are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site.

The information collected in this way can be used to identify you unless you modify your browser settings. None of our cookies store any credit/debit card information nor password details.

The tables below explains the cookies we use and why.

STRICTLY NECESSARY

These cookies are essential in order to enable you to move around the website and use its features, such as accessing secure areas of the website. Without these cookies, services you have asked for, like shopping baskets or e-billing, cannot be provided.

Cookie Name	**Purpose**
currency_V6	This is used to remember what currency the user has chosen.
locale_V6	This is used to remember what language the user is viewing the website in.
ElysiumBasketcoggles_V6	This is used to access what the user has already put in their basket in that session or a previous visit.
NSC_*[followed by name of relevant server]*	This acts as a load balancer between the various servers we use on our website i.e. it ensures the user's interaction with the website is uninterrupted when the user transfers across servers.
_EDOFC_V6	This is used to store information relating to the contents of the user's basket.
VisitorId_coggles_V6	This is used to access the user's details during a session or from a previous visit.
JSESSIONID	This is used for the purposes of session management in our application server.

PERFORMANCE COOKIES

These cookies collect information about how visitors use our website, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies do not collect information that identifies a visitor. All information these cookies collect is aggregated and therefore anonymous. It is only used to improve how our website works. By using our website, you agree that we can place these type of cookies on your device.

Cookie Name	**Purpose**
_utma	These cookies are used to collect information about how visitors use our site. We use the information to compile reports and to help us improve the site. The cookies collect information in an anonymous form, including the number of visitors to the site, where
_utmb	
_utmc	

Appendix F: Phase Two Privacy Policies A, B and C

Privacy Policy A – www.trendyclothes4u.co.uk

We are committed to protecting and respecting your privacy.

This policy (together with our Terms of Use and any other documents referred to on it) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

For the purpose of the Data Protection Act 1998 (the Act), the data controller is Trendy Stuff Limited T/A Trendy Clothes 4 U of The Old School, Stone Road, Blackbrook, Newcastle-under-Lyme, Staffordshire, ST5 5EG.

Our nominated representative for the purpose of the Act is Jonathan Capener.

INFORMATION WE MAY COLLECT FROM YOU

You do not have to register to view most of our website. However, some personal information is required if you choose to place an order, contact us via email or request a catalogue.

We may collect and process the following data about you:

- If you contact us, we may keep a record of that correspondence.
- We may also ask you to complete surveys that we use for research purposes, although you do not have to respond to them.
- Details of transactions you carry out through our site and of the fulfilment of your orders.
- Details of your visits to our site including, but not limited to, traffic data, location data, weblogs and other communication data, whether this is required for our own billing purposes or otherwise and the resources that you access.
- Information that you provide by filling in forms on our site www.trendyclothes4u.co.uk (our site). This includes information provided at the time of registering to use our site, subscribing to our service, posting material or requesting further services. We may also ask you for information when you enter a competition or promotion sponsored by Trendy Stuff Ltd T/A Trendy Clothes 4 U, and when you report a problem with our site.

IP ADDRESSES AND COOKIES

We may collect information about your computer, including where available your IP address, operating system and browser type, for system administration and to report aggregate information to our advertisers. This is statistical data about our users' browsing actions and patterns, and does not identify any individual.

For the same reason, we may obtain information about your general internet usage by using a cookie file which is stored on the hard drive of your computer. Cookies contain information that is transferred to your computer's hard drive. They help us to improve our site and to deliver a better and more personalised service. They enable us:

- To estimate our audience size and usage pattern.
- To store information about your preferences, and so allow us to customise our site according to your individual interests.
- To speed up your searches.
- To recognise you when you return to our site.

You may refuse to accept cookies by activating the setting on your browser which allows you to refuse the setting of cookies. However, if you select this setting you may be unable to access certain parts of our site. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies when you log on to our site.

Please note that our advertisers and tracking software may also use cookies (third-party), over which we have no control.

WHERE WE STORE YOUR PERSONAL DATA

The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff maybe engaged in, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. By submitting your personal data, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy.

All information you provide to us is stored on secure servers. Any payment transactions will be encrypted (using SSL technology). Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Athough we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

USES MADE OF THE INFORMATION

We use information held about you in the following ways:

- To ensure that content from our site is presented in the most effective manner for you and for your computer.
- To provide you with information, products or services that you request from us or which we feel may interest you, where you have consented to be contacted for such purposes.
- To carry out our obligations arising from any contracts entered into between you and us.
- To allow you to participate in interactive features of our service, when you choose to do so.
- To notify you about changes to our service.

If you are an existing customer, we will only contact you by electronic means (e-mail or SMS) with information about goods and services similar to those which were the subject of a previous sale to you.

If you are a new customer, and where we permit selected third parties to use your data, we (or they) will contact you by electronic means only if you have consented to this. If you do not want us to use your data in this way, or to pass your details on to third parties for marketing

purposes, please tick the relevant box situated on the form on which we collect your data (the order form).

DISCLOSURE OF INFORMATION

We do not pass on your details to any third party unless you give us permission to do so notwithstanding the following exceptions:

We may disclose your personal information to any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 736 of the UK Companies Act 1985.

We may disclose your personal information to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets.
- If Trendy Stuff Ltd Limited or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets.
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our Terms of Use or Terms and Conditions of Supply and other agreements; or to protect the rights, property, or safety of Trendy Stuff Ltd T/A Trendy Clothes 4 U, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

YOUR RIGHTS

You have the right to ask us not to process your personal data for marketing purposes. We will usually inform you (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we use to collect your data. You can also exercise the right at any time by contacting us at The Old School, Stone Road, Blackbrook, Newcastle-under-Lyme, Staffordshire, ST5 5EG or enquiries@trendyclothes4u.co.uk

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

ACCESS TO INFORMATION

The Act gives you the right to access information held about you. Your right of access can be exercised in accordance with the Act. We will provide you with a readable copy of the personal data that we keep about you within 15 working days. There is no charge for this, but evidence of proof of your identity will be required.

It is in our interest and yours to hold accurate date. If the data we hold on you is inaccurate in any way where appropriate you may have the data: erased; rectified or amended; completed.

CHANGES TO OUR PRIVACY POLICY

Any changes we may make to our privacy policy in the future will be posted on this page and, where appropriate, notified to you by e-mail.

DISPUTE

We aim to ensure that we have resolved any matters satisfactorily, however if you are not satisfied with our response you may contact:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 01625 545 700
Fax: 01625 524 510
DX: 20819 Wilmslow
Email: mail@dataprotection.gov.uk
Website: http://www.dataprotection.gov.uk

CONTACT

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to our Customer Service team at enquiries@trendyclothes4u.co.uk or:

Trendy Clothes 4 U
The Old School
Stone Road
Blackbrook
Newcastle-under-Lyme
Staffordshire
ST5 5EG

Or telephone: 09887 765487

Privacy Policy B – www.stylishclothes4u.co.uk

(i) When you order we will ask for your name, e-mail address and delivery address. These details will enable us to process your order and contact you in the event of any queries. We will also ask for your telephone number, so that we can contact you urgently if necessary in the event of any problem with your order. We will communicate with you by e-mail, telephone or letter.

(ii) We may also use the information we hold to notify you occasionally about important changes to the web site, new Clothing Gifts Limited services and special offers. We may invite you to take part in market research. If you would rather not receive these notifications or invitations, please contact us or send an e-mail to contact@stylishclothes4u.co.uk.

(iii) When you enter a competition or prize draw, we will ask for your name, address and e-mail address so that we can administer the competition and notify the winners. We may also ask for further information for marketing purposes. You do not have to provide this information in order to enter the competition or prize draw.

(iv) Other carefully selected companies may also make further offers to you. If you do not wish to receive these offers, please contact us.

(v) You have the right to ask for a copy of the information we hold on you and to have any inaccuracies corrected.

(vi) We reserve the right to store shopping pattern data in order to provide a better service for our customers. We may occasionally use some of the information we hold for the purposes of testing our internal systems. Such testing is only carried out where necessary, and your information will be treated with the utmost care and respect.

(vii) By using our site you consent to the collection, retention and use of this information by Clothing Gifts Limited. Any changes to our privacy policy will be notified on this page.

(viii) We work with third-party data analytics and advertising companies. Some of these companies may use anonymous information (but they do not collect or use any personally identifiable information) about your visits to this and other websites in order to provide advertisements or provide data based on which we may provide advertisements about goods and services of interest to you. Learn more about this practice or about your choice to opt-out of this practice: Struq privacy policy & opt-out [new window], Criteo privacy policy & opt-out [new window], Google privacy policy & opt-out [new window], Coremetrics privacy policy & opt-out [new window].

For more information about cookies and how to control which cookies you allow, visit www.allaboutcookies.org/ new window.
For more information about behavioural advertising, visit www.youronlinechoices.com/uk/ new window.

Stylish Clothes 4 U is a trading style of Clothing Gifts Ltd.
Registered Office: 2 Gregory Street, Hyde, Cheshire SK14 4TH
Registered Number 718151
VAT No. : 125688644
Clothing Gifts is authorised and regulated by the Financial Services Authority.
Our customer service number is 0871 200 0378.
Please use the contact us link to contact us securely or send an e-mail to contact@stylishclothes4u.co.uk.

Privacy Policy C – www.koolerclothes4u.co.uk

Privacy Policy for www.koolerclothes4u.co.uk

We take your privacy seriously and we are committed to protecting your privacy. We follow the procedures set out in this policy when using your information.

By using this Website to give us your information you accept the terms of and consent to us using your information in accordance with this policy.

Information Collected

For the purpose of the Data Protection Act 1998 the data controller is Kooler Clothes 4 U Limited, whose contact details are set out at the end of this document. We will use the information we collect about you lawfully and to process your order and to provide you with the best possible service.

If you use the Services or if you contact us with an enquiry we will collect personal information such as your name, contact details, phone number, e-mail address, address credit/debit card details and age and use them to respond to your enquiry.

We will never collect sensitive information about you without your consent. We may contact you by telephone, post or email.

Use of Information

The information you provide will be held on a database in the UK and may be accessed by our staff and by those who provide support services to us. We may also share it with third parties such as banking / merchant services and third party suppliers where necessary to provide services to you. We use third party suppliers to provide some of our products and your order contact details (but not your credit / debit card or financial details) shall be passed to those relevant third party suppliers for the purpose of delivery of your order.

Where you permit it we may also use your personal information and may allow selected third parties to provide you with information about goods and services which may be of interest to you. Where you have agreed that we may pass your information on to third parties by clicking on the option boxes when ordering your products through the website, we or they may contact you about these by e-mail, mail, telephone or other means. We will not share your information with any third party for marketing purposes without your consent.

We may pass aggregate information on the usage of our Website to third parties but this will not include information that can be used to identify you.

We will not e-mail you or contact you by SMS or MMS in the future unless you have given us your consent other than to confirm orders or discussions related to products that you have previously ordered.

Once you have consented to the transfer of your personal information to a third party such as a marketing company, you must follow the opt-out procedures provided for by such third party, to opt out or modify your personal information contained in such third party's database.

You will have the opportunity to opt out of receiving any marketing e-mail from us or from other third parties in the future by emailing customer.service@koolerclothes4u.co.uk or phoning 0800 0830 930 or clicking on the 'unsubscribe' button of any email you receive.

If we intend to transfer your information outside the European Economic Area (other than to fulfil your order) we will obtain your consent prior to such transfer.

We do our best to ensure that all information held relating to you is kept up-to-date, accurate and complete. However we also rely on you to notify us if your information requires updating or deleting. We will respond to requests from you to update or delete your information in an efficient and timely manner.

Use of Cookies

Unless you have indicated your objection when disclosing your information to us, our system will issue cookies to your computer when you log on to the Website. Cookies are small amounts of information regarding your browsing habits which we store on your computer. Cookies make it easier for you to log on to and use the Website during future visits. They also allow us to monitor Website traffic and to personalise the content of the Website for you. You may have the ability to accept or decline cookies. Most web browsers automatically accept cookies, but if you prefer you may be able to modify your browser settings to decline all cookies, or to notify you each time a cookie is tendered and permit you to accept or decline cookies on an individual basis. If you choose to decline cookies, however, that may hinder the performance of the web Website. For specific details about how to configure your browser you should refer to its supplier or manufacturer.

Security

We employ security measures to protect your information from access by unauthorised persons and against unlawful processing, accidental loss, destruction and damage, however, transmission of information via the internet is not completely secure. We will use reasonable endeavours to protect your personal data but we cannot guarantee the security of it.
We will retain your information for a reasonable period or as long as the law requires. We will only disclose your personal data in the event that we sell any or all of our business or assets, if we are acquired by a third party or where we are required or permitted to by law.

You are entitled to receive a copy of your personal data and we are entitled to charge you a fee of £10 for this to cover administration costs.

We may amend this Privacy Policy at any time. If we make any substantial changes in the way we use your Personal Information we will notify you by posting them on the Website.

All comments, queries and requests relating to our use of your information are welcomed and should be addressed to Kooler Clothes 4 U Limited, Unit 35 Romsey Industrial Estate, Greatbridge Road, Romsey, Hampshire, SO51 0HR or emailed to Kooler Clothes 4 U customer.service@koolerclothes4u.co.uk.

Appendix G: Phase Four Usability Handout

Privacy Policy User Study 2016

Thank you for taking the time to participate in this study, it should take approximately 15 minutes to complete. After you have read the participant information sheet and completed the consent form please answer the questions below by **circling one response**:

Q: What is your age?

18-20	21-25	26-30	31-35	36-40	41-45	46-50	51+	Prefer not to say

Q: What is your gender?

Male	Female	Prefer not to say

Q: Are you from the U.K.?

No	Yes	Prefer not to say

Q: When did you last purchase a product or service online?

Within the last week	Within the last month	Within the last two months	Within the last six months	Longer than six months ago

Setup Instructions

Step 1

Open the Google Chrome web browser and navigate to:

https://co-project.lboro.ac.uk/lsdj3/index22.html

Step 2

Click on the policy A link.

Step 3

Open a separate tab within the web browser and navigate to the same webpage specified in step 1.

Step 4

Click on the policy B link.

You should now have policy A and policy B open in separate tabs within the browser window. Please put your hand up if you do not have policy A and policy B open in separate browser tabs.

Step 5

Turn to the next page where we will run through a practice question.

Practice question

Step 1. *Navigate to policy A. Locate and then circle the correct answer to the practice question stated below.*

Question: Based on the policies, does the website collect your date of birth when you sign up or purchase a product?

Policy A	No	Yes	Policy does not say

Step 2. *For statements 1a and 1b below please **circle one response** that characterises how you feel where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree and 5=strongly agree.*

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
I could locate the information required to answer to the practice question **with ease**:					
Policy A	1	2	3	4	5
I could locate the information required to answer to the practice question **quickly**:					
Policy A	1	2	3	4	5

Step 3. *Navigate to policy B and repeat the process by answering the same practice question and responding to the statements below.*

Policy B	No	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
I could locate the information required to answer to the practice question **with ease**:					
Policy B	1	2	3	4	5
I could locate the information required to answer to the practice question **quickly**:					
Policy B	1	2	3	4	5

You should end up with something like this (depending on your answers/feelings towards the policy – the answers below are not necessarily correct) …

Policy A

Policy A	No	[✓ Yes]	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
I could locate the information required to answer to the practice question **with ease**:					
Policy A	1	2	3	[✓ 4]	5
I could locate the information required to answer to the practice question **quickly**:					
Policy A	1	[✓ 2]	3	4	5

Policy B

Policy B	[✓ No]	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
I could locate the information required to answer to the practice question **with ease**:					
Policy B	1	2	[✓ 3]	4	5
I could locate the information required to answer to the practice question **quickly**:					
Policy B	1	[✓ 2]	3	4	5

Question 1: Based on the policies, can you prevent your personal data being used to send you information about products or services?

Policy A

Policy A		No	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1a: I could locate the information required to answer question 1 with ease.					
Policy A	1	2	3	4	5
1b: I could locate the information required to answer question 1 quickly.					
Policy A	1	2	3	4	5

Policy B

Policy B		No	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1c: I could locate the information required to answer question 1 with ease.					
Policy B	1	2	3	4	5
1d: I could locate the information required to answer question 1 quickly.					
Policy B	1	2	3	4	5

Question 2:

Do the policies provide any links to external websites about cookies?

Policy A

Policy A	No	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
2a: I could locate the information required to answer question 1 with ease.					
Policy A	1	2	3	4	5
2b: I could locate the information required to answer question 1 quickly.					
Policy A	1	2	3	4	5

Policy B

Policy B	No	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
2c: I could locate the information required to answer question 1 with ease.					
Policy B	1	2	3	4	5
2d: I could locate the information required to answer question 1 quickly.					
Policy B	1	2	3	4	5

Question 3:

Based on the policies, might your personal data be shared with another organisation that may use it to send you information about products or services?

Policy A

Policy A	No	Yes	Yes with consent	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
3a: I could locate the information required to answer question 1 with ease.					
Policy A	1	2	3	4	5
3b: I could locate the information required to answer question 1 quickly.					
Policy A	1	2	3	4	5

Policy B

Policy B	No	Yes	Yes with consent	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
3c: I could locate the information required to answer question 1 with ease.					
Policy B	1	2	3	4	5
3d: I could locate the information required to answer question 1 quickly.					
Policy B	1	2	3	4	5

Question 4:

Based on the policies, might your personal data be sent outside the European Economic Area (EEA)?

Policy A

Policy A	No	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
4a: I could locate the information required to answer question 1 with ease.					
Policy A	1	2	3	4	5
4b: I could locate the information required to answer question 1 quickly.					
Policy A	1	2	3	4	5

Policy B

Policy B	No	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
4c: I could locate the information required to answer question 1 with ease.					
Policy B	1	2	3	4	5
4d: I could locate the information required to answer question 1 quickly.					
Policy B	1	2	3	4	5

Question 5:

Based on the policies, can you contact an independent organisation and complain about the processing of your personal data?

Policy A

Policy B		No	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
5a: I could locate the information required to answer question 1 with ease.					
Policy A	1	2	3	4	5
5b: I could locate the information required to answer question 1 quickly.					
Policy A	1	2	3	4	5

Policy B

Policy B		No	Yes	Policy does not say

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
5c: I could locate the information required to answer question 1 with ease.					
Policy B	1	2	3	4	5
5d: I could locate the information required to answer question 1 quickly.					
Policy B	1	2	3	4	5

The set of statements below compares both privacy policies you have just viewed.

Instruction: *For each statement* ***please circle one response for policy A and one response for policy B*** *that characterises how you feel where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree and 5=strongly agree.*

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
6: The privacy policy was easy to use.					
Policy A	1	2	3	4	5
Policy B	1	2	3	4	5
7: The privacy policy could be used to find information quickly.					
Policy A	1	2	3	4	5
Policy B	1	2	3	4	5
8: The privacy policy layout was straightforward.					
Policy A	1	2	3	4	5
Policy B	1	2	3	4	5
9: I understood where I needed to look to find information when answering questions 1 to 5.					
Policy A	1	2	3	4	5
Policy B	1	2	3	4	5
10: The privacy policy headings were signposted clearly.					
Policy A	1	2	3	4	5
Policy B	1	2	3	4	5
11: I could use the privacy policy efficiently to answer questions 1 to 5.					
Policy A	1	2	3	4	5
Policy B	1	2	3	4	5
12: The privacy policy was simple to use.					
Policy A	1	2	3	4	5
Policy B	1	2	3	4	5

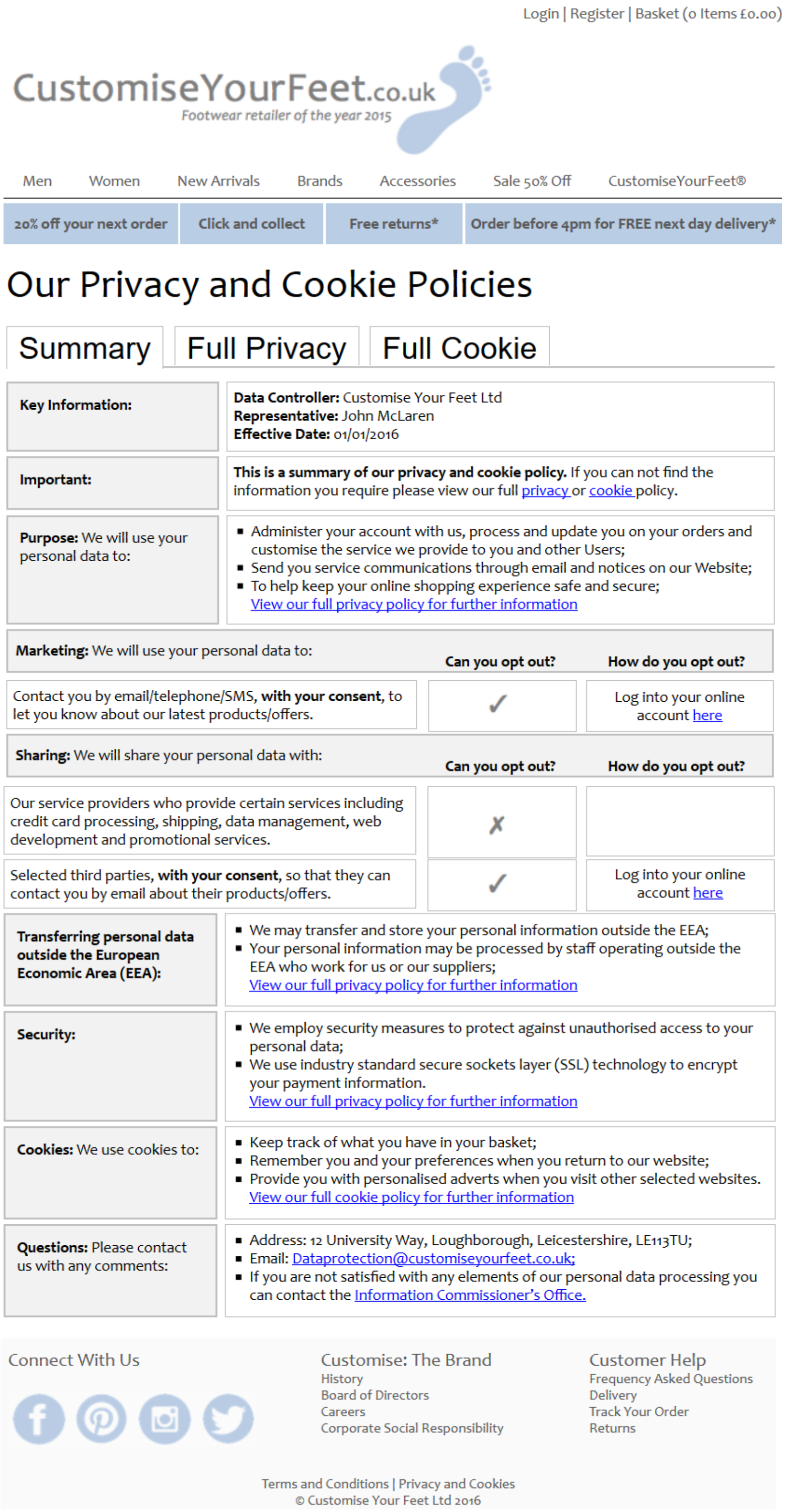
This section about privacy policies in general. It only applies to policy A.

Instruction: *For each statement please* ***circle one response*** *that characterises how you feel where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree and 5=strongly agree.*

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
13: It would be a good idea to have a summary policy page on all websites.					
Policy A	1	2	3	4	5
14: It would be a good idea to have a summary policy page that has a consistent look and feel across all websites.					
Policy A	1	2	3	4	5
15: It would be a good idea to have privacy policies that have a consistent look and feel across all websites.					
Policy A	1	2	3	4	5
16: I would like websites to offer variety in the way in which they present their privacy policies.					
Policy A	1	2	3	4	5

That’s the end of the study. Thank you for participating.

Appendix H: Phase Four Standardised Privacy Policy



Our Privacy and Cookie Policies

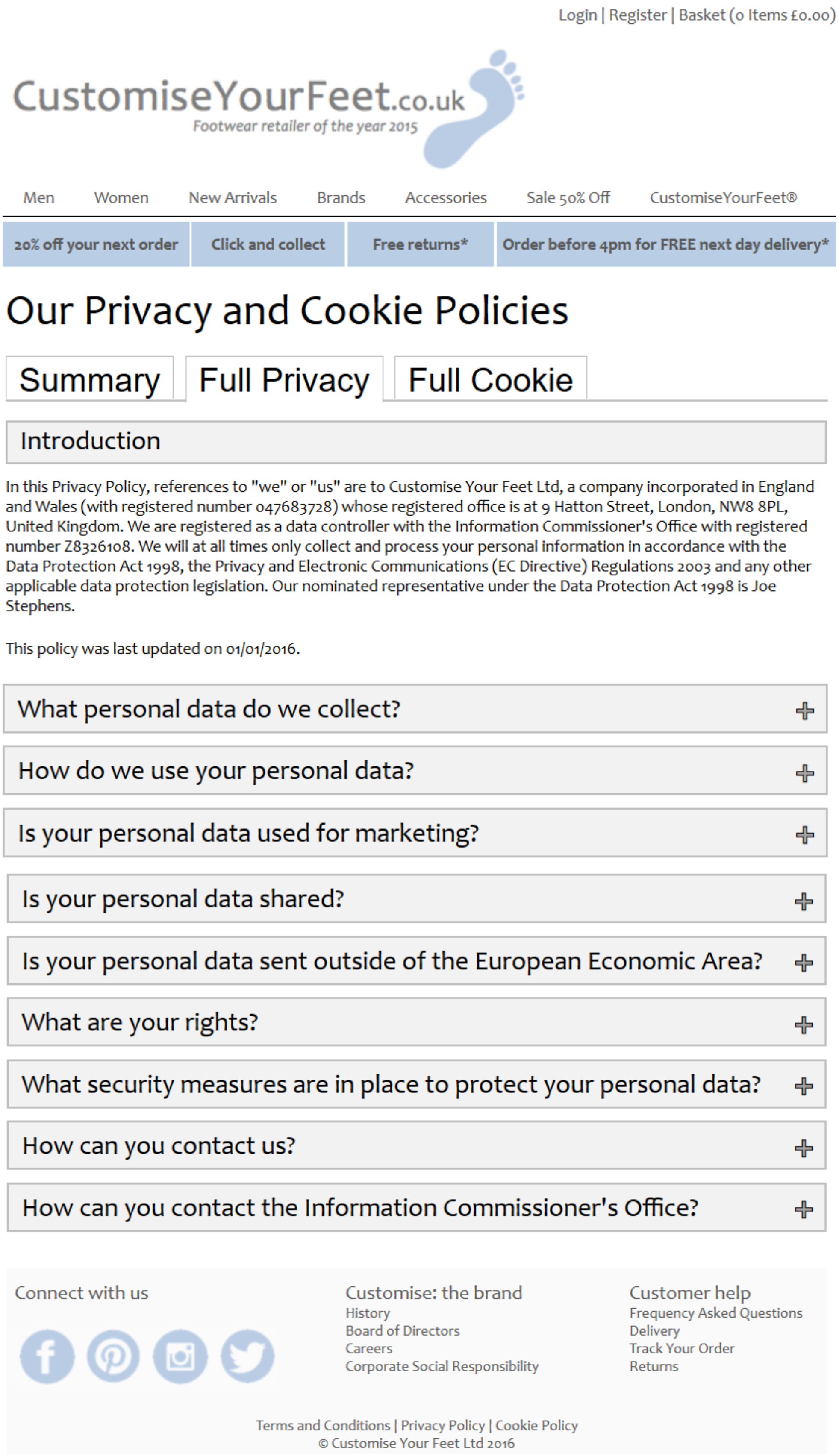
Key Information:	**Data Controller:** Customise Your Feet Ltd **Representative:** John McLaren **Effective Date:** 01/01/2016
Important:	**This is a summary of our privacy and cookie policy.** If you can not find the information you require please view our full privacy or cookie policy.
Purpose: We will use your personal data to:	▪ Administer your account with us, process and update you on your orders and customise the service we provide to you and other Users; ▪ Send you service communications through email and notices on our Website; ▪ To help keep your online shopping experience safe and secure; View our full privacy policy for further information

Marketing: We will use your personal data to:	**Can you opt out?**	**How do you opt out?**
Contact you by email/telephone/SMS, **with your consent**, to let you know about our latest products/offers.	✓	Log into your online account here

Sharing: We will share your personal data with:	**Can you opt out?**	**How do you opt out?**
Our service providers who provide certain services including credit card processing, shipping, data management, web development and promotional services.	✗	
Selected third parties, **with your consent**, so that they can contact you by email about their products/offers.	✓	Log into your online account here

Transferring personal data outside the European Economic Area (EEA):	▪ We may transfer and store your personal information outside the EEA; ▪ Your personal information may be processed by staff operating outside the EEA who work for us or our suppliers; View our full privacy policy for further information
Security:	▪ We employ security measures to protect against unauthorised access to your personal data; ▪ We use industry standard secure sockets layer (SSL) technology to encrypt your payment information. View our full privacy policy for further information
Cookies: We use cookies to:	▪ Keep track of what you have in your basket; ▪ Remember you and your preferences when you return to our website; ▪ Provide you with personalised adverts when you visit other selected websites. View our full cookie policy for further information
Questions: Please contact us with any comments:	▪ Address: 12 University Way, Loughborough, Leicestershire, LE113TU; ▪ Email: Dataprotection@customiseyourfeet.co.uk; ▪ If you are not satisfied with any elements of our personal data processing you can contact the Information Commissioner's Office.

Connect With Us
Customise: The Brand
History
Board of Directors
Careers
Corporate Social Responsibility
Customer Help
Frequency Asked Questions
Delivery
Track Your Order
Returns
Terms and Conditions | Privacy and Cookies
© Customise Your Feet Ltd 2016



Login | Register | Basket (0 Items £0.00)

CustomiseYourFeet.co.uk
Footwear retailer of the year 2015

Our Privacy and Cookie Policies

Introduction

In this Privacy Policy, references to "we" or "us" are to Customise Your Feet Ltd, a company incorporated in England and Wales (with registered number 047683728) whose registered office is at 9 Hatton Street, London, NW8 8PL, United Kingdom. We are registered as a data controller with the Information Commissioner's Office with registered number Z8326108. We will at all times only collect and process your personal information in accordance with the Data Protection Act 1998, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any other applicable data protection legislation. Our nominated representative under the Data Protection Act 1998 is Joe Stephens.

This policy was last updated on 01/01/2016.

What personal data do we collect? +

How do we use your personal data? +

Is your personal data used for marketing? +

Is your personal data shared? +

Is your personal data sent outside of the European Economic Area? +

What are your rights? +

What security measures are in place to protect your personal data? +

How can you contact us? +

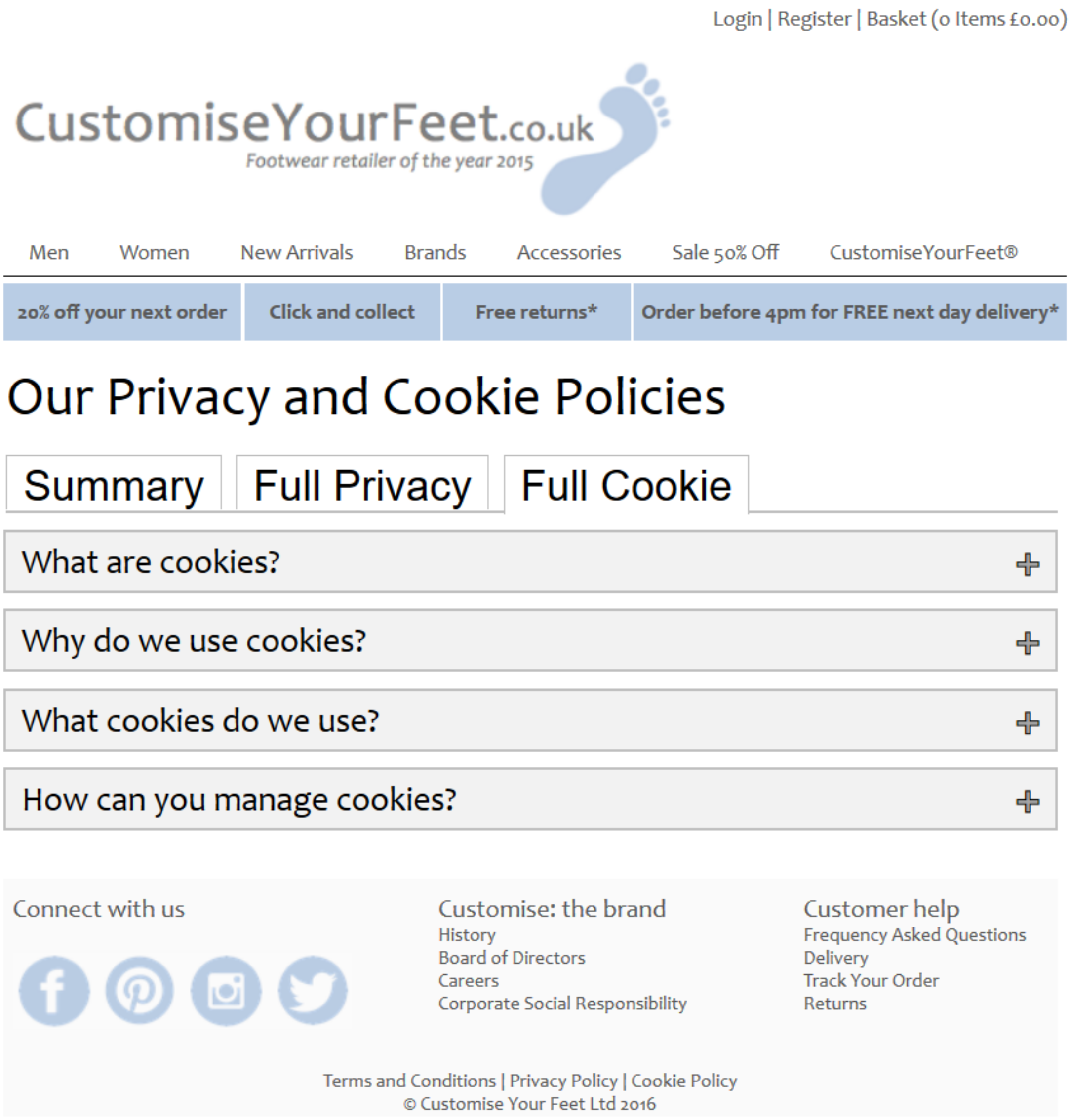
How can you contact the Information Commissioner's Office? +

Connect with us

Customise: the brand
History
Board of Directors
Careers
Corporate Social Responsibility

Customer help
Frequency Asked Questions
Delivery
Track Your Order
Returns

Terms and Conditions | Privacy Policy | Cookie Policy
© Customise Your Feet Ltd 2016



Login | Register | Basket (0 Items £0.00)

CustomiseYourFeet.co.uk

Footwear retailer of the year 2015

Men Women New Arrivals Brands Accessories Sale 50% Off CustomiseYourFeet®

20% off your next order | Click and collect | Free returns* | Order before 4pm for FREE next day delivery*

Our Privacy and Cookie Policies

Summary | Full Privacy | Full Cookie

What are cookies? +

Why do we use cookies? +

What cookies do we use? +

How can you manage cookies? +

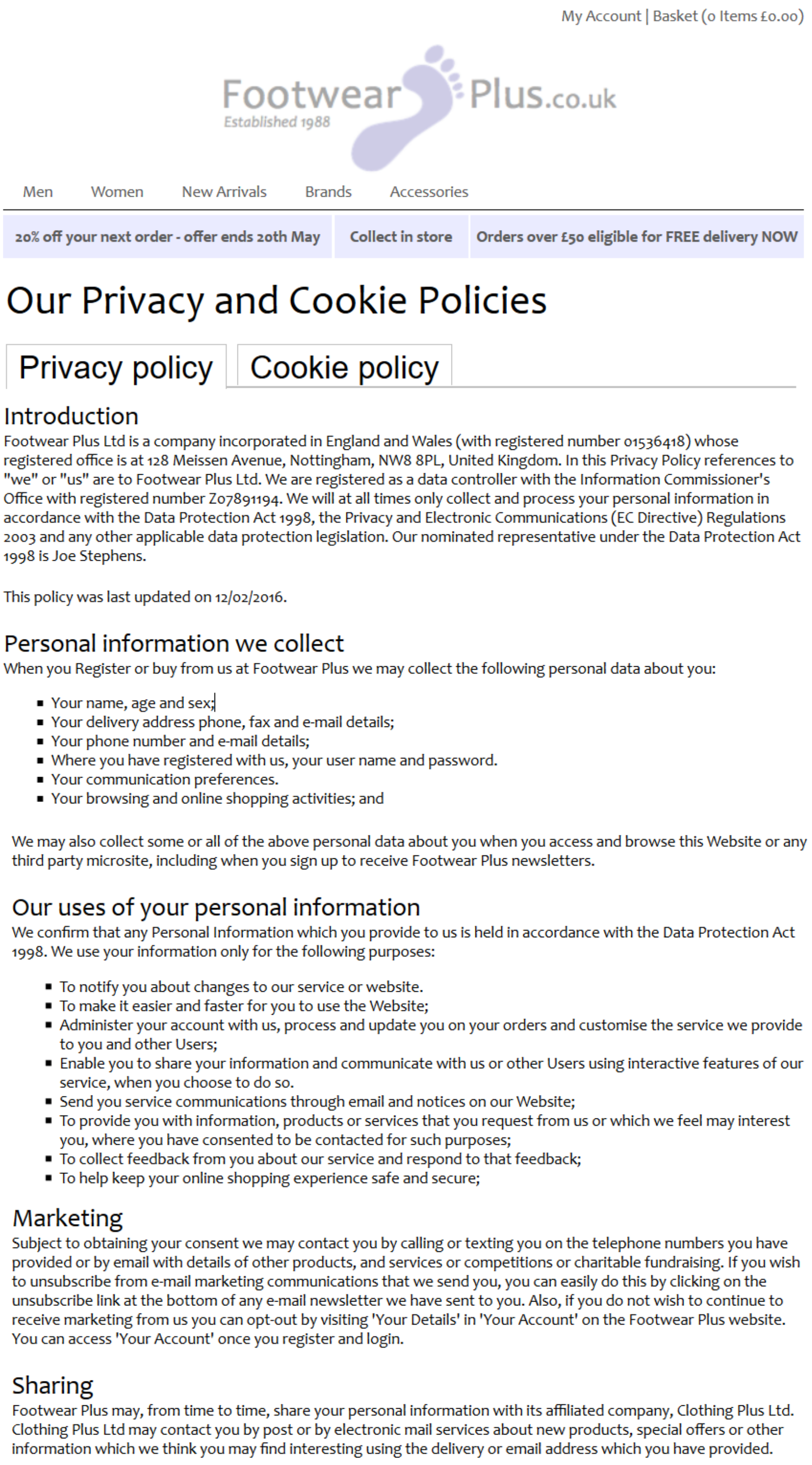
Connect with us

Customise: the brand
History
Board of Directors
Careers
Corporate Social Responsibility

Customer help
Frequency Asked Questions
Delivery
Track Your Order
Returns

Terms and Conditions | Privacy Policy | Cookie Policy
© Customise Your Feet Ltd 2016

Appendix I: Phase Four Typical Privacy Policy


My Account | Basket (0 Items £0.00)
Footwear Plus.co.uk
Established 1988
Men
Women
New Arrivals
Brands
Accessories
20% off your next order - offer ends 20th May
Collect in store
Orders over £50 eligible for FREE delivery NOW
Privacy policy
Cookie policy

Our Privacy and Cookie Policies

Introduction

Footwear Plus Ltd is a company incorporated in England and Wales (with registered number 01536418) whose registered office is at 128 Meissen Avenue, Nottingham, NW8 8PL, United Kingdom. In this Privacy Policy references to "we" or "us" are to Footwear Plus Ltd. We are registered as a data controller with the Information Commissioner's Office with registered number Z07891194. We will at all times only collect and process your personal information in accordance with the Data Protection Act 1998, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any other applicable data protection legislation. Our nominated representative under the Data Protection Act 1998 is Joe Stephens.

This policy was last updated on 12/02/2016.

Personal information we collect

When you Register or buy from us at Footwear Plus we may collect the following personal data about you:

- Your name, age and sex;
- Your delivery address phone, fax and e-mail details;
- Your phone number and e-mail details;
- Where you have registered with us, your user name and password.
- Your communication preferences.
- Your browsing and online shopping activities; and

We may also collect some or all of the above personal data about you when you access and browse this Website or any third party microsite, including when you sign up to receive Footwear Plus newsletters.

Our uses of your personal information

We confirm that any Personal Information which you provide to us is held in accordance with the Data Protection Act 1998. We use your information only for the following purposes:

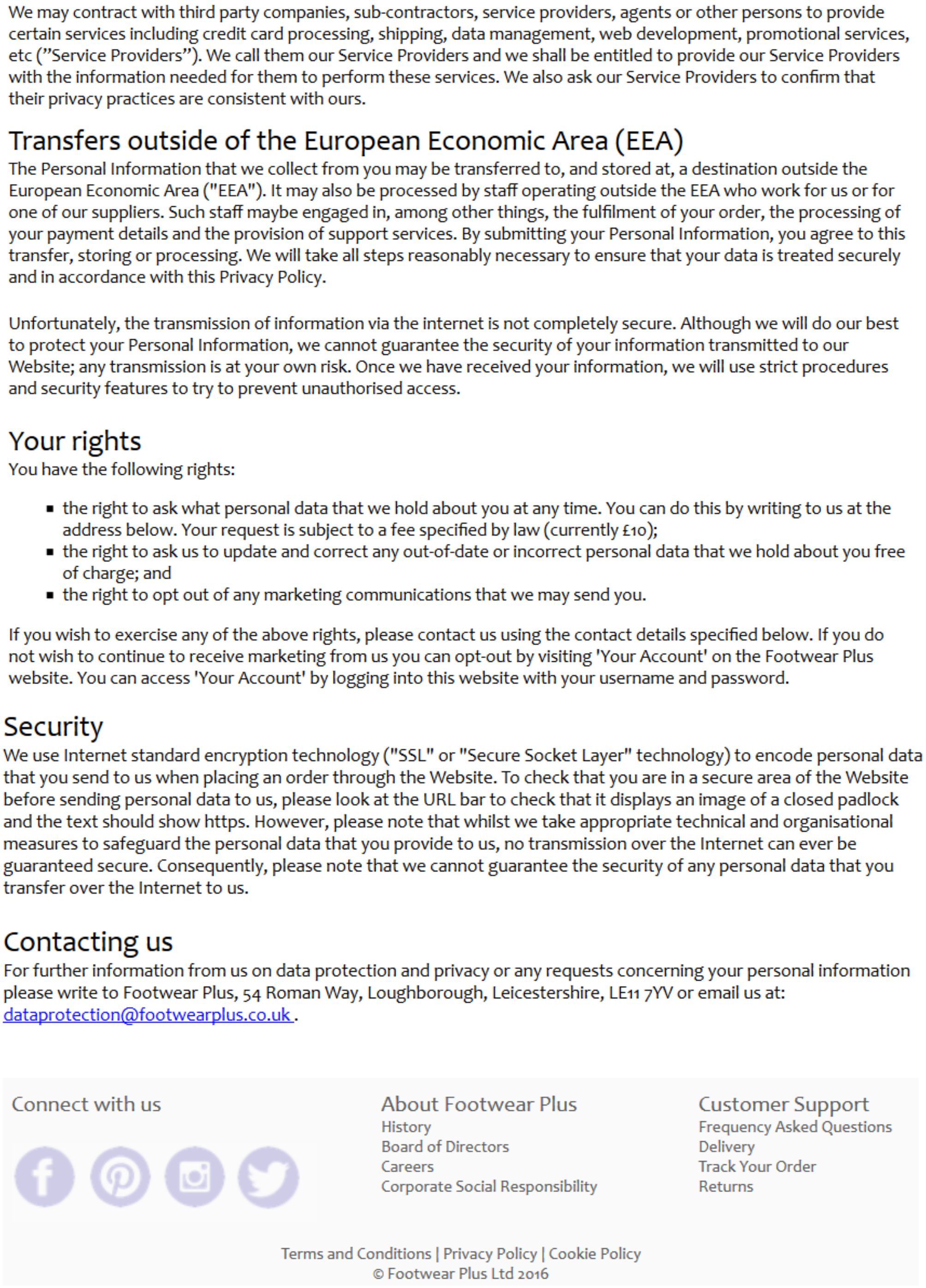
- To notify you about changes to our service or website.
- To make it easier and faster for you to use the Website;
- Administer your account with us, process and update you on your orders and customise the service we provide to you and other Users;
- Enable you to share your information and communicate with us or other Users using interactive features of our service, when you choose to do so.
- Send you service communications through email and notices on our Website;
- To provide you with information, products or services that you request from us or which we feel may interest you, where you have consented to be contacted for such purposes;
- To collect feedback from you about our service and respond to that feedback;
- To help keep your online shopping experience safe and secure;

Marketing

Subject to obtaining your consent we may contact you by calling or texting you on the telephone numbers you have provided or by email with details of other products, and services or competitions or charitable fundraising. If you wish to unsubscribe from e-mail marketing communications that we send you, you can easily do this by clicking on the unsubscribe link at the bottom of any e-mail newsletter we have sent to you. Also, if you do not wish to continue to receive marketing from us you can opt-out by visiting 'Your Details' in 'Your Account' on the Footwear Plus website. You can access 'Your Account' once you register and login.

Sharing

Footwear Plus may, from time to time, share your personal information with its affiliated company, Clothing Plus Ltd. Clothing Plus Ltd may contact you by post or by electronic mail services about new products, special offers or other information which we think you may find interesting using the delivery or email address which you have provided.



We may contract with third party companies, sub-contractors, service providers, agents or other persons to provide certain services including credit card processing, shipping, data management, web development, promotional services, etc (”Service Providers”). We call them our Service Providers and we shall be entitled to provide our Service Providers with the information needed for them to perform these services. We also ask our Service Providers to confirm that their privacy practices are consistent with ours.

Transfers outside of the European Economic Area (EEA)

The Personal Information that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff maybe engaged in, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. By submitting your Personal Information, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your Personal Information, we cannot guarantee the security of your information transmitted to our Website; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Your rights

You have the following rights:

- the right to ask what personal data that we hold about you at any time. You can do this by writing to us at the address below. Your request is subject to a fee specified by law (currently £10);
- the right to ask us to update and correct any out-of-date or incorrect personal data that we hold about you free of charge; and
- the right to opt out of any marketing communications that we may send you.

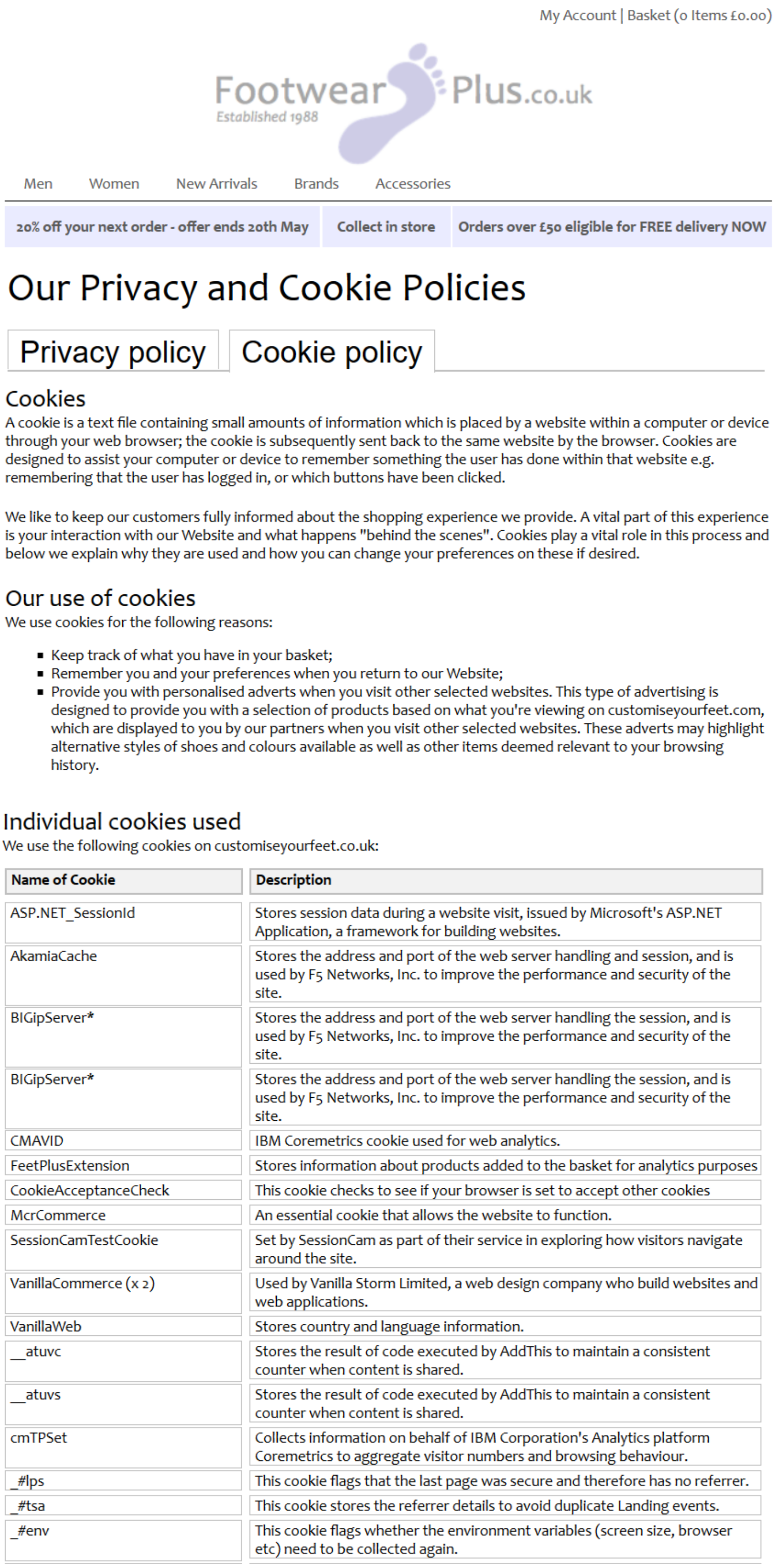
If you wish to exercise any of the above rights, please contact us using the contact details specified below. If you do not wish to continue to receive marketing from us you can opt-out by visiting 'Your Account' on the Footwear Plus website. You can access 'Your Account' by logging into this website with your username and password.

Security

We use Internet standard encryption technology ("SSL" or "Secure Socket Layer" technology) to encode personal data that you send to us when placing an order through the Website. To check that you are in a secure area of the Website before sending personal data to us, please look at the URL bar to check that it displays an image of a closed padlock and the text should show https. However, please note that whilst we take appropriate technical and organisational measures to safeguard the personal data that you provide to us, no transmission over the Internet can ever be guaranteed secure. Consequently, please note that we cannot guarantee the security of any personal data that you transfer over the Internet to us.

Contacting us

For further information from us on data protection and privacy or any requests concerning your personal information please write to Footwear Plus, 54 Roman Way, Loughborough, Leicestershire, LE11 7YV or email us at: dataprotection@footwearplus.co.uk .



My Account | Basket (0 Items £0.00)

Footwear Plus.co.uk
Established 1988

Men Women New Arrivals Brands Accessories

20% off your next order - offer ends 20th May | Collect in store | Orders over £50 eligible for FREE delivery NOW

Our Privacy and Cookie Policies

Privacy policy | Cookie policy

Cookies

A cookie is a text file containing small amounts of information which is placed by a website within a computer or device through your web browser; the cookie is subsequently sent back to the same website by the browser. Cookies are designed to assist your computer or device to remember something the user has done within that website e.g. remembering that the user has logged in, or which buttons have been clicked.

We like to keep our customers fully informed about the shopping experience we provide. A vital part of this experience is your interaction with our Website and what happens "behind the scenes". Cookies play a vital role in this process and below we explain why they are used and how you can change your preferences on these if desired.

Our use of cookies

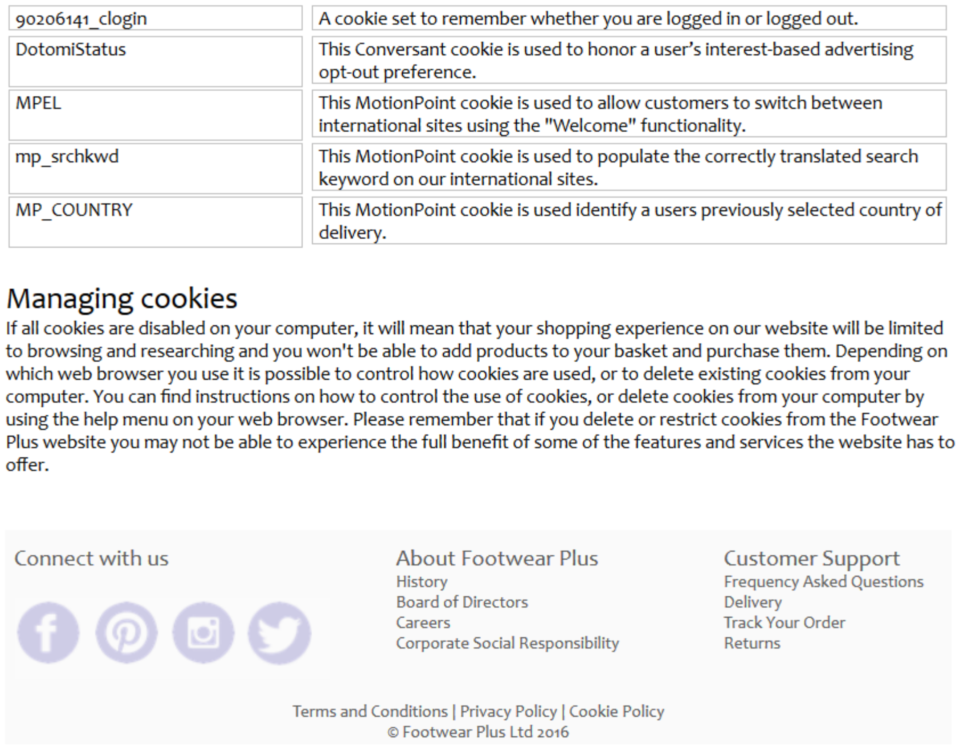
We use cookies for the following reasons:

- Keep track of what you have in your basket;
- Remember you and your preferences when you return to our Website;
- Provide you with personalised adverts when you visit other selected websites. This type of advertising is designed to provide you with a selection of products based on what you're viewing on customiseyourfeet.com, which are displayed to you by our partners when you visit other selected websites. These adverts may highlight alternative styles of shoes and colours available as well as other items deemed relevant to your browsing history.

Individual cookies used

We use the following cookies on customiseyourfeet.co.uk:

Name of Cookie	Description
ASP.NET_SessionId	Stores session data during a website visit, issued by Microsoft's ASP.NET Application, a framework for building websites.
AkamiaCache	Stores the address and port of the web server handling and session, and is used by F5 Networks, Inc. to improve the performance and security of the site.
BIGipServer*	Stores the address and port of the web server handling the session, and is used by F5 Networks, Inc. to improve the performance and security of the site.
BIGipServer*	Stores the address and port of the web server handling the session, and is used by F5 Networks, Inc. to improve the performance and security of the site.
CMAVID	IBM Coremetrics cookie used for web analytics.
FeetPlusExtension	Stores information about products added to the basket for analytics purposes
CookieAcceptanceCheck	This cookie checks to see if your browser is set to accept other cookies
McrCommerce	An essential cookie that allows the website to function.
SessionCamTestCookie	Set by SessionCam as part of their service in exploring how visitors navigate around the site.
VanillaCommerce (x 2)	Used by Vanilla Storm Limited, a web design company who build websites and web applications.
VanillaWeb	Stores country and language information.
__atuvc	Stores the result of code executed by AddThis to maintain a consistent counter when content is shared.
__atuvs	Stores the result of code executed by AddThis to maintain a consistent counter when content is shared.
cmTPSet	Collects information on behalf of IBM Corporation's Analytics platform Coremetrics to aggregate visitor numbers and browsing behaviour.
_#lps	This cookie flags that the last page was secure and therefore has no referrer.
_#tsa	This cookie stores the referrer details to avoid duplicate Landing events.
_#env	This cookie flags whether the environment variables (screen size, browser etc) need to be collected again.



90206141_clogin	A cookie set to remember whether you are logged in or logged out.
DotomiStatus	This Conversant cookie is used to honor a user's interest-based advertising opt-out preference.
MPEL	This MotionPoint cookie is used to allow customers to switch between international sites using the "Welcome" functionality.
mp_srchkwd	This MotionPoint cookie is used to populate the correctly translated search keyword on our international sites.
MP_COUNTRY	This MotionPoint cookie is used identify a users previously selected country of delivery.

Managing cookies

If all cookies are disabled on your computer, it will mean that your shopping experience on our website will be limited to browsing and researching and you won't be able to add products to your basket and purchase them. Depending on which web browser you use it is possible to control how cookies are used, or to delete existing cookies from your computer. You can find instructions on how to control the use of cookies, or delete cookies from your computer by using the help menu on your web browser. Please remember that if you delete or restrict cookies from the Footwear Plus website you may not be able to experience the full benefit of some of the features and services the website has to offer.

Connect with us

About Footwear Plus
History
Board of Directors
Careers
Corporate Social Responsibility

Customer Support
Frequency Asked Questions
Delivery
Track Your Order
Returns

Terms and Conditions | Privacy Policy | Cookie Policy
© Footwear Plus Ltd 2016