

Online trust and perceived utility for consumers of web privacy statements

Mark Gazaleh

17.08.2008

WBS



Table of Contents:

1. Introduction..... 3

2. Objective..... 4

3. Methodology..... 5

4. Literature overview on web trust and web privacy statements..... 7

 Importance of trust for trade & business development..... 7

 Web trust and control 8

 The advantages of trust for web commerce 8

 Web site strategies to engender trust 10

 The issue of Web privacy..... 10

 What is privacy? 11

 How is privacy impacted on the web? 11

 The Privacy Statement 12

 Concern regarding Privacy Statements..... 13

 Privacy Notices and the Law..... 13

 Privacy seals and trust..... 14

 Literature Review Conclusion regarding Trust and Privacy 15

5. Primary Research..... 16

 Privacy Statements on UK web sites 16

 UK privacy statements content 17

 Focus groups..... 18

 Questionnaire..... 19

6. Conclusion 26

Bibliography..... 28

Annex A – Web site rankings (February-March 2008) 32

Annex B – An overview of privacy statement attributes of three top UK sites 34

Annex B/1 – Amazon.co.uk Privacy Statement..... 35

Annex B/2 – Argos.com Privacy Statement..... 42

Annex B/3 – Play.com Privacy Statement 46

Annex C – Material Preparation for Focus Group Sessions..... 50

Annex D – Main conclusions of Focus Group Sessions..... 51

Annex E – Questionnaire 53

1. Introduction

The issue of trust has been deemed critical in most aspects of commercial exchange. The realm of electronic business is no exception to this rule. The prominence of this issue has been highlighted by recent events in which the security of personal data has been compromised by large corporations and state entities. When shopping online, the consumer is aware that their personal data may be used in an unauthorized manner, lost or sold to third parties. The role of privacy and the security of personal data figures prominently in literature discussing the importance of trust in commercial web interactions.

Industry best-practice and regulatory requirements have encouraged or mandated the use of 'privacy statements'. However, it is unclear whether the inclusion of different types of privacy statements has had a real impact on consumer behaviour. For example, although statements potentially provide increased transparency to the consumer, the immediacy of the web medium may at best preclude the likelihood that the statements are reviewed prior to on-line registration.

Much literature has stated that trust in a web site is likely to be based on the strength of its brand, previous consumer experience with the company and the look and feel of the website. In this context, research will examine the extent to which consumers are aware of the role of privacy statements and whether these statements actually strengthen trust in a web site.

2. Objective

The objective of the research is to examine the role of privacy statements at the point when consumers are deciding whether to use a web site. Much literature confirms the importance of trust and the significance of privacy and data security to web consumers. Privacy and data security would seem to be key elements in the establishment of trust between transacting parties on the web.

The paper will seek to assess whether the reading of a website's privacy statement is a required action for it to become trusted by web site consumers. This question will be examined within the context of the main attributes required for trust by these 'online' consumers. To achieve this, the research will examine the validity of the following statements:

H1] Internet consumers are concerned about the privacy of their personal information

Higher levels of concern may suggest that privacy protection will play an important role in the fostering of trust in a web site.

H2] The reading of privacy statements does not establish consumer trust in the web site

If the reading of privacy statements does not engender user trust, then the information in the statements may be deemed unhelpful or counterproductive.

H3] Privacy statements are generally not read by internet consumers

If privacy statements are not read then their general utility to users may be quite limited.

H4] Among the many factors contributing to internet user trust, the company brand, the look and feel (performance) of the site are the strongest in engendering trust in the web site.

If other factors appear to play a far more dominant role in establishing users' trust in a web site, then the role of privacy statements in generating trust may not be significant.

If, as the literature suggests, privacy statements are rarely consulted prior to web site use, then an analysis will be carried out as to the possible reasons why these statements are neglected by website users.

3. Methodology and Project Plan

The paper relies on the analysis of primary and secondary research resources. The secondary research reviewed articles available through libraries and on-line research facilities. This included a review of available books, manuals, and journal articles. The project entailed research in the following areas:

Secondary Research:

The project first focused on a review of literature of the general realm of trust and its antecedents within the context of web-based commercial interactions. This was followed by a review of literature regarding the role played by privacy statements, and other privacy 'tools', in the establishment of consumer trust for web sites. A thorough literature review was thought most appropriate, given that the theoretical underpinnings for the concepts of both trust and privacy are found in a variety of disciplines.

Primary Research:

Primary research was conducted to examine the form and placement of the privacy statements on the three top web sites in the UK. The study looked at indicative placement and content patterns of three top UK commercial web sites. The results provided the necessary structure for a small set of individual (focus group) interviews of university web users. The focus group sessions focused on the validity of the hypotheses H1-H4 noted in the paper's objectives (Section 2).

The interviews' semi-flexible structure confirmed the most pertinent areas for investigation and effective questions format for later research. As a result, the questionnaire took into account the findings in the focus groups and was also structured to examine the hypotheses H1-H4. The questionnaire method was chosen as the most efficient means available to assess patterns and frequencies in research data.

A web-based questionnaire was used so that as many subjects as possible were able to participate in the study. Furthermore, it was thought that a well-structured questionnaire data may well be easier to process than interview-derived results. The efficiency offered by the questionnaire method was deemed crucial when considering the limited time and resource available for the project (Zoltan 2003). Information regarding the size of the questionnaire sample and response rates is detailed later in this paper.

The literature review assisted in the interpretability of the interview, focus group and questionnaire survey data. The research design was in part determined by resource constraint (access to literature, time and cost). The focus group research was conducted primarily to validate the hypotheses of this paper and the structure of the subsequent questionnaire survey. This research benefitted from the low cost, quick results, and the efficiency of being able by talking with several people at once. Its semi-flexible structure was also beneficial as it allowed ad-hoc examination of detailed areas of enquiry. The questionnaire survey was considered suitable as it could be delivered widely and processed at low cost. A certain bias within the sample groups may well be significant – in that the sample was drawn from the author's personal, professional and academic network of contacts and peers. Bias and the limitations of this research will be discussed in greater

detail later in this paper. Through the 'methodological triangulation' of the results of the primary and secondary research, this study will hopefully provide a clearer understanding of the chosen topic.

The details of the project plan and timeframe are included in Annex F.

4. Literature overview on web trust and web privacy statements

Many observers have argued that the growth of electronic business (e-business) is partly dependant on how well the general public trusts the virtual environment.¹ Trust is seen as a facilitator of business growth and as such generated considerable academic and professional interest. A great deal of literature exists on trust on the internet. It has been recognised that the virtual environment should eventually match systems that have evolved in the real world in order to prevent deception and fraud (Castelfranchi 2001). In cases of information asymmetry, there is always a risk of opportunistic behaviour by one of the transacting parties (Yao-Hua 2001). It is important to note, that “Trust has been shown to have significant positive effects on people’s intentions to make online purchases and disclose personal information willingly” (Chau 2007). It has been argued that trust is mainly required in situations of risk. The levels of risk and vulnerability are determined by the amount of information available to the two parties. Trust entails four key concepts: propensity to be vulnerable to another, perception of ability and competence of another, perceived benevolence of the other and perceived integrity of the other (Roy 2001).

Significance of trust for trade & business development

Trust has been seen as a form of ‘social glue’ which fosters economic activity and efficiency. For example, the establishment of trust may preclude the requirement for monitoring and/or sanctioning mechanisms to ensure that transactions complete successfully (Mutz 2005). In brief, trust

- requires a good relationship between parties
- takes some time to be established
- requires an exchange of tangible and/or intangible favours
- is needed when uncertainty and risks are recognised
- allows exchanges to be carried out more smoothly

It has been suggested by May (2002) that trust is one of the four ‘must-haves’ for e-business success. These four include satisfaction-quality, value, risk, trust. Trust is seen as an essential element in any type of transaction (May 2002) and especially relationship marketing, as it encourages companies to “preserve relationship investments and resist attractive short-term opportunistic alternatives” (Mukherjee 2003).

Trust has been seen to be a crucial requirement for the development of trade over distances. It would remain important alongside the development of credit reports, product catalogues and long distance delivery services. For example, credit records may act as (partial) substitutes for trust, and act as “parallel, portable self(s) that could be known and acted upon when the real self was distant in time and place” (Mutz 2005). Even now, web trust may be negatively impacted when web buyers and sellers are “physically separated, contingencies are difficult to predict, and cyber-laws not well defined” (Mukherjee 2003).

¹ Others have described different types of trust: these included trust in the environment and infrastructure (socio technical system); trust in your agent or mediating agents; trust in your partners; trust in the authorities. It is also important to note that trust requires more than just secure connectivity (via say, public key cryptography). The (prospective) client must also be able to trust the quality of the information being provided by his/her partner and also whether his/her partner will safeguard his data

Trust may thus be seen a key component to (commercial) exchange and is a “catalyst for the development of marketing relationships” (Thompson 2007). Trust has been described as a “belief that a party’s word or promise is reliable” and is “a willingness to rely on an exchange partner in whom one has confidence” (Caldwell 2000). In this manner, trust plays an important role in interactions involving uncertainty and dependency. Since uncertainties exist in transactions over the internet, the stimulation and safeguarding of trust is critical (Thompson 2007).

Web trust and control

The realities of real physical separation and anonymity on the web do not help foster trust between buyers and sellers. Some have suggested this is partly to blame for the state of ‘perceived insecurity’ between users on the internet (Caldwell 2000). Scholars have argued that trust will remain a prerequisite for successful commerce, because consumers will remain hesitant to make a purchase unless they can trust the seller (Ferrin 2008). Others have suggested that a strong link exists between trust and perceived control. Trust, or the lack of it, may be effectively substituted by a “functionally equivalent control mechanism”. Examples of effective substitution mechanisms may include insurance policies, deposits or legal penalties (Williamson 1975).

The appropriate level of trust given to a web site by a user is determined through various cues. These cues, and the level of trust they engender, change over time. The user’s trust will be based on his/her evaluation of the site’s perceived professionalism (Roy 2001)² and reputation (Sisson 2000),³ alongside with its architecture navigation and control mechanisms (Chau 2007).⁴ It has also been suggested that customer orientation to information technology is frequently a ‘proxy’ for trust in electronic commerce. Any user disappointment regarding the competency of the system (network and download speed, navigability, reliability, connectivity and availability) usually negatively impacts the credibility of the web site (Lee 2001).

The advantages of trust for web commerce

Of the many business advantages trust can provide, the most notable are the reduction in transaction complexities, costs, the establishment of stable long-term relationships, the easing of concerns regarding the disclosure of confidential information, and a general reduction of perceived risk. Trust obviates the necessity for control mechanisms, contractual obligations, legal contracts, monitoring and litigation in internet business transactions (May 2002). The fostering of trust between transacting parties in e-business is thus most desirable. The establishment of trust, as noted above has many requirements, as one meta-study by Mc Cole (2002) summarizes these to include the following:

- Availability – the website offers fast solutions and response times. It is convenient and is available 24/7 to get things done
- Competence – transactions are completed competently without complication; performance and appearance meet expectations (Caldwell 2000)
- Consistency – interactions follow familiar patterns
- Discrete – any information exchanged is kept in confidence

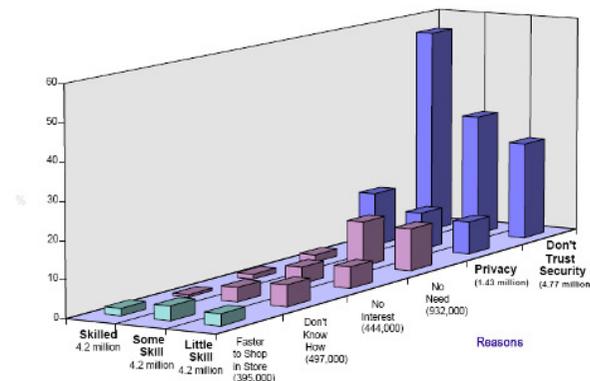
² For example, the coherence in the web site’s interface and design, functionality, usability and language places a important role. According to Nielsen (1994) usability often refers to the ease of learning how to use the interface, the efficiency of the interface design (consistency), the ease to memorise how to use the interface (learnability), user guidance (support), the reduction of errors, and the general satisfaction with the interface. (Roy 2001)

³ As noted by Sisson (2000), company size, brand and perceived reputation are key trust drivers.

⁴ Third party assurances, guarantees, legal system recourse with professional associations may support an online purchase decision.

- Fairness – cost saving over going through another medium. The merchant does not exploit opportunistic advantages (goodwill of its actions and lack of opportunistic behaviour)
- Integrity – truthfulness and honesty in information presented; good reputation (Flavian 2006)
- Openness – transparency with all information clearly presented
- Fulfilment – delivery made as to expectation/specification. This includes the goods, delivery time, costs etc
- Receptivity – user feels the benefit of focused/tailored information delivered to him/her (McCole 2002)

It has been noted that internet environment continues to be feared as a 'risky' environment – mainly due to perceived menace of identity loss, privacy loss and security intrusion. Many consumers remain reluctant to disclose personal information, especially if related to financial status and credit facilities. Surprisingly this perception and reluctance – as shown in the Nielsen Media Research (1997) chart below – has been suggested to be strongest in those who are the most skilled internet users (May 2002). Negative user perceptions regarding security and privacy appear to increase as users become more proficient with the web medium (Hoffman 1999). The primary research shown later in this paper has focused on highly educated and experienced internet users. The preliminary conclusions of the research on the whole confirm the view that these users are somewhat concerned about their internet privacy.



Reasons Consumers Do Not Buy On the Web (Nielsen Media Research 1997)

It is important to note the significance given to the elements of discretion, fairness and openness as pre-requisites for trust and e-business growth. These elements – and their particular relationships to privacy – will be discussed in greater detail, especially as they relate to privacy, later in this paper.

Web site strategies to engender trust

Research has shown that online organisations have not only understood that trust is important for their success, but have sought to mitigate consumer perceptions of risk while using their online stores. There are a number of examples of these mitigating strategies. These include the use of 'risk relievers' or signals for 'cue-based trust' such as money back guarantees, return policies or security and privacy disclosures (Andrews 2008).

Other organisations have sought to reduce risk perceptions and alleviate any trust issues through the transfer of risk back to the company itself. This has been done by increasing the company's perceived trustworthiness,⁵ assumption of greater risk in the transaction, and providing additional value to the consumer's transaction (achieved for example with lower costs). Nevertheless, within the general scope of trust for e-business, there remains a sense that consumers remain uneasy about disclosing personal information to a seemingly distant and impersonal channel. Many potential transactions may fail as the trust levels are deemed insufficient to overcome perceived risks (May 2002). One widely identified area of risk has been the impact on privacy through the disclosure of personal information which has led to fraud and identity theft.

Given their prevalence, the use of privacy statements is common on most commercial web sites. Not only has the law or industry self regulation played a large role in this, but the statements may also play a role in a mitigation strategy used by companies to help promote trust. Their mere heuristic presence may be helpful to create a seemingly more trusting environment.

The issue of Web privacy

Individuals using the net may have yet to fully appreciated the extent to which web technologies are able to collect, disseminate and combine vast amounts of user data. This ability fundamentally changes the 'data intelligence' relationship between online merchants and consumers (Pollach 2005). Web businesses admit that personal information is now being collected, sometimes without users' knowledge,⁶ as an 'unavoidable' by-product of electronic commerce. Furthermore, once the data is captured, users may not realise their now limited control over the use of their data – which may be traded, rented, or sold (Ontario 2001) without further notice (Clay 2000). In addition, it has not been fully understood that web sites may be forced, regardless of any assurances previously given, to disclose their clients' personal data in a court of law (Bouguettaya 2003). In this environment it would seem quite easy to compile a dossier on an individual by combining data compiled from different data sources (web sites).

Unlike in conventional retailing, web-based consumers are unable to remain anonymous in internet transactions (Kai-Lung 2007). The web's impact on the consumer's privacy,⁷ and the information

⁵ Perceived trustworthiness can be increased by a number of factors. This could include third party endorsements, risk transference (though guarantees), and increased user transparency (order processing).

⁶ Some users remain unaware of the new forms of personal information being gathered. Much more detail is being recorded, beyond just transactional data. They are being profiled by their 'click-paths' of web activity.

⁷ Privacy has been defined in terms of an individual's control over disclosure and subsequent uses of personal information. The OECD refers to five key elements required for the establishment of privacy. These are

- a) notice awareness: participants should receive notice of an entities information practices before they divulge any personal information;
- b) choice/consent: participants should be given options as to the uses if any personal information collected from them, especially for secondary uses that are unrelated to the original transaction (sale of information to third parties);

asymmetry between web site and user, may require “an offset of higher levels of trust” (Schoder 2004). This ‘trust offset’, or investment in additional trust, should counteract the fear of opportunistic behaviour by unscrupulous web sites (Schoder 2004). This opportunistic behaviour may result in the transfer of sensitive data to unauthorized third parties, the misuse of personal information, the possibility of price discrimination and unauthorized marketing solicitations (Laufer 1977). Lack of web trust has been attributed to the perceived lack of control web-consumers feel when disclosing their personal information and conducting their business on-line. Studies have shown that consumer expectations for data security are far higher for the internet environment than those found in traditional media fields.⁸ A study performed by IBM showed that 77% of American consumers declared themselves to be confident regarding the confidentiality of the information transmitted to their banks. However, only 21% stated similar confidence when communicating personal information for on-line purchases (IBM 1999).

There is much literature documenting continued consumer concern regarding their online privacy (Hoffman 1999). A Jupiter Communications study in 2002, suggested that the web sector lost \$18 billion worth of business per annum due to consumer concerns over their privacy. Similarly in 2006, research from the Gartner Group confirmed that the lack of confidence by web user in their online privacy could well be the greatest long-term inhibitor for consumer-based e-business (Bouguettaya 2003).

What is privacy?

It is useful here to briefly pause to assess the make up of the concept of privacy. Privacy is a broad intellectual and philosophical idea and generally refers to the protection of personal information and the “right to be alone” (Clarke 1999). As such, privacy has been seen primarily as a human or social right, arising from an individual having free will (De Boni 2002). Privacy concerns are “an example of human value (a desire to control personal information flows) instantiated via the design of software systems and services” (Brunk 2002). Privacy also refers to the individual’s right to control the extent to which his/her personal information is shared and how it can be used. It has also been said that privacy is important, especially in a democracy, as it affects the way we feel and act (Brunk 2002). Studies indicate a growing preoccupation with the disclosure of personal information and web-use history privacy. Furthermore, these studies also show a desire to avoid even anonymous sharing of personal information to third parties without explicit consent (McCole 2002). It seems possible that there is a trust issue regarding privacy and the loss of control over personal information.

How is privacy impacted on the web?

Consumers may have yet to understand the extent to which technology is increasing able to make sense of the huge volume of personal data harvested from internet transactions and interactions. As they gain more experience, users may then become less tolerant to the information risks they face on the internet. Furthermore, data aggregators are known to combine data from separate sources in order to fully develop the consumer profiles of specific individuals. It also is important to note again,

-
- c) access and participation: participants should have access to information recorded about them and be able to modify any information deemed incorrect
 - d) integrity/security: collectors must take steps to ensure data integrity, convert it into anonymous form before using it for secondary purposes and to destroy untimely data
 - e) enforcement/redress: there must be a mechanism in place to enforce the privacy policies (Jamal 2005)

⁸ 87% of respondents felt that they should have complete control of their personal data, while 71% felt that they should be news laws to protect their privacy on line (Georgia Tech Research Group 1997).

that data previously authorised for release by the individual may no longer controllable or retractable once it is in the hand of third parties (Henderson 2005). There is also a risk that once the data is combined with that of other sources, this may result in third parties having knowledge which the consumer would not authorise them to have (Schoder 2004). The extent to which web sites can acquire different types of personal data is extensive. A few examples of the methods and technologies were provided by Bouguettaya (2003). Some of which have been listed below. These include:

- Data Magnets (tools used to collect personal data)
 - Various techniques exist:
 - Online registration requirement.
 - IP (MAC) addresses identification and link to user ID
 - Secure downloads with embedded unique identifiers
 - Cookies (small files lodged on client PC to track user activity)
- Weak security
 - Allowing unauthorized access due to weak access or hacking
- Trojan Horses
 - software spawning malicious features such as the acquisition of personal data
- Web beacons (web bugs, pixel tags or clear gifs)
 - small transparent graphic image that monitor user activity
- Screen Scraping
 - Process to capture valuable information from user web pages
- Indirect information collection and processing
 - Information is collected and analysed. This produces new and (unauthorised) knowledge or facts about the subject’s person and or personality

While concern for the confidentiality of personal information seems widespread, 64% of US adult consumers report that they have not sought advice on how to protect their information and 40% report being unaware about how to prevent web sites from collecting their information (Bouguettaya 2003).

The Privacy Statement

Industry self-regulation (due in part to market demand) and government regulation has mandated increased transparency in the information privacy sector. As a result, web sites usually now declare their policy regarding personal data in privacy statements published on their web sites. The policies should in principle refer to implicit and explicit rules that determine what information will be acquired, retained and transferred, and whether that information will be manipulated in any way (Bouguettaya 2003). The ‘trust’ role of the policy statement is to reduce the information asymmetry between the merchant and the consumer (Pollach 2005). However, it has been suggested be that the full ‘trust’ potential of the statement can only be fully realized if consumers read and use the information contained in the notices (Milne 2004). This paper’s research indicates that this is not the case – as users rarely, if ever, read the contents of these privacy statements.

Concern regarding Privacy Statements

Despite both EU legal and US self-regulation requirements for privacy notices, there does not seem to be an agreed format and content standard that the industry should follow. These notices are frequently very long, and of varying style/format, making comprehension difficult and time consuming. Site users may be ill-inclined to read long and detailed statements as these will diminish their ability to transact rapidly on the web. It also has been suggested that statements may be in place solely for compliance purposes, as their contents seem “exhaustive and not really accessible to consumers (or even) informative” (Milne 2004).

Privacy statements have also been described as vague, perhaps in order to allow the issuing organisation to retain flexibility over the use of the data it is acquiring (Milne 2004). It has also been demonstrated that some privacy statements might even be deceptive, with a use of language that “mitigates (the) negative effects of their policies and obscures responsibility and causality” (Pollach 2005). One researcher strikingly asserted that most readers are unable to fully evaluate the contents of a privacy statement. Moreover, he stated that the comprehension of 80% of U.S. privacy statements required a university level education (Pollach 2005).

Even if the suggested high levels of web privacy concern are confirmed, research has shown that relatively few users take concrete actions to protect their information while online (Arcand 2007, pp.661-681). Using U.S. consumers as an example, two studies reported that only 5% of consumers read privacy statements at all (E-marketer, 2003), while 31% only bothered to read them “most of the time” (E-marketer, 2002). As stated earlier, many simply do not look at these statements as they detract from the immediacy of the medium (Arcand 2007). Privacy statements have also been criticised because their policies are ‘self proclaimed’ and not necessarily corroborated (Luo 2004). Other findings suggest privacy notices are less read once consumers have prior positive experience with the organisation (Milne 2004).

Research suggests that consumers perform simple risk-benefit calculations in deciding whether or not to disclose their information. Consumers are more likely to disclose their personal information once they perceive that the benefit of disclosure exceeds the risks of such an action (Culnan 1999). Also, once privacy information is made more visible, people will tend to purchase from merchants that offer more privacy protection and even pay a premium to purchase from such merchants (Tsai 2007, p.22). Furthermore, it has been noted that the presence (but not necessarily the reading) of privacy statement may also increase users’ feeling of ‘perceived’ control. This perceived control in turn may increase their level of trust granted to a web site (Arcand 2007, p.663) and encourages users to disclose private information. This was noted to be especially the case if disclosure made a financial gain (for example, special pricing or discounts) possible (Kai-Lung 2007).

However there remains a suspicion that privacy statements are rarely read and thus their role in promoting trust is limited. It has been suggested that they are not being reviewed prior to personal information being disclosed because the risk to the individual’s privacy is deemed insignificant or statements’ contents are thought to untrustworthy or inaccurate (Milne 2004).

Privacy Notices and the Law

It would seem that the privacy of individuals on internet is protected by UK law. Data protection here is regulated by the Data Protection Act, which was amended in 1998 and complies with the EU’s

Directive on Data Protection.⁹ It should be noted, however, that the UK has a more permissive interpretation of the Directive than most other EU member states.¹⁰ One study noted that UK privacy statements were harder to find than those on US sites and their levels of non-compliance to UK and EU privacy laws were substantial (Jamal 2005).

Clearly if long-term abuse of private information occurs on the web then the trust and credibility of this medium will be damaged. Privacy statements are a means for consumers to determine the risk of disclosing personal information to a particular web site. Disclosure of personal information does require trust – as information asymmetries limit the consumers’ knowledge of what will happen to their information. Privacy notices are intended to reduce this information imbalance and to foster a trusted environment to assist in a site’s success (Henderson 2005).

It has been suggested that rather than reading privacy statements, consumers rely on alternative signals to assess the safety of their personal information. Here the ‘quality and trust’ of a site is assessed through evidence of

- direct 3rd party endorsement through privacy seals
- quality web site design and performance
- on- and off-line company credibility and reputation
- a strong company brand

It has also been suggested that certain users’ perceptions on their data’s security can be improved through positive previous experience with the company in the ‘real world’ (Henderson 2005).

This paper’s research confirmed that brand strength, previous positive experience with the company and web site performance (look and feel) were the most important factors for trust. Privacy seals and privacy statements were only somewhat helpful for trust maintenance. Their contents were rarely examined in detail by the site users.

Privacy seals and trust

As noted above, consumers can sometimes assess the privacy protection afforded them on a web site by examining the detail of its privacy seal. The purpose of third party seals is to assure the customer that the online vendor is trustworthy. Seal programmes mostly advocate privacy, security and reliability standards that are required by consumers. Privacy seals are more often found in self-regulated web environments such as in the United States rather than in Europe (where legal protection has been enacted). Privacy seals have been designed to invoke a transfer of trust, whereby the customer will transfer their trust from a known entity (for example, a trusted third party seal issuer) to a potentially unknown site with which the customer has little or no previous experience (Cook 2003).

However, the literature regarding the efficacy of privacy seals to establish trust is mixed. For example, it has been said that

⁹ The Directive stipulates that personal data must be processed fairly and lawfully and only collected for a specified, explicit and legitimate purpose. Data cannot be used for any secondary purpose beyond those stated. [Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data]

¹⁰ It allows consent to be implied so long as consumers are provided with an opportunity to opt out of the use of their personal data for secondary purposes.

- there was no significant effect of privacy seals – because the users did not trust or understand the particular seals being used (Kai-Lung 2007)
- seals engendered more trust but they did not significantly and consistently influence disclosures of personal information
- consumers mainly use seals heuristically to confirm the site as ‘privacy safe’ while ignoring the seal’s contents (and the detail of the site’s privacy policy)
- seals gave privacy statements greater credibility to the reader about what was being collected, how it was collected and with whom it was shared (Rifon 2005)
- many users still remain unaware that websites (and their privacy statements) can be endorsed by third parties (Kim 2008)

Furthermore, certain privacy seal programmes have not been without their own problems. Some seal authorities have been found to have violated their own privacy and security standards by selling client information to third party marketing companies (Rifon 2005). Also in another case, a major seal issuer ([TrustE](#)) has been accused of not being tough enough on deficient web sites it had accredited. TrustE, and web seal companies like them, are faced with an inherent conflict of interest – they cannot make the lives of companies that sponsor them too difficult (Erlanger 2004).

As noted above this paper’s indicative research found that privacy seals were not considered a significant contributor to web trust. This may be due in part to the proportion of UK respondents in the focus groups and survey. Privacy seals may play a larger role in self-regulated internet markets such in the United States – than in the regulated single European market.

Literature review conclusions regarding Trust and Privacy

The literature seems to indicate a clear link between trust and privacy. The literature suggests that the continued development of consumer trust seems to be a significant issue upon which the growth of any internet business will depend. Trust and control – including control over personal information – will remain important considerations for commercial internet success. Strategies have been put in place to help rebalance perceived information asymmetries. The literature suggests that privacy statements, amongst other tools, are used to reduce user perceived information risk.

Users may yet have to fully appreciate the extent to which internet linked technology can collect and assimilate personal information. The literature suggests that users have ‘significant’ concerns about the security of their information. The results of the paper’s primary research that follow validate this privacy concern but only up to a point. Privacy statements may be ‘risk relievers’ and helpful heuristic tools – but the brand, previous experience and site performance are the key drivers for consumer trust in a web site.

5. Primary Research

Primary research was conducted to examine the form and placement of the privacy statements on the three top web sites in the UK. The study looked at indicative placement and content patterns of three top commercial UK web sites.

The purpose of this section of the study was to

- provide the necessary structure for a small set of individual (focus group) interviews of university web users
- confirm the most pertinent areas for investigation and effective questions format for later questionnaire research
- provide the details for a better understanding of the attribute of privacy statements on commercial UK web sites and to provide additional validation for the findings of the secondary research

a) Privacy Statements on UK web sites

The research selected three examples of privacy statements in use on UK web sites. Three examples were sought in order provide greater details on the attributes of these statements. The research sought information to identify the three top retailer web sites by visit in the UK.¹¹

Interactive Media In Retail Group (IMRG) publishes with HITWISE a monthly top 50 ranking of UK website. The ranking is based on popularity as indicated by number of visits. IMRG, has a large number of UK PLC’s as members, and is an industry advocacy group that purportedly promotes e-commerce best practice. HITWISE, which is part of the Experian group of companies, refers to itself as a leading online competitive intelligence service. Experian has over 1400 global clients (Hitwise 2008). The ranking below, may arguably be the best available (for no cost) to the researcher.

The chart below, while only indicative, shows which web sites were at the top of the UK retail web charts at the beginning of 2008.¹² This research used these results as the basis for choosing the three top UK retail websites over a recent period. These were deemed the most appropriate for a short review of their privacy statements.

	November 2007	February 2008
Amazon.co.uk	1	1
Argos.co.uk	3	2
Play.com	2	3
Apple.com	5	4
Tesco.com	4	5

Source: IMRG Hitwise Hot Shop List February 2008

¹¹Web ranking data in the public domain was hard to come by. The only the exception to this, was the data provided free of charge by the IMRG.

¹²Please see **Appendix A** for further information.

UK privacy statements content

The privacy statement of the three top web sites underwent a brief analysis. The detail of this summary has been included in **Annex B**, with the reference policy statements for each site have been added in **Annexes B/1-3**.

Accessibility to the three statements was not an issue – links to the privacy statements were available in small type at the bottom of all pages. Nevertheless, it should be noted that the link positions were not prominent – and were sometime lost at the bottom of very long web pages (thus off screen). As such, it is more like that site users would have to actively look for the privacy statements – rather than find them by accident.

The statement lengths go from long (for example 3-4 screens for [play.com](#) and [argos.co.uk](#)) to very long (10 screens for [amazon.co.uk](#)). They are considered to be long in terms of the time required to read and understand the statements. The language in many parts of the texts downplays the extent of a potential threat or its occurrence. Examples of this include the words ‘might’, ‘may’, ‘occasionally’ and ‘some’. This confirms previous analysis which concluded that these statements are typically long-winded and hard for the average user to understand (Pollach 2005). Long sentences and complicated syntax (legalese) is also known not to be helpful.

The statements confirmed the use of various (extensive) technologies to track and profile users. The blocking of cookies would degrade the user functionality of the web site (the shopping carts in particular). Furthermore, it was stated that not only personal data could be shared and sold to third parties but it could even be exported outside the EU’s legal jurisdiction. Also, the sites hosted 3rd party content, advertisements and links to sites that were not bound by the terms of the privacy statement. Users would then have to research the privacy statements of these linked sites to determine the risk of proceeding.

The policies confirm that users’ data is protected by legislation (be it, UK law ([amazon.co.uk](#) and [argos.co.uk](#)), Jersey law ([play.com](#)), or Luxembourg law ([play.com](#) and [amazon.co.uk](#)). It is therefore assumed that users know what (level of) protection these legal jurisdictions afford them. It is unclear if users know how they are protected by the law. Furthermore, the language and length of the statements may well impair the likelihood that the privacy statements are understood fully or even read. The nature, format and length of the example privacy statements may not be in keeping with the immediacy of the web medium. The web consumer’s progress will be slowed considerably if comprehension of the site’s privacy policy is a prerequisite for (initial) web transaction.

More than eighty percent of all questionnaire respondents reported not reading privacy statements (80% of all respondents stated that they had used the [amazon.co.uk](#) web site). The focus group respondents -- most of whom reported accessing the site -- confirmed that its personal statement was not deemed useful for their immediate use. The long length of the statements, their legal references, lack of clarity and complexity – may indicate that most users would end up with greater privacy uncertainty if they read the site’s statement in detail.¹³

¹³ Further detail regarding the privacy statement attributes of top UK web sites have been listed in **Annex B**.

b) Focus groups

The research sought postgraduates that were reasonably heavy (experienced) web communicators and shoppers. The subjects needed not be experts in the web channel or its technologies, but it was assumed that they would have ample personal experience to assist them in answering the survey questions.

Two small focus groups were held at the end of May and the beginning of June 2008. The former group had two members while the latter had three members.

Focus group results:

Please see **Annexes C & D** for greater detail on the focus group results.

Focus group profile:

Focus group was well educated (all being post-graduates) individuals living in London. They were all experienced moderate to heavy Internet users who used the internet net every day to shop, research, read news and to communicate. Most perceived themselves to moderate to expert users of the net. Views regarding the level of legal protection of personal information were mixed. It should be noted that the groups were limited in number, size and population diversity.

Focus group conclusions:

H1] Internet consumers are concerned about the privacy of their personal information

Most (80%) felt the internet was not a safe environment. All interviewees were risk aware and used firewalls, virus protection on their computers. Biggest threats perceived were the risk of virus/malware attack and identity theft. Mechanical failure and loss privacy were not prominent concerns. All were aware of the role of privacy statements, but only half of the interviewees were aware the role of privacy seals and web certificates.

H2] The reading of privacy statements does not establish consumer trust in the web site

Most (80%) respondents stated that they did not read privacy statements to trust a web site.

H3] Privacy statements are generally not read by internet consumers

The remainder stated that statements were reviewed in order to build trust prior to a high value transaction. They stated that they did not read statements because of a perceived lack of time and relevance.

H4] Among the many factors contributing to internet user trust, the company brand, the look and feel (performance) of the site are the strongest in engendering trust in the web site.

The brand, look and feel, performance of a web site was stated to be key determinants of the level of trust it would receive. The privacy statement was only of a minor ‘trust’ consideration.

c) Questionnaire survey

Questionnaire Background

The research sought postgraduates that were reasonably heavy (experienced) web communicators and shoppers. The subjects similarly needed not be experts in the web channel or its technologies, but it was assumed that they would have ample personal experience to assist them in answering the survey questions. The questionnaire sought to determine how trust and utility perceptions were influenced by the privacy statements used on visited web sites.

128 complete samples were received by the web site. The survey was made available from 16 June 2008 to 3 July 2008 and distributed via www.surveymonkey.com/s.aspx?sm=Ft3rLXp2X2AT4G9nB35N_2bw_3d_3d. 154 complete and partial responses were received over the period. Twenty six responses were found to be incomplete and were subsequently filtered out from subsequent analysis.

Survey results:

Please see **Annex E** for detail on the questions and responses to the questionnaire.

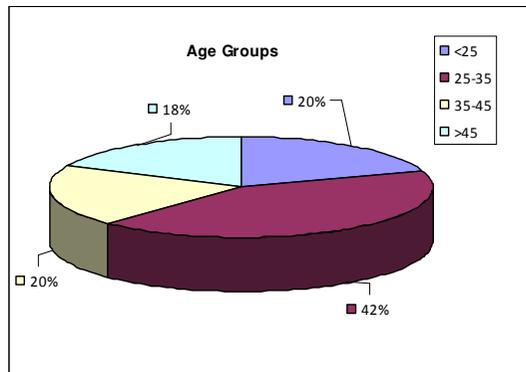
Sample Group Profile

Sample profile was well educated, mainly white, UK residents, and mostly professionals in higher income groups. The sample population contained mainly experienced Internet users who are on the net almost every day to shop, research, read news and to communicate.

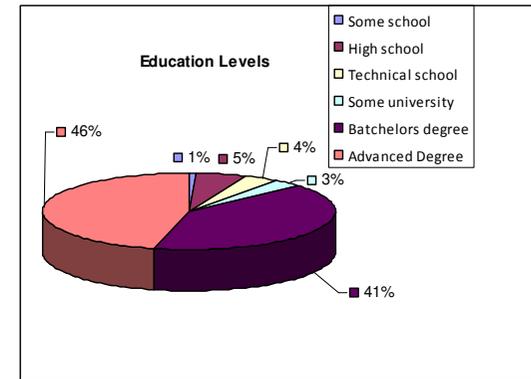
Questionnaire results: summary

Sample profile was well educated, mainly white, UK residents, mostly professionals in higher income groups.

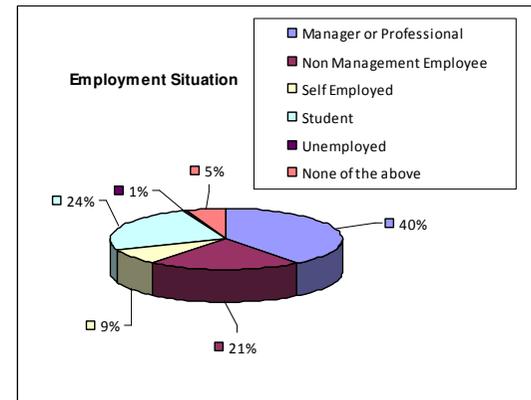
A majority of the respondents (62%) were between the ages of 25 and 35. Less than 20% of the sample was under 25 years old.



More than half (60%) were female. A majority were well educated with over 86% having a university degree; a high proportion of which (46%) had advanced degrees.



Higher income groups figured prominently, with approximately 50% and 30% earning more than £30K and £50K respectively per annum. Just under 69% of the group stated their ethnicity to be white. Less than 40% declared themselves to be managers or professionals, and just fewer than 25% declared themselves to currently be students.



Over three quarters (78%) are living in the UK. Over 65% of the population had been UK residents for over a year. Over two thirds (68.8%) of the sample know of someone who had been a victim of fraud.

The sample population was mainly experienced Internet users who are on the net almost every day to shop, research, read news and to communicate.

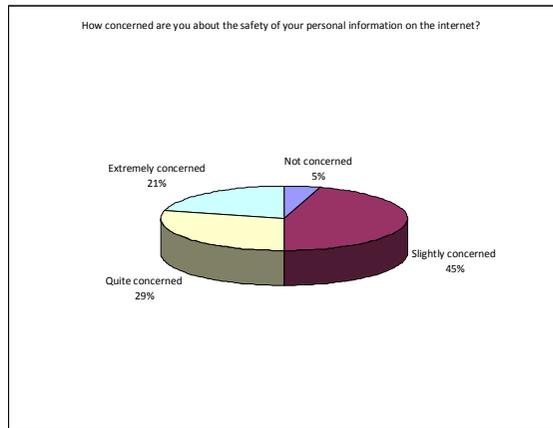
A very high proportion of the respondents (95%) have been using the internet for over five years. Almost all (98%) are on the internet at least part of every day. Above 87% of the population reported internet use for communications, news, research, shopping and work.

The following conclusions may be made regarding the four hypotheses of this research:

H1] Internet consumers are concerned about the privacy of their personal information

The sample reported varying degrees of concern regarding the security of their personal information. Most expressed at least some concern about the information on the internet.

Only 21% of the sample considered themselves to be extremely concerned about the safety of their personal information.¹⁴ Nevertheless, almost all the subjects (95%) reported having at least some information safety concerns. A higher proportion was bothered by internet profiling (70%) and by a feeling that too much of their personal information was stored on internet sites (77.3%).



Only 19% of the respondents felt that their personal information was protected by the law. The remainder stated that they felt either inadequately protected (36%) or were unsure what would be protected by law (45%).

Over 60% of the sample group stated that they would not provide personal data to untrustworthy sites, while over 20% of the remainder stated that they were unsure how they would act if they found themselves on a 'perceived' unsafe site. A large majority (80%) stated that financial gain would not induce them to use a site they perceived to be untrustworthy.

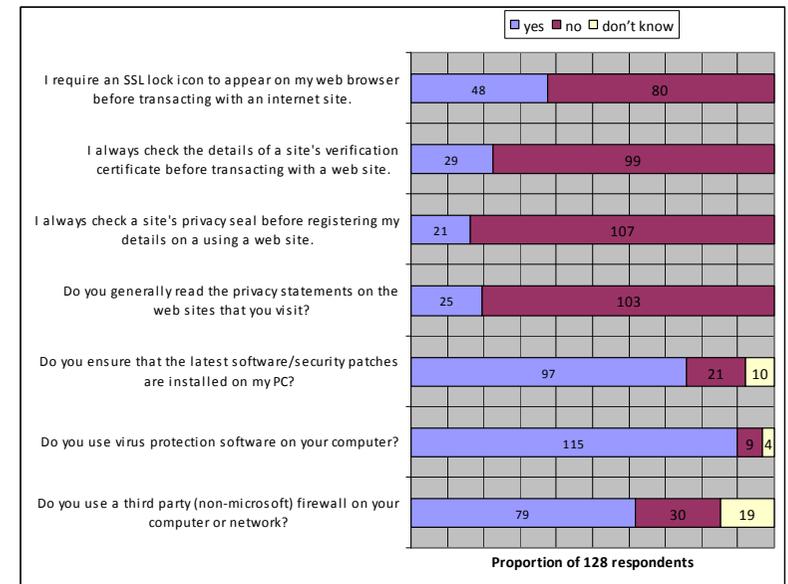
¹⁴ It should also be noted that 74% responded that they were *slightly to quite concerned* about the security of their personal information

While a large proportion of the sample considered themselves to medium to heavy users, they were aware of and employed varying levels of PC/internet security technologies.

Less than three quarters (74%) of the sample population perceived themselves to be medium to heavy internet users. The majority of this selection considered themselves heavy users.

A majority (51%) of the group feel that the internet is a safe environment, while 29% remain unsure. Many (89%) use virus protection, and three quarters ensure that the latest security patches are installed on their computers while only 60% use a non-Microsoft supplied firewall.

While most respondents were unaware of role of privacy seals (70%) or web digital certificates (56.3%), a large majority (88%) were aware of the role of privacy statements.



A large proportion of the sample (83.6%) reported not checking the details of web site privacy seals. A significant number also stated that they did not check the details of site verification certificates (77.3%). Moreover, 62% did not require proof of communication encryption (SSL icons) before transacting with the site.

H2] The reading of privacy statements does not establish consumer trust in the web site

Only a minority of the respondents stated that they read privacy statements in order to trust a web site

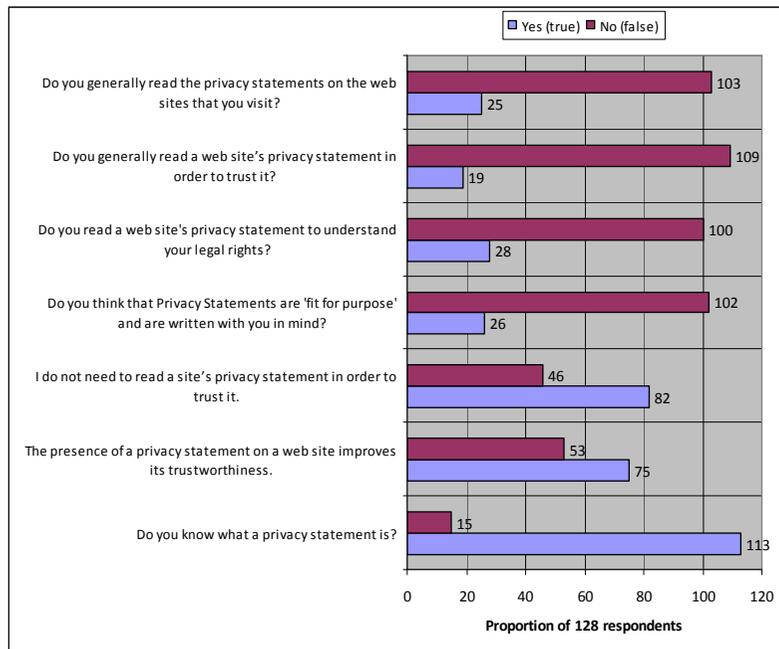
Only a minority (15%) of the sample group stated that they read privacy statements in order to trust a web site. Furthermore, a majority (64%) stated that they did not need to read privacy statements in order to trust a web site.

H3] Privacy statements are generally not read by internet consumers

Although there was awareness of the role of privacy statements, generally they were left unread.

Most (88%) reported that they were aware of the statements role. However, a similar majority (81%) stated that they generally did not read privacy statements. A large proportion (70.3%) stated that they rarely or never read the statements.

The two frequent cited reasons for not reading privacy statements was the lack of time (40%) or that they were hard to understand (40%). A clear majority (80%) stated that privacy statements were 'not fit for purpose' or written with them in mind.



H4] Among the many factors contributing to internet user trust, the company brand, the look and feel (performance) of the site are the strongest in engendering trust in the web site.

While the presence of a privacy statement was nevertheless helpful to build trust, other factors (brand, previous experience, and performance) were considered far more important.

A small majority (59%) felt that the presence of the privacy statement improves the trustworthiness of a web site. The group's responses suggest that the company brand (68%

ranked this attribute first), previous experience with the company (61% ranked this attribute second) and the look and feel of the site (42.5% ranked this attribute third) played the most important role in influencing trust.

Survey limitations and bias

The significance of the results of the survey is handicapped by a number of factors. Some of these limitations may have had a significant impact of the surveys findings. The validity of the survey may have been impacted by the following:

- 1] The small total sample size and short sampling period
- 2] The impact of small sub group sizes
 - 2.1] larger sub groups would better allow statistically stronger profiling of sub-group actions and preferences (men/women, ethics, salary)
- 3] Heavy bias in selection limits universal applicability
 - 3.1] mainly university educated
 - 3.2] large proportion higher income groups
 - 3.3] large proportion white race
 - 3.4] perceived heavy internet users – who are active on the net every day
 - 3.5] mainly UK responses
 - 3.6] mainly younger and more technologically savvy
- 4] Survey design issues
 - 4.1] inconsistent responses to check questions
 - 4.2] more testing required subject's responses to different questions
- 5] Sample achieved solely through social, university and professional contacts
- 6] Stronger statistical review of results are required in order to judge the validity of the survey conclusions

Further investigations in this area of study may wish to address these weaknesses in order to strengthen the validity of their conclusions.

Survey conclusions:

Despite the significant limitations of the survey, the data nevertheless provides an indication of the validity of the four hypotheses.

H1] Internet consumers are concerned about the privacy of their personal information

The sample reported varying degrees of concern regarding the security of their personal information. Most expressed at least some concern.

A large proportion of the sample considered themselves to be medium to heavy users; they are aware of and employ varying levels of computer and internet security.

H2] The reading of privacy statements does not establish consumer trust in the web site

Only minority of the respondents stated that they read privacy statements in order to trust a web site.

The presence of a privacy statement does increase trust in a web site somewhat.

H3] Privacy statements are generally not read by internet consumers

Although there is awareness of the role of privacy statements, they were generally not read.

H4] Among the many factors contributing to internet user trust, the company brand, the look and feel (performance) of the site are the strongest in engendering trust in the web site.

While the presence of a privacy statement was nevertheless helpful to build trust, other factors (brand, previous experience, and performance) were considered far more important.

Further detailed research, the design of which takes these limitations into account, should be considered in order to further clarify the position of privacy statements for web based trust.

6. Conclusion

This paper has summarised research in the literature, in the field (on the internet), focus groups and survey questionnaires in order to complete an investigation through 'methodological triangulation.'

The objective of the research was to examine the role that privacy statements play in establishing consumer confidence and trust in web sites. Much literature confirmed the importance of trust and the significance of privacy and data security for web consumers. Consumer control, privacy and data security seem to be key elements in the establishment of trust between transacting parties on the web. Companies have recognised the possible trust impact of perceived information asymmetry and have applied mitigation strategies to address it. The literature suggests that privacy statements, amongst other tools, are used to reduce users' perceived information risk. The subsequent review of sample UK web sites confirmed the literature's predominant view that privacy statements – despite being accessible – are too complex, long or technical to be understood by the average user. Their format is not congruent with the immediacy of the web medium. The web consumer's progress will be slowed considerably if comprehension of the site's privacy policy is a prerequisite for trust to exist. A majority of the focus group and questionnaire respondents were users of the top reference site (Amazon). They also confirmed that its statement was not deemed useful for immediate use or fit for purpose and therefore left it unread.

The focus group research suggested a users' perception that the internet was not a safe environment and that precautions needed to be taken. However, the loss of privacy was not a prominent concern and most statements were left unread. The groups confirmed the literature's view that brand, performance, look and feel were key determinants of trust generation for a web site. Regardless of awareness of web privacy risks, privacy statements were not deemed to be a core issue for the Focus Group participants.

The questionnaire respondents similarly reported at least some concern regarding their information security. With moderate levels of demonstrated concern, it made sense that the reading of privacy statements was not a priority or important for trust generation. Nevertheless, the survey did confirm the literature's view regarding the heuristic qualities of the statements. Their mere presence was reported to increase trust in web sites. Thus, the literature review, focus group and questionnaire results concur that while the presence of a privacy statements were helpful to build trust, other factors (brand, previous experience, and performance) were considerably more important.

Further research on the exact role of privacy statements in developing web based trust would be helpful to address the noted limitations of this paper. A larger sample (sub) group size would provide more meaningful profiling of the different socio-economic groups. Statistical analysis of the results would also be helpful to better indicate the validity of the finding presented here. Also, more detailed research on how users details are being harvested and assimilated would be useful. It would be useful to further detail how users protect different aspects of their internet activity. Furthermore, as there has been a suggestion that consumers apply real world strategies to determine risks on the internet, further study regarding how market forces are best able to offer redress for any opportunistic behaviour should be considered.

The literature suggested that users would have 'significant' concerns about the security of their information. The results of the paper's primary research that follows validate this privacy concern but only up to a point. It may well be that users may yet have to fully appreciate the extent to which internet technologies are able to assimilate their information. As this awareness grows, strategies and solutions may be implemented to mitigate the risks associated with loss of privacy. Privacy statements may become more significant 'risk relievers' and more helpful heuristic tools in the

future. However, group and questionnaire respondents clearly felt that privacy statements were not 'fit for purpose.' The inherent irony is that the reading of current privacy statements may provoke more questions and privacy uncertainty for web site users. If this is the case, the real use of a privacy statement may even be counter-productive to generating web-based trust.

Bibliography

- Andrews, L. & Boyle, M. (2008) *Consumers' accounts of perceived risk online and the influence of communication sources*, Qualitative Market Research: An International Journal, Vol. 11, No.1, pp. 59-75.
- Bouguettaya, A. & Eltoweissy, M. (2003) *Privacy on the Web: facts, challenges, and solutions*, Security & Privacy, IEEE, Vol. 1, Issue 6, pp. 40-49.
- Brunk, B. (2002) *Understanding the Privacy Space, First Monday; Peer-Reviewed Journal on the Internet, First Monday*, Vol. 7, No. 10, available on http://firstmonday.org/issues/issue7_10/brunk/index.html, sourced 10 March 2008, pages 2.
- Caldwell, H. (2000), *Building Trust to Develop Competitive advantage in E-Business Relationships*, Competitiveness Review, Vol. 10, No. 2, pp. 160-168.
- Castelfranchi, C. & Yao-Hua T. (2001) *The role of trust and deception in virtual societies*, System Sciences: Proceedings of the 34th Annual Hawaii International Conference on System Science, Vol. 6, No. 3, pp. 55-70.
- Chang Lee, K., Kang, O. & McKnight, D. (2007) *Transfer from Offline Trust to Key Online Perceptions: An Empirical Study*, Engineering Management - IEEE Transactions on Engineering Management, Vol. 54, Issue 4, pp. 729-741.
- Chau, P., Jen-Hwa Hu, P., Lee, B. & Au, A. (2007) *Examining customers' trust in online vendors and their dropout decisions: An empirical study*, Electronic Commerce Research and Applications, Elsevier Science Publishers, Vol. 6, Issue 2, pp. 171-182.
- Cheskin Research (2000), *Trust in the wired Americas*, published on 5 July 2000, available on <http://www.cheskin.com/think/studies/trust2.html>, accessed 10 Mar 2008
- Clarke, R. (1999) *Internet privacy concerns confirm the case for intervention*, Communications of the ACM, Vol. 42, Issue 2, pp. 60-67.
- Clay, K. & Strauss, R. (2000) *Trust, Risk and Electronic Commerce: Nineteenth Century Lessons for the Twenty-First Century*, National Tax Association, November 2000, pp. 234-247
- Cook, D. & Wenhong, L. (2003) *The Role of Third-Party Seals in Building Trust Online*, e-Service Journal, Vol. 2, No. 3, pp. 71-84.
- Cook, J. & Wall, T. (1980) *New work attitude measures of trust, organizational commitment, and personal need fulfilment*. Journal of Occupational Psychology, Vol. 5, pp. 39-52.
- Cranor, L. (1999) *Internet Privacy*, Communications of the ACM, Vol. 42, No. 2, pp. 29-31.
- Culnan, M. & Armstrong, P. (1999) *Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation*, Organization Science, Vol. 10, No. 1 (1999), pp. 104-115.
- De Boni, M. & Prigmore, M. (2002) *Cultural Aspects of Internet Privacy*, Proceedings of the UKAIS 2002 Conference, Leeds, UK.
- Doney, P., Cannon, J. & Mullen, M. (1998) *Understanding the influence of national culture on the development of trust*, The Academy of Management Review, Vol. 23, No. 3, pp. 601-20.
- Dörnyei, Z. (2003) *Questionnaires in Second Language Research: Construction, Administration, and Processing*, Mahwah, New Jersey: Lawrence Erlbaum Associates, pp. 9-14.

E-Marketer (2002), *Frequency of reading online privacy policies among US consumers*, EBrain Market Research/Consumer Electronics Association, May, eMarketer Database, available at: www.emarketer.com/products/chart.php?26317, accessed 10 February 2008.

E-Marketer (2003), *Amount of time US adults spend reading website privacy policies*, Harris Interactive/ Privacy Leadership Initiative, December 2001, eMarketer Database, available at: www.emarketer.com/products/chart.php?31594, accessed 10 February 2008.

Erlanger, L. (2004) *Should You Trust TrustE? PC Magazine*, published 17 February 2004, p. 59, available on www.pcmag.com/article2/0,1759,1463331,00.asp, accessed on 12 February 2008.

Ferrin, D., Kim, D., & Rao, H. (2008) *A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents*. *Decision Support Systems*, Vol. 44, pp. 544-564.

Flavián, C., Guinaliú, M. & Torres E. (2006) *How bricks-and-mortar attributes affect online banking adoption*, *International Journal of Bank Marketing*, Vol. 24, No. 6, pp. 406-423.

Flick, U. (2006) *An introduction to qualitative research*, 3rd Edition, London: Sage Publishing, pp. 128-9

Georgia Tech Research Group, Visualization and Usability Centre's GVU 7th WWW User Survey, June 1997

Henderson, B. (2005) *Opt In or Opt Out: Are These the Only Options?* *Journal of Internet Law*, Vol. 8, No. 11, pp. 11-18.

Hitwise, (2008) *Corporate Fact Sheet*, available on <http://www.hitwise.co.uk/who-we-are/corporate-fact-sheet.php>, undated, downloaded on 08 May 2008.

Holland, C. & Lockett, A. (1998) *Business trust and the formation of virtual organizations*. in *Proceedings of the 31st Annual Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computer Society, Vol. 6. pp. 143-177.

Hoffman, D., Novak, P. & Peralta, M. (1999) *Building Consumer Trust in Online Environments: The Case for Information Privacy*, *Communications of the ACM*, Vol. 42, No. 4, pp. 80-85.

IBM (1999), *IBM Multi-National Consumer Privacy Survey: A comprehensive and comparative look at consumers in the United States, Germany and United Kingdom and their attitudes toward privacy in everyday business transactions*. Dated February 7th 2000 via <http://www.ibm.com/services/e-business/privkshop.html>, sourced on 10 Feb 2008.

Jamal, K. (2005) *Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom*, *Journal of Accounting Research*, Vol. 43, pp. 73-96.

Jones, S., Wilikens, M., Morris, P. & Masera M. (2000) *Trust requirements in e-business*, *Communications of the ACM*, Vol. 43, No. 12, pp. 81-87.

Kai-Lung, H. & Hai Teo, T. & Sang-Yong, T., (2007) *The Value of Privacy Assurance: An Exploratory Field Experiment*, *MIS Quarterly*, Vol. 31 No. 1, pp. 19-33.

Lacoheea, H., Phippen, A. & Furnell, S. (2006) *Risk and restitution: Assessing how users establish online trust*, *Computers & Security*, Vol. 25, Issue 7, pp. 486-493.

Lauffer, R., & Wolfe, M. (1977) *Privacy as a concept and a social issue: A multidimensional development theory*. *Journal of Social Issues*, Vol. 33, No. 3, pp. 22-42.

Lee, M., Turban, E. (2001) *A trust model for consumer Internet shopping*, *International Journal of Electronic Commerce*, Vol. 6, No.1, pp. 75-91.

Luo, W. & Najdawi, M. (2004) *Trust-building measures: a review of consumer health portals*, *Communications of the ACM*, Vol. 47, No. 1, pp. 108-113.

Arcand, M., Nantel, J., Arles-Dufour, M. & Anne, V. (2007) *The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust*, *Online Information Review*, Vol. 31, No. 5, pp. 661-681.

Marsh, M. & Dabbour, A. (2000) *Putting Trust into e-Commerce - One Page at a Time*, *Proceedings of the Fourth International Conference on Autonomous Agents* (Agents' 2000), Barcelona, Spain, pp. 73-80.

May, W. & Sculli, D. (2002) *The role of trust, quality, value and risk in conducting e-business*, *Industrial Management & Data Systems*, Vol. 102, No. 9, pp. 503-512.

Mayer, R., Davis, J. & Schoorman, F. (1995) *An integrative model of organizational trust*. *Academy of Management Review*, Vol. 20, No. 3, pp. 709-734.

McCole, P. (2002) *The role of trust for electronic commerce in services*, *International Journal of Contemporary Hospitality Management*, Vol. 14, No. 2, pp. 81-87.

McKnight, D., Choudhury, V. & Kacmar, C. (2002) *Developing and Validating Trust Measures for e-Commerce: An Integrative Typology*, *INFORMATION SYSTEMS RESEARCH*, Vol. 13, No. 3, pp. 334-359.

Milne, G. & Culnan, M. (2004), *Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices*, *Journal of Interactive Marketing*, Vol. 18, No.3, pp. 15-29.

Mukherjee A. & Nath P. (2003) *A model of trust in online relationship banking*, *The International Journal of Bank Marketing*, Vol. 21, No. 1, pp. 5-15.

Mutz, D. (2005) *Social Trust and E-Commerce: Experimental Evidence for the Effects of Social Trust on Individuals, Economic Behavior*, *Public Opinion Quarterly*, Vol. 69, pp. 393-416.

Nagmetov, B. (2007) *Trust, as a main barrier in adoption to B2C E-Commerce*, Internet, 2007. ICI 2007. 3rd IEEE/IFIP International Conference in Central Asia on System Science, Publication Date: 26 - 28 Sept. 2007, pp. 1-5.

Nardi, P. (2003) *Doing survey research: a guide to quantitative methods*, 2nd ed., London: Pearson/Allyn and Bacon, 2006.

Nielsen Media Research (1997) *Nielsen Media Research/CommerceNet Internet Demographics Study*, from <http://www.nielsenmedia.com/commercenet/>, accessed 12 February 2008.

Olivero N. & Lunt, P. (2004) *Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control*, *Journal of Economic Psychology*, Vol. 25, Issue 2, pp. 243-262.

Ontario. Office of the Information and Privacy Commissioner and Microsoft Canada Inc, *An Internet Privacy Primer: Assume Nothing*, August 2001, available on <https://ozone.scholarsportal.info/bitstream/1873/6487/1/10297266.pdf>, downloaded 10 February 2008, screen 3.

Pollach, I., (2005) *A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent*, *Journal of Business Ethics*, Vol. 62, No. 3, pp. 221-235.

Poritz, J. (2007) *Who Searches the Searchers? Community Privacy in the Age of Monolithic Search Engines*, *The Information Society*, Vol. 23, Issue 5, pp. 383-389.

Ribak, R. & Turow, J. (2003) *Internet Power and Social Context: A Globalization Approach to Web Privacy Concerns*, *Journal of Broadcasting & Electronic Media*, Vol. 47, Issue 3, pp. 328-349.

Annexes

Rifon, N., LaRose, R., Choi, S. (2005) *Your privacy is sealed: effect of web privacy seals on trust and personal disclosures*, *Journal of Consumer Affairs*, Vol. 39, No. 2, pp. 339-62.

Robson, C. (2002) *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*, 2nd Edition, Wiley-Blackwell Publishing.

Roy M., Dewit O., & Aubert, B. (2001) *The Impact of Interface Usability on Trust in Web Retailers*, *Internet Research: Electronic Networking Applications and Policy*, Vol. 11, No. 5, pp. 388-398.

Schoder, D. & Haenlein, M. (2004) *The Relative Importance of Different Trust Constructs for Sellers in the Online World*, *Electronic Markets*, Vol. 14, No. 1, pp. 48-57.

Schoeman, D. (ed) 1984, *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.

Shah, V. (2005) *Web Site Privacy Policies*, *EDUCAUSE Review*, vol. 40, no. 3, pp. 70-71. Available from <http://connect.educause.edu/Library/EDUCAUSE+Review/WebSitePrivacyPolicies/40555?1208261867> accessed 10 February 2008.

Shaw, P. (2002) *Web-Site Privacy Checklist*, *Journal of Corporate Accounting & Finance*, Vol. 13, Issue 4, pp. 49-51.

Simpson, I. (1990), *How to interpret statistical data*, London: Library Association Publishing

Singer, M. (2004) *Improving Web Trust; Intel collaborates with MIT in a bid to build trust between a Web site and its customers*, On Internetnews.com, available on <http://www.internetnews.com/ec-news/article.php/340857>, accessed 10 March 2008, pages 2

Sisson, D. (2000) *ecommerce | Trust & Trustworthiness on philosophe.com A thoughtful approach to web site quality*, available on <http://www.philosophe.com/commerce/trust.html>, last accessed 15 April 2008.

Srinivasan, S. (2004) *Role of trust in e-business success*, *Information Management & Computer Security*, Vol. 12, No. 1, pp. 66-72.

Stewart, K. (2003) *Trust Transfer on the World Wide Web*, *Organization Science*, vol. 14, no. 1, pp. 5-17.

Yao-Hua, T. & Theon, W. (2001) *Towards a Generic Model of Trust for Electronic Commerce*, *International Journal of Electronic Commerce*, Vol. 5, No. 2, pp. 61-74.

Thompson, T. & Liu, J. (2007) *Consumer trust in e-commerce in the United States, Singapore and China*, *Omega*, Exeter: Elsevier, Vol. 35, No. 1, pp. 22-38.

Tsai, J., Egelman, S., Cranor, L. & Acquisti, A. (2007) *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, Carnegie Mellon University, The 6th Workshop on the Economics of Information Security (WEIS), June 2007, accessed via <http://weis2007.econinfocsec.org/papers/57.pdf>, 22 pages, downloaded ? March 2008.

Williamson, O. (1975) *Markets and Hierarchies: Analysis and Antitrust Implications*, New York: Free Press.

Wingreen, S. & Baglione, S. (2005) *Untangling the Antecedents and Covariates of E-Commerce Trust: Institutional Trust vs. Knowledge-Based Trust*, *ELECTRONIC MARKETS*, Vol. 15, No. 3.

Xu, K. & Koh, A. (2004) *Comparison of Online Trust Building Factors*, *Journal of the Association for Information Systems*, Vol. 5, No. 10, pp.392-420.

Annex A – Web site rankings (February-March 2008)



FEBRUARY 2008

Nov 07		
1	= 1	Amazon UK www.amazon.co.uk
2	▲ 3	Argos www.argos.co.uk
3	▼ 2	Play.com play.com
4	▲ 5	Apple Computer www.apple.com
5	▼ 4	Tesco.com www.tesco.com
6	▲ 7	Amazon.com www.amazon.com
7	▲ 13	Thomson Holidays www.thomson.co.uk
8	▲ 9	Tesco Direct direct.tesco.com
9	▼ 6	Dell EMEA www.euro.dell.com
10	▲ 12	Expedia.co.uk www.expedia.co.uk
11	▲ 19	easyJet www.easyjet.co.uk
12	▼ 8	Marks & Spencer www.marksandspencer.com
13	▼ 10	Next www.next.co.uk
14	▲ 15	Currys www.currys.co.uk
15	▼ 14	lastminute.com www.lastminute.com
16	▼ 11	HMV.co.uk www.hmv.co.uk
17	▲ 18	RyanAir www.ryanair.com
18	▲ 20	British Airways www.britishairways.com
19	▼ 17	John Lewis www.johnlewis.com
20	▲ 21	Comet UK www.comet.co.uk
21	▲ 24	PC World www.pcworld.co.uk
22	▼ 16	Ticketmaster UK www.ticketmaster.co.uk
23	▲ 48	Thomas Cook www.thomascook.com
24	▲ 30	Ebuyer www.ebuyer.com
25	▼ 23	GAME shop.game.net
26	= 26	O2 Shop shop.o2.co.uk
27	▲ 29	ASOS www.asos.com
28	= 28	Debenhams www.debenhams.com
29	▲ 32	B&Q www.diy.com
30	▲ 34	Littlewoods www.littlewoods.com
31	▼ 27	Symantec Store www.symantecstore.com
32	▲ 33	The Orange Shop www.diy.com
33	▲ 36	ASDA www.asda.co.uk
34	▼ 22	Woolworths UK www.woolworths.co.uk
35	▼ 25	Boots www.boots.com
36	▲ 39	Odeon Cinemas www.odeon.co.uk
37	NEW	LOVE FILM www.lovefilm.com
38	▲ 43	IKEA www.ikea.com
39	▲ 40	Screwfix Direct www.screwfix.com
40	▼ 35	QVCUK.com www.qvcuk.com
41	▼ 38	Topshop www.topshop.co.uk
42	▼ 37	Carphone Warehouse www.carphonewarehouse.com
43	▲ 45	Sainsbury's www.sainsburys.com
44	▲ 50	Thomsonfly www.thomsonfly.com
45	▼ 41	HP www.hp.com
46	BACK	Flybe.com www.flybe.com
47	BACK	Maplin Electronics www.maplin.co.uk
48	▼ 46	Dixons www.dixons.co.uk
49	▼ 47	Apple iTunes www.apple.com/itunes
50	▼ 42	River Island www.riverisland.com

The IMRG-Hitwise Hot Shops List of the top 50 UK e-retailers* is the key indicator of online merchant performance. The List is published quarterly and tracks popularity, as indicated by visits, of those selling goods and services within the IMRG Capgemini Index Classification**. This List is based on January 2008 data.

* The IMRG-Hitwise Hot Shops List excludes eBay and price comparison / aggregator websites such as Kelcoo and Froogle.

** IMRG Capgemini Index Classification: Beer / wine / spirits; Books; CDs / tapes / records; Clothing / footwear / accessories; Computer hardware / peripherals / consumables; Consumer electronics; Digital downloads (e.g. music, software); Flowers; Food, beverages and household supplies; Furniture; Garden / DIY; Health and beauty; Home appliances (e.g. washing machines); Household goods (e.g. kitchenware, bedding); Jewellery / watches; Software; Sporting goods; Tickets (e.g. cinema, theatre, events); Toys; Travel (e.g. flights, holidays, hotels, car hire); Video games; Videos / DVDs

© IMRG 2008 www.imrg.org +44 (0) 7000 46 46 74

Source: <http://www.imrg.org/ItemList.aspx?cig=Infotems&cid=is&language=en-GB>

Annex B – An overview of privacy statement attributes of three top UK sites

No.1 – Amazon.co.uk (See document in Annex B/1)

Privacy notice position: small type link at bottom of long home page (requires long scroll down home and other pages)

Privacy notice size, length and detail: Long and high (10 screens)

Practices: Shares and retains profiles, transfers data outside the EEA, uses [U.S. Safe Harbour](#) programme

Data Collection/Processing: Some described (cookies, IP tracking, e-mail tracking, java script, web beacons, and other 'technologies', and information from other sources). Not clear what Amazon does with the information, though data is shared with 3rd parties and sold along with divested business units. Host 3rd party advertisements (not subject to or controlled by this privacy notice). These 3rd party advertisements 'may' be used by 3rd parties to profile the users. User blocking of 'cookies' tracking will mean that the functionality of the web site will be impaired.

Data Retention: not specified, unclear

Openness and transparency: not clear how information will be used, very long document that is unlikely to be read in detail. For example, readers will need to spend much time further researching the privacy statements of the 3rd party advertiser to fully understand the privacy implications of their action on the web site.

Language/Clarity: use of conditional (such as, 'may', 'might', 'whenever') found throughout text

Assessment: Generally aware of privacy rights and law, but vague and unclear in certain areas

No.2 – Argos.co.uk (See document in Annex B/2)

Privacy notice position: type link at bottom of long home page (requires scroll down home and other pages)

Privacy notice size, length and detail: shorter – less than half the length of amazon.co.uk, length, less detail, but still 3 screens long.

Practices: Argos provides data protection as that required under applicable UK legislation

Data Collection/Processing: Few described (cookies, IP tracking and information from other sources), information shared with 3rd parties, can transfer data outside the EEA, user blocking of 'cookies' tracking will mean that the functionality of the web site will be impaired.

Data Retention: not specified, unclear

Openness and transparency: vague, information will be used for assessment and analysis

Language/Clarity: use of conditional (such as, 'or otherwise', 'some', 'may', 'might', 'whenever') found throughout text

Assessment: Generally aware of privacy rights and law, vague and short on detail.

No.3 – Play.com (See document in Annex B/3)

Privacy notice position: small type link at bottom of long home page (requires long scroll down home and other pages).

Privacy notice size, length and detail: shorter than that of Amazon.co.uk, but still 4 screens long.

Practices: protection as required under Jersey and Luxembourg law. Assumption is that EU data protection laws apply. It is unclear how the company's international group structure may affect its data protection issue.

Data Collection/Processing: Few described (cookies, IP tracking, clickstream, and information from other sources) information shared with 3rd parties, may be sold off along with divested business units, will sell data if allowed by law.

Data Retention: not specified, unclear

Openness and transparency: in part vague, use of deceptive language to reduce perception of threat (for example, "We will not sell, distribute or disclose information about you or your personal usage of the Site without your express consent or unless required or permitted to do so by law".)

Language/Clarity: use of conditional (such as, 'some', 'may', 'whenever') found throughout text.

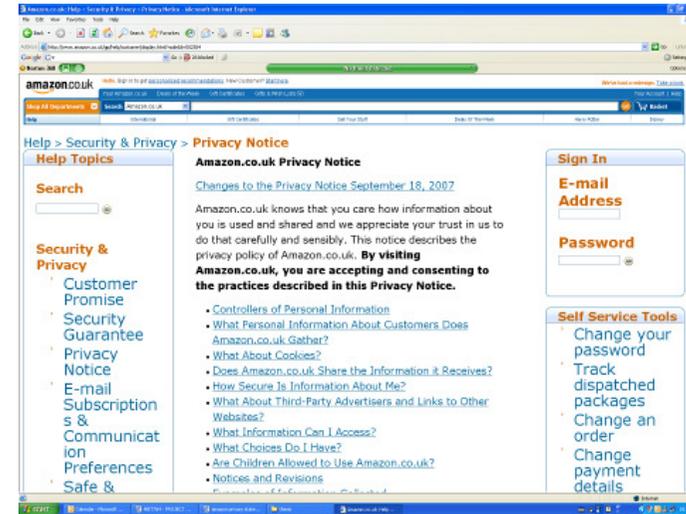
Assessment: Generally compliant regarding the law, but similarly vague and short on detail in areas. Language used attempts to hide the potentially extensive use of personal data provided to the site.

Annex B/1 – Argos.com Privacy Statement



Amazon.co.uk Privacy Notice

[Changes to the Privacy Notice September 18, 2007](#)



[Changes to the Privacy Notice September 18, 2007](#)

Amazon.co.uk knows that you care how information about you is used and shared and we appreciate your trust in us to do that carefully and sensibly. This notice describes the privacy policy of Amazon.co.uk. **By visiting Amazon.co.uk, you are accepting and consenting to the practices described in this Privacy Notice.**

- [Controllers of Personal Information](#)
- [What Personal Information About Customers Does Amazon.co.uk Gather?](#)
- [What About Cookies?](#)
- [Does Amazon.co.uk Share the Information it Receives?](#)
- [How Secure Is Information About Me?](#)
- [What About Third-Party Advertisers and Links to Other Websites?](#)
- [What Information Can I Access?](#)
- [What Choices Do I Have?](#)
- [Are Children Allowed to Use Amazon.co.uk?](#)
- [Notices and Revisions](#)
- [Examples of Information Collected](#)

Controllers of Personal Information

Any personal information provided to or to be gathered by Amazon.co.uk is controlled primarily by Amazon EU Sarl and Amazon Services Europe Sarl, the data controllers, both at 5, Rue Plaetis L-2338, Luxembourg and secondarily by Amazon.co.uk Ltd of Patriot Court, 1-9 The Grove, Slough, Berkshire, England SL1 1QP UK, the data processor.

Amazon.com, Inc. and its controlled US subsidiaries are **participants in the Safe Harbour programme developed by the US Department of Commerce and the European Union.** These Amazon Group companies have certified that they adhere to the Safe Harbour Privacy Principles agreed upon by the US and the EU. For more information about the Safe Harbour and to view these Amazon Group companies' certification, visit the [U.S. Department of](#)

Privacy statement key coding references

Section with personal data relevance

Section with personal data significance

Key words

[may share transfer sell](#)

[might cookie some](#)

[third parties law](#)

[accept IP address](#)

[control](#)

Section with personal data relevance

Section with personal data significance

Key words

[may share transfer sell](#)

[might cookie some](#)

[third parties law](#)

[accept IP address](#)

[control](#)

Commerce's [Safe Harbour](#) website. If you would like to contact Amazon directly about the Safe Harbour programme, please send an e-mail to safeharbor@amazon.com.

[Back to top](#)

What Personal Information about Customers Does Amazon.co.uk Gather?

The information we learn from customers helps us personalise and continually improve your shopping experience at Amazon.co.uk. We use the information to handle orders, deliver products and services, process payments, communicate with you about orders, products, services and promotional offers, update our records and generally maintain your accounts with us, display content such as wish lists and customer reviews and recommend merchandise and services that **might** be of interest to you. We also use this information to improve our store and platform, prevent or detect fraud or abuses of our website **and enable third parties to carry out technical, logistical or other functions on our behalf**.

Section Comment: **third party have access to the user data and profiles. language unclear with the words 'might'.**

Here are the types of information we gather.

- **Information You Give Us:** we receive and store any information you enter on our website or give us in any other way. [Click here](#) to see examples of what we collect. You can choose not to provide certain information but then you **might** not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customising future shopping for you, improving our stores, and communicating with you.
- **Automatic Information:** we receive and store certain types of information whenever you interact with us. For example, like many websites, we use "cookies" and **we obtain certain types of information when your Web browser accesses Amazon.co.uk. A number of companies offer utilities designed to help you visit websites anonymously.** Although we will not be able to provide you with a personalised experience at Amazon.co.uk if we cannot recognise you, we want you to be aware that these tools exist.
- **E-mail Communications:** to help us make e-mails more useful and interesting, we often receive a confirmation when you open e-mail from Amazon.co.uk if your computer supports such capabilities. We also **compare our customer list to lists received from other companies in an effort to avoid sending unnecessary messages to our customers.** If you do not want to receive e-mail or other mail from us, please adjust your [Customer Communication Preferences](#).
- **Information from Other Sources:** we **might** receive information about you from other sources and add it to our account information.

Section Comment: **Amazon uses cookie to profile users. Users may block these cookies in order to be anonymous. Without cookies, we are told later, you cannot make purchases (add items into a shopping cart). Language unclear with the word 'might'.**

[Back to top](#)

What About Cookies?

- **Cookies** are alphanumeric identifiers that we **transfer** to your computer's hard drive through your Web browser to **enable our systems to recognise your browser** and to provide features such as [1-Click](#) purchasing, [New for You](#), personalised greetings and storage of items in your Shopping Basket between visits.
- The Help menu on the menu bar of most browsers will **tell you how to prevent your browser** from accepting new **cookies**, how to have the browser notify you when you receive a new **cookie** and how to disable **cookies** altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash **cookies**, by changing the add-on's settings or visiting the website of its manufacturer. However, because **cookies** allow you to take advantage of some of Amazon.co.uk's essential features, we recommend that you leave them turned on. **For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping cart, proceed to Checkout, or use any Amazon.co.uk products and services that require you to sign in.**

Section Comment: **Without cookies one is unable to make purchases (add items into a shopping cart).**

- If you do leave **cookies** turned on, be sure to sign off when you finish using a shared computer. [Click here](#) for more information on how to sign off.

[Back to top](#)

Does Amazon.co.uk **share** the Information it receives?

Information about our customers is an important part of our business and we are not in the business of selling it to others. **Amazon.co.uk shares customer information only as described below** and with Amazon.com, Inc. and the subsidiaries which Amazon.com, Inc., controls and that are **either subject to this Privacy Notice or follow practices at least as protective** as those described in this Privacy Notice.

- **Affiliated Businesses We Do Not Control:** We work closely with our affiliated businesses. In some cases, such as Marketplace, zShops and Auctions sellers, these businesses operate stores at Amazon.co.uk or **sell** offerings to you at Amazon.co.uk. In other cases, we operate stores, provide services or **sell** product lines jointly with or on behalf of these businesses. [Click here](#) for some examples of co-branded and joint offerings. You can tell when a third party is involved in your transactions **and we share customer information related to those transactions with that third party.**
- **Third Party Service Providers:** We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analysing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments and providing customer service. **They have access to personal information needed to perform their functions, but may not use it for other purposes. Further, they must process the personal information in accordance with this Privacy Notice and as permitted by the UK's Data Protection Act.**
- **Promotional Offers:** Sometimes we send offers to selected groups of Amazon.co.uk customers on behalf of other businesses. When we do this, we do not give that business your name and address. If you do not want to receive such offers, please adjust your [Customer Communication Preferences](#).
- **Business Transfers:** As we continue to develop our business, we **might sell** or buy stores, subsidiaries or business units. **In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise).** Also, **in the unlikely event that Amazon.com, Inc. or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.**

Section Comment: **"might sell" is unclear; the users' personal data is considered an asset of the company and will be transferred. Data may be sold to affiliates that Amazon does not control. Data is protected by UK/EU law. Personal Data is an asset of the company and will be sold if the company is transferred to new owners. language unclear with the words 'may' and 'might'.**

- **Protection of Amazon.co.uk and Others:** We release account and other personal information when we believe release is appropriate to comply with the law; enforce or apply our Conditions of Use and other agreements; or protect the rights, property or safety of Amazon.co.uk, our users or others. This includes exchanging information with other companies and organisations for fraud protection and credit risk reduction. Obviously, however, this does not include selling, renting, sharing or otherwise disclosing personally identifiable information from customers for commercial purposes in a way that is contrary to the commitments made in this Privacy Notice.
- **With your consent:** other than as set out above, you will receive notice when information about you **might** go to third parties and you will have an opportunity to choose not to **share** the information.

Whenever we transfer personal information to countries outside of the European Economic Area in the course of sharing information as set out above, we will ensure that the information is transferred in accordance with this Privacy Notice and as permitted by the applicable laws on data protection.

Section Comment: **Language more than suggests that the information will go to third parties and the EEA. The user is protected by the law. Language unclear with the word 'might' and 'whenever'.**

[Back to top](#)

How Secure Is Information About Me?

- We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input.
- We reveal only the last five digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.

- We maintain physical, electronic and procedural safeguards in connection with the collection, storage and disclosure of personally identifiable customer information. Our security procedures mean that we [may](#) occasionally request proof of identity before we disclose personal information to you.
- It is important for you to protect against unauthorised access to your password and to your computer. Be sure to sign off when you finish using a shared computer. [Click here](#) for more information on how to sign off.

[Back to top](#)

What About Third-Party Advertisers and Links to Other Websites?

Our site [may](#) include third-party advertising and links to other websites. We do not provide any personally identifiable customer information to these advertisers or third-party websites. [Click here](#) for some examples as well as information on [how to contact these companies to learn more or opt-out of their information collection practices](#).

These [third-party websites and advertisers](#), or Internet advertising companies working on their behalf, sometimes use technology to send (or "serve") the advertisements that appear on our website directly to your browser. They automatically receive your IP address when this happens. They [also use cookies](#), JavaScript, web beacons (also known as action tags or single-pixel gifs), and other technologies to measure the effectiveness of their ads and to personalise advertising content. We do not have access to or control over [cookies](#) or other features that they [use](#), and the information practices of these advertisers and third-party websites are not covered by this Privacy Notice. Please contact them directly for more information about their privacy practices. In addition, the [Network Advertising Initiative](#) offers useful information about Internet advertising companies (also called "ad networks" or "network advertisers"), including information about [how to opt-out of their information collection](#).

Section comment: Many technologies in place to track and analyse users, these are used on the web site by third parties who are not subject to the conditions of this privacy notice. User is required to conduct further research to understand what policies apply. Language unclear with the words 'may'.

Amazon.co.uk also displays targeted advertising based on personal information about users. Although Amazon.co.uk does not provide any personal information to advertisers, [advertisers \(including ad-serving companies\)](#) [may](#) assume that users who interact with or click on a targeted advertisement meet the targeting criteria used to display the ad (for example, users in the United Kingdom who like classical music).

Section Comment: Unclear at best, deceptive at worst. The language means that 3rd party advertisements will lead to profiling and targeted communications, language unclear with the words, 'may',

[Back to top](#)

What Information Can I Access?

Amazon.co.uk gives you access to a broad range of information about your account and your interactions with Amazon.co.uk for the limited purpose of viewing and, in certain cases, updating that information. [Click here](#) to see some examples. This list will change as our website evolves.

[Back to top](#)

What Choices Do I Have?

- As discussed above, you can always choose not to provide information, even though it [might](#) be needed to make a purchase or to take advantage of such Amazon.co.uk features as your [About You](#) area, [Wish Lists](#) and [Customer Reviews](#).
- You can add or update certain information on pages such as those listed in [Which Information Can I Access?](#) When you update information, we usually keep a copy of the previous version for our records.
- If you do not want to receive e-mail or other mail from us, please adjust your [Customer Communication Preferences](#). (If you do not want to receive [Conditions of Use](#) and other legal notices from us, such as this Privacy Notice, those notices will still govern your use of Amazon.co.uk and orders placed with Amazon.co.uk, and it is your responsibility to review them for changes.)
- The Help menu on the menu bar of most browsers will tell you how to prevent your browser from accepting new [cookies](#), how to have the browser notify you when you receive a new [cookie](#) and how to disable [cookies](#) altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash [cookies](#), by changing the add-on's settings or visiting the website of its manufacturer. However, because [cookies](#) allow you to take advantage of some of Amazon.co.uk's essential features, we recommend that you leave them turned

on. For instance, if you block or otherwise reject our [cookies](#), you will not be able to add items to your [Shopping Cart](#), proceed to [Checkout](#), or use any Amazon.co.uk products and services that require you to [Sign in](#).

Section Comment: If you block Amazon's cookies that it is unlikely that you will be able to make a purchase for the site. User must enable cookies to use the site, language unclear with the words, 'might'

[Back to top](#)

Are Children Allowed to Use Amazon.co.uk?

Amazon.co.uk does not [sell](#) products for purchase by children. We [sell](#) children's products for purchase by adults. If you are under 18, you [may](#) use Amazon.co.uk only with the involvement of a parent or guardian.

[Back to top](#)

Notices and Revisions

If you have any concern about privacy at Amazon.co.uk, please [e-mail us](#) a thorough description and we will try to resolve the issue for you.

Our business changes constantly and our Privacy Notice and the [Conditions of Use](#) will change also. We [may](#) e-mail periodic reminders of our notices and conditions, unless you have instructed us not to, but you should check our website frequently to see recent changes. Unless stated otherwise, our current Privacy Notice applies to all information that we have about you and your account. We stand behind the promises we make, however, and will never materially change our policies and practices to make them less protective of customer information collected in the past without the consent of affected customers.

Related Practices and Information:

- [Conditions of Use](#)
- [Amazon.co.uk Marketplace, Auctions & zShops Participation Agreement](#)
- [Amazon.co.uk Marketplace, Auctions and zShops Community Rules](#)
- [Help Desk](#)

[Back to top](#)

Examples of Information Collected

Information You Give Us

You provide most such information when you search, buy, bid, post, participate in a contest or questionnaire or communicate with customer service. For example, you provide information when you: search for a product; place an order through Amazon.co.uk or one of our third-party sellers; make an Auction bid or purchase; provide information in [Your Account](#) (and you [might](#) have more than one if you have used more than one e-mail address when shopping with us) or your [About You](#) area; communicate with us by phone, e-mail or otherwise; complete a questionnaire or a contest entry form; compile [Wish Lists](#) or other gift registries, provide and rate [Reviews](#); and employ other personal notification services such as such as Available to Order Notifications. As a result of those actions, you [might](#) supply us with such information as: your name; address and phone number; credit card information; people to whom purchases have been shipped (including addresses and phone numbers); people (with addresses and phone numbers) listed in [1-Click](#) settings; content of reviews and e-mails to us; the personal description in your [About You](#) area; and financial information.

Section Comment: Amazon collects and retains all personal information, language unclear with words 'might' and 'may'.

Automatic Information

Examples of the information we collect and analyse include: the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information such as browser type and version; operating system and platform; purchase history, which we sometimes aggregate with similar information from other customers to create features such as Top Sellers; the full Uniform Resource

Locators (URL clickstream to, through and from our website (including date and time); [cookie](#) number; products you viewed or searched for; zShops you visited; your Auction history; and any phone number used to call our customer service number. We [may](#) also use browser data such as [cookies](#), Flash [cookies](#) (also known as Flash Local Shared Objects), or similar data on certain parts of our website for fraud prevention and other purposes. During some visits we [may](#) use software tools such as JavaScript to measure and collect session information, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.

Section Comment: Amazon uses many technologies to assist with the profiling of their audience, language unclear with the use of the word 'may'.

Information from Other Sources

Examples of information we receive from other sources include: updated delivery and address information from our carriers or other third parties, which we use to correct our records and deliver your next purchase or communication more easily; [account information](#), [purchase or redemption information](#) and [page-view information](#) from some merchants with which we operate co-branded businesses or for which we provide technical, fulfillment, advertising or other services; search term and search result information from some searches conducted through the Web search features offered by Amazon Group Companies, Alexa Internet and A9; search results and links, including [paid listings](#) (such as Sponsored Links from Overture); and [credit history information from credit bureaus](#), which we use to help prevent and detect fraud and to offer certain credit or financial services to some customers.

Section Comment: Does combine with data from 3rd parties, use examples to make it seem reasonable, but does involve the combination of profiles

Information You Can Access

[Examples of information you can access easily at Amazon.co.uk include:](#) up-to-date information regarding recent orders; personally identifiable information (including name, e-mail, password, communications preferences, address book and 1-Click settings); payment settings (including credit-card information and gift certificate, gift card and cheque balances); e-mail notification settings (including Alerts, Available to Order notifications, Delivers, New for You and newsletters); recommendations (including recent product-view history, prior-order history and Favourites); Wish Lists, Auctions, zShops and Marketplace seller accounts and your About You area (including your product reviews, requests and recommendations, your Listmania lists and your personal profile).

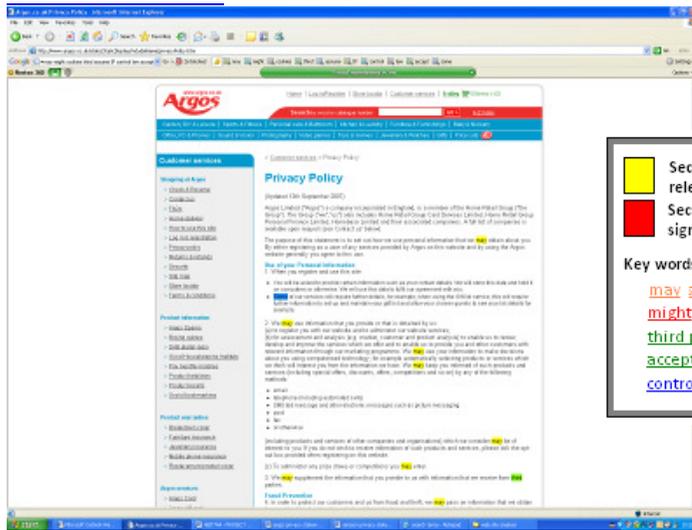
Section Comment: Does not say what you cannot access – in particular the third party information or profiling information

Co-Branded and Joint Offerings

In the future we [may](#) offer joint or co-branded products and services such as those offered on Amazon.com's US website for Target, Hotwire, Gap, Nordstrom, Office Depot and Virginmega.com.

Section Comment: "may" is unclear and also creates uncertainty regarding future policy

Annex B/2 – Argos.com Privacy Statement



Privacy Policy

(Updated 12th September 2007)

Argos Limited ("Argos") a company incorporated in England, is a member of the Home Retail Group ("the Group"). The Group ("we", "us") also includes Home Retail Group Card Services Limited, Home Retail Group Personal Finance Limited, Homebase Limited and their associated companies. A full list of companies is available upon request (see 'contact us' below).

The purpose of this statement is to set out how we use personal information that we **may** obtain about you. By either registering as a user of any services provided by Argos on this website and by using the Argos website generally you agree to this use.

Use of your Personal Information

1. When you register and use this site:

- You will be asked to provide certain information such as your contact 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 for example.

2. We **may** use information that you provide or that is obtained by us:

- to register you with our website and to administer our website services;
- for assessment and analysis (e.g. market, customer and product analysis) to enable us to review, develop and improve the services which we offer and to enable us to provide you and other customers with relevant information through our marketing programmes. We **may** use your information to make decisions about you using computerised technology, for example automatically selecting products or services which we think will interest you from the information we have. We **may** keep you informed of such products and services (including special offers, discounts, offers, competitions and so on) by any of the following methods:

- email
- telephone (including automated calls)

- SMS text message and other electronic messages such as picture messaging
- post
- fax

or otherwise

(including products and services of other companies and organisations) which we consider **may** be of interest to you. If you do not wish to receive information of such products and services, please tick the opt-out box provided when registering on this website.

(c) To administer any prize draws or competitions you **may** enter.

3. We **may** supplement the information that you provide to us with information that we receive from **third parties**.

Section Comment: vague statement with words 'or otherwise', 'may' and 'some', will combine data from 3rd parties, may use information to make decisions about the user, may contact you by any method (for example, 'or otherwise');

Fraud Prevention

4. In order to protect our customers and us from fraud and theft, we **may** pass on information that we obtain from making identity checks and other information in our customer records, including how you conduct your account, to other Group companies, other retailers and to financial and other organisations (including **law** enforcement agencies) involved in fraud prevention and detection, to use in the same way.

Section Comment: vague statement with word 'may'

Disclosure of Your Information

5. We **may** give information about you to the following, who **may** use it for the same purposes as set out above:

- to other companies in the Group;
- to employees and agents of the Group to administer any accounts, products and services provided to you by the Group now or in the future;
- agents who (on our behalf) profile your data** so that we **may** tailor the goods/services we offer to your specific needs;
- to other organisations for the administration of prize draws or competitions.
- to **anyone to whom we transfer it**, **may** transfer our rights and duties under our agreement with you;
- if we have a duty to do so or if the **law** allows us to do so.

6. In carrying out the activities specified in this section, we **may** transfer data to reputable companies outside the European Economic Area. We take steps to ensure that your information will be afforded the same level of protection as that required of us under applicable UK data protection legislation.

7. If you are purchasing a television from us, please note that the Wireless Telegraphy Act (1967) requires us to notify the TV Licensing Authority within 28 days of each transaction, giving full details of the buyer.

Section Comment: can provide personal data to third parties, or the company's agents, under protection of the law, can transfer the data outside the EU (and EU Legal protection)

Cookies

8. New technologies are emerging on the Internet that help us to deliver customised visitor experiences. In particular, there is a technology called "**cookies**" which **may** be used by us to provide you with, for example, customised information from our website. A cookie is an element of data that a website can send to your browser, which **may** then store it on your system. **Cookies** allow us to understand who has seen which pages and advertisements, to determine how frequently particular pages are visited and to determine the most popular areas of our website. Depending on the type of cookie we use, **cookies** also allow us to make our website more user friendly, for example, permanent **cookies** allow us to save your password so that you do not have to re-enter it every time you visit our website. If you wish, you can usually adjust your browser so that your computer does not **accept** cookies. If you do this, you will still be able to browse around the site but the functions that allow you to add items to your trolley, set up a new account or access an existing account will not be available. Alternatively you can adjust your browser to tell you when a website tries to put a cookie on your computer. How you adjust your browser to stop it accepting **cookies** or to notify you of them, will depend on the type of internet browser programme your computer uses. If your computer uses Microsoft Internet Explorer or Netscape Navigator, you will need to follow these instructions after clicking onto this link www.aboutcookies.org (Argos.co.uk is not responsible for the content of external websites. This link will open a new window.) Go to the heading "Manage **Cookies**". Click onto the option you prefer, either stopping **cookies** being installed, or notifying you of them. From the list provided, click onto the programme which your computer uses. If this is not shown on the list, click on the "help" heading on the bar at the top of this page, search for information on "**cookies**" - an explanation of how to delete **cookies** will appear, then follow these instructions.

9. Please remember, **cookies** do not contain confidential information such as your home address, telephone number or credit card details. We do not exchange **cookies** with any **third** party websites or external data suppliers.

10. Your browser also generates other information, including which language the site is displayed in, and your Internet Protocol address ("IP address"). An **IP** address is a set of numbers which is assigned to your computer during a browsing session whenever you log on to the Internet via your internet service provider or your network (if you access the Internet from, for example, a computer at work). Your **IP** address is automatically logged by our servers and used to collect traffic data about visitors to our websites. We do not use your **IP** address to identify you personally.

11. We only keep **cookies** for the duration of your visit to our website, except where you save your login name as referred to above.

Section Comment: Section Comment: vague statement with the word 'may', functionally of the web site will be degraded if cookies are disabled. User IP addresses are logged.

Security

12. We endeavour to take all reasonable steps to protect your personal information. However, we cannot guarantee the security of any data you disclose online. You **accept** the inherent security risks of providing information and dealing online over the Internet and will not hold us responsible for any breach of security unless this is due to our negligence or wilful default.

13. For further information about the steps we take to protect your information and make online shopping as secure as possible, please see information on [Secure online shopping](#).

Section Comment: Do not guarantee security of personal data disclosed. User accepts risks of providing information.

General

14. You have the right to see personal data (as defined in the Data Protection Act) that we keep about you, upon receipt of a written request and payment of a fee. If you are concerned that any of the information we hold on you is incorrect please contact us (see details below).

15. Please be aware that our site **may** link to other websites which **may** be accessed through our site. We are not responsible for the data policies or procedures or the content of these linked websites.

How can I get my name removed from the argos.co.uk mailing list?

If you want to be removed from our mailing list, please send an email to reply@argos.co.uk with the word 'remove' in the subject line and the email address that you wish to be removed within the email. Please note that it **may** take up to 28 days to action your request. In addition, each electronic mailing we send you will contain details of how you can unsubscribe.

How do I change any details stored on Argos.co.uk?

To change any of your registered details on argos.co.uk, click on 'log in & registration' and enter your login name and password. Once logged in change any of the details shown and click 'update my details'.

For further information about shopping on Argos.co.uk, please read our [Terms and conditions](#) and [Home delivery information](#).

Contact Us

If you have any comments or queries in connection with our privacy policy, please [Email customer services](#) or call 0845 640 2020 or write to Customer services, Argos Direct, Acton Gate, Stafford, ST18 9AR.

Annex B/3 – Play.com Privacy Statement



Privacy Policy

We take our commitment to your privacy seriously and treat any information you supply to us with care.

- Policy statement
- The data we collect
- Sharing Data
- Surveys and user groups
- Competitions
- 'Email a friend'

Policy statement

In relation to the website: www.play.com ('the Site').

The Site is a Jersey-based website owned by PlayLimited and complies with the **Data Protection (Jersey) Law** of 2005 relating to the personal information you supply online.

PlayTrade S.à.r.l ('PlayTrade') and PlayMedia S.à.r.l ('PlayMedia'), both at 4-6 Avenue de la Gare L-1610 Luxembourg are its wholly owned subsidiaries.

Any personal information that you provide to PlayLimited, PlayTrade and PlayMedia whilst contracting with these entities is stored and controlled by PlayHoldings Limited, located at 40 the Esplanade Saint Helier Jersey JE 49RJ Channel Islands.

For the purposes of **Luxembourg's legislation on Data Protection** and particularly the **law** of August 2nd 2002, PlayHoldings Limited is the Data Controller, whilst PlayTrade and PlayMedia are Data Processors. The information you provide to PlayLimited, PlayTrade and PlayMedia **may be shared with other companies controlled by the PlayHoldings** group that are either subject to this Privacy Policy or follow practices that offer the same level of protection as those described herein.

By using our services, you give us your express consent to process your personal data as described hereafter.

[^]Top

Section Comment: Uses Jersey, Luxembourg Data Protection Law (assumes EU Law compliance?). Complex company structure may complicate perceptions. Data shared with other controlled companies.

The data we collect

The information collected by the aforementioned entities when you register with us at the www.play.com website is generally used to communicate with you and improve our services where possible, and specifically, to process payments or enable **third parties** to carry out technical or commercial supporting functions. These functions **may be** carried out by us or appointed **third parties** who are bound by Data Protection covenants and must process the personal information in accordance with this Privacy Policy and the Data Protection Laws of Luxembourg.

In addition to personal data such as name, e-mail address, delivery address, billing address, credit or debit card number and expiry date, we also analyse data about participants in order to provide a safe shopping environment for **all users**. Examples of the data we **may** collect and analyse include **the internet protocol (IP) address** used to connect your computer to the Internet, login, password, computer and connection information such as browser type and version, your operating system and platform, the full Uniform Resource Locators (URL) clickstream to, through and from our website (including date and time), cookie number, products you viewed or searched for, your **purchase history**, personal preferences and any phone number recorded or used to call our customer services number. In using the Site you **accept** that your personal data **may be used** for such purposes.

We **will not sell, distribute or disclose information about you** or your personal usage of the Site without your express consent or **unless required or permitted to do so by law**. If you subscribe to our mailing lists for new release and other information, we also ask you to answer various general questions about yourself. You will be asked to specify the areas in which you are interested so that we can tailor the information which we send to you to cover the topics and merchandise which we believe you **might be** interested in. By **subscribing to our mailing lists, you accept that your personal data may be used for such purposes**.

Please note that we **provide links to other sites**, which **may not be governed by this Privacy Policy** and you should view the respective privacy policies of those sites for further information.

Participants have the right to access their stored data, to rectify them if required and to object to the storage of their data for legitimate purposes. We would like to keep your information up-to-date, you **may change any of the basic information** we keep about you at any time by e-mailing us at privacy@play.com.

In addition to the information which you supply to us, **information and data may be automatically collected through the use of cookies**. Cookies are small text files the Site can use to recognise repeat users and allow us to **observe behaviour** and compile **aggregate data** in order to improve the Site for you. For example, **cookies** will tell us whether you viewed the Site with sound or with text on your last visit. **Cookies** also allow us to count the **number of unique and return visitors to our Site**.

You can configure your Internet browser to **accept** or reject certain **cookies** or inform you when a cookie is saved.

We do not cross the information recorded in the **cookies** with the personal information collected at the time of your registration on the Site or with your online activity.

Some of our business partners may themselves use **cookies on their own websites**. We have **no access or control** of these **cookies**, therefore we cannot **accept** liability for any malfunctioning of your PC or its installed web browser as a result of your access to any of the websites.

We **may** monitor customer traffic patterns, Site usage and related Site information in order to optimise your use of the Site and we **may** give aggregated statistics to a reputable **third-party**, but these statistics will include no information personally identifying you.

We **may** also use the Information we gather to notify you about important functionality changes and alterations to the Site, or offers of products, services or information that **might be** of particular interest to you. **Your information may also be transferred to another company (based in the European Union or in a country ensuring an adequate level of protection) in the event of sale of our company to a third party**. In that event, we will endeavour to ensure that your rights and freedoms in respect of the processing of your personal data are adequately and appropriately protected. By submitting your Information and ticking the requisite boxes on any order form or when subscribing to the services available on our Site, you **expressly consent to such use and transfer, to the extent permitted by applicable law**. If at any time you wish to stop receiving our newsletter or any other information you **may** have requested from us or any other company, please email or write to Customer Services at the address given for us above or click the Unsubscribe link at the bottom of any e-mail you receive from us.

[^ Top](#)

Section Comment: Language unclear with the words 'may', 'some' throughout the text, personal data can be sold along with the company (will endeavor to protect users' rights), user expressly consents to this transfer and use,

Sharing data

We have business and technical partners whom we share data with to handle orders, process credit and debit card payments and provide a range of services, including for fraud protection purposes. They are bound by Data Protection covenants and must process the personal information in accordance with this Privacy Policy and the Data Protection Laws of Luxembourg.

In case any fraudulent activity is detected on the website, or, without limitation, in connection with the breach of intellectual property rights through the use of the website, we may release personal information in order to comply with any applicable regulation or assert our rights as well as our business partners'.

Section Comment: Third parties have access to the user data and profiles. Language unclear with the words 'may. They will use data if required by law.

[^ Top](#)**Surveys and user groups**

We always aim to improve the services we offer. As a result we occasionally canvass our customers using surveys, provided that they have given their prior and express consent. Participation in surveys is voluntary, and you are under no obligation to reply to any survey you might receive from us. Should you choose to do so, we will treat the information you provide with the same high standard of care as all other customer information.

[^ Top](#)**Competitions**

Your participation on our website may mean that we occasionally contact you with the opportunity to enter competitions. Entry to competitions is voluntary, and you are under no obligation to take up an invitation from us to enter. Should you choose to enter a competition, we will treat the information you provide with the same high standard of care as all other customer information, and use the information provided strictly within the entry terms of the competition and this Privacy Policy.

[^ Top](#)

Section Comment: language unclear with the words 'might' and 'may'

'Email a friend'

We may from time to time operate an 'Email a friend' service. This is a referral service, designed to make it easy for customers to recommend our Site and related websites or offers to a friend, and is a two-step process. First, a customer sends us the friend's name and email address, and secondly, we contact the friend, telling them who we are, and inviting them to take advantage of a particular offer, or to visit our website. When we contact your friend, we always advise them of the name and email address of the friend who made the original referral. We will not use your friend's details for any other purpose.

When a customer wishes to sponsor a friend and provides us with his/her name and e-mail address, we reasonably assume that such customer has obtained his/her friend's prior consent in order for us to process his/her data. Customers supply such information freely and voluntarily, under their sole responsibility.

If any of the information you provide on the form you complete when ordering a product from the website or subscribing to the services changes, please e-mail us at privacy@play.com.

We may occasionally modify this Privacy Policy, such variations becoming effective immediately upon posting to the Site and by continuing to use the website, you will be deemed to accept any such variations.

Should you have any queries regarding the above Privacy Policy, please e-mail us at privacy@play.com.

[^ Top](#)

Section Comment: Language unclear with the word 'may'

Annex C – Material Preparation for Focus Group Sessions

Mark Gazaleh
MSc Final Project E-Business
Focus Group Research Section

Target Group:

I ideally seek postgraduates that are reasonably heavy (experienced) web communicators and shoppers. The subjects need not be experts in the area, but it would be helpful for them to have ample anecdotal material to assist this research.

Group size:

2 groups: i] students and ii] young professionals

Target Dates:

Within period 30 May – 7 June

Location: Various: Marylebone Campus and in London

Topic Background:

There has been much discussion recently on how to provide personalization of Internet services while still protecting users' privacy. Web sites everywhere want to take advantage of the one-to-one nature of communications on the Internet to provide customers with personalized information and services, or to target advertising. To make this personalization and targeting possible, web sites often ask visitors for personal information. Web users suffer the inconvenience of providing the same information many times to different web sites without knowing how the information will be used, or by whom.

Topic Discussion:

A structured discussion will be held to cover these general areas:

- 1] How important web based services are in daily life [when, how do we (not) use it]
- 2] Personal perceptions of the safety and credibility of the web in general, what threats exist
- 3] How we judge whether a web site is safe or credible
- 4] How we act on the internet, how do we protect ourselves (what methods are used)
- 6] Perception of legal protection
- 6] Personal perception and use of privacy statements and 3rd party seals

Duration: 1 hour

5 minutes individual for basic profiling (subject's background, hours on internet per web, usage type etc)

5 minutes background on project

45 minutes structured discussion on topic within group

5 minutes summary conclusions

Inducement:

£10 Odeon Cinema Gift Voucher

Annex D – Main conclusions of Focus Group Sessions

Focus Group Session 1

Participants: BQ
NDTM
Location: Friday 30th May
Time/Date: 14.45-16.00

Main conclusions:

1] Demographics:

Both subjects are post graduate students, working and international (non-UK nationals) living in the UK for last 3 years, both aware of risk of general fraud but not directly impacted (friend had money stolen from account though); one male, one female subject, all not registered on MPS/TPS/FPS

2] How important is the web:

- a) Indispensable (shopping, comparison, social web, banking) – always open at home and work, use Amazon, Play and Argos, self-perception as expert, don't clear cache or cookies, do virus protect, no firewall
- b) Helpful (buy books, news, information – limited shopping, NO banking) – always open at home and work, use Amazon only, self-perception as expert, don't clear cache or cookies, do virus protect, no firewall

3] Perception of safety and threats on the internet:

- a) Like real world – same threats (real world 80% safe, 20% hostile; virtual world 80% safe, 20% hostile), not concerned about internet privacy, trust is earned, biggest threat is malware and loss of privacy; aware of threat, keep financial information back (paypal), not concerned about internet privacy; unaware of privacy seals and site certificates
- b) Not safe enough for all information (real world 80% safe, 20% hostile; virtual world 40% safe, 60% hostile) – need to keep doors locked, concerned about internet privacy, trust is earned, biggest threat is virus, malware and loss of privacy, adverse to threats, not concerned about internet privacy (only use Amazon); aware of site certificates but unaware of privacy seals, will not provide personal data to un-trusted web sites

4] How do you judge if a site is safe:

- a) see if they show effort and care, but if price is compelling then will proceed usually with on-line due diligence, vendor brand is important, front-end and back-end. Don't need to read PS to trust site, unfamiliar with role of PS, don't read PS, don't look for privacy seal, read statement when high cost is involved (read PS after providing info to 5 insurance comparison sites), don't check site certificates, don't read PS because of lack of time, PS are not written for me in mind, will provide personal data to web sites
- b) Look at the interface, logo, brand, information design, interaction quality, famous brand, quality of advertisements on site. Don't need to read PS to trust site, unfamiliar with role of PS, don't read PS, don't look for privacy seal, read statement when high risk is involved, don't check site certificates, don't read PS because of lack of time, PS are not written for me in mind, will not provide personal data to un-trusted web sites

5] Perception of legal protection

- a) very little legal protection, follow-up to any breach of trust would be very costly, even if government is a bad custodian
- b) doubt any real protection exists, both consumers and companies are equally vulnerable

Focus Group Session 2

Participants: IB
GR
AA
Location: Saturday 7 June
Time/Date: 12.00-13.00

Main conclusions:

1] Demographics:

Three subjects post graduate students, working and international (non-UK nationals) living in the UK for last 10 years, both aware of risk of general fraud but not directly impacted (friend impacted through internet fraud, and family had money stolen from account though); two males, one female subjects, all fluent but English not mother tongue, all not registered on MPS/TPS/FPS

2] How important is the web:

- a) critical personal and professional tool (shopping, comparison, business communication, social web, banking, travel organisation) used between 20-40 hours per week (6 days per week), internet always open at home and work, One subject did NOT use Amazon, Play or Argos, other two used Amazon. None used Play.com. Subjects perceived themselves to have strong internet skills. Two users cleared their cache and cookies, while one did not, all use virus protection, two use 3rd party firewalls or while the third uses Macintosh PC (stated thus was no need for a firewall)

3] Perception of safety and threats on the internet:

Internet is not safe environment
Subjects state combinations of 1] Mechanical failure, identity theft, 2] Virus/malware, identity theft, and 3] virus and identity theft as most serious risk
All state they are aware of risks to their information (not adverse), and moderately concerned about the risks to privacy; Most aware about web privacy seals (66%) and certificates (100%)

4] How do you judge if a site is safe:

All do not read a PS in order to trust the site
Two out of three were unfamiliar with the role of PS on a web site
Two out of three did not read PS, 2/3 would consider reading the statement only if they planned a high value transaction
One out of three looked at privacy seals occasionally, the other two never looked at privacy seals;
One out of three (same single subject as above) looked at certificates occasionally, the other two did not look at them at all.
Brand, look and feel, performance were the KEY prompts for trust
Difficulty to understand, lack of time and relevant reasons given for not reading PS
All felt that the PS not written with them in mind – not fit for purpose
All would not give personal information to an untrusted site
Two out of three bothered by profiling

5] Perception of legal protection

Two out of three stated that personal information is adequately protected
A different two out of three reported reading the PS in order to understand their rights
A further different two out of three believed that UK legislation protected their data privacy rights

Annex E – Questionnaire

Questionnaire

Responses

The Efficacy of Internet Privacy Statements

1. What is your age group?		
	Response Percent	Response Count
25 or under 	19.5%	25
25-35 	42.2%	54
35-45 	19.5%	25
Over 45 	18.0%	23
Prefer not to answer <input type="checkbox"/>	0.8%	1
<i>answered question</i>		128
<i>skipped question</i>		0

2. What is your gender?		
	Response Percent	Response Count
Female 	59.4%	76
Male 	40.6%	52
<i>answered question</i>		128
<i>skipped question</i>		0

3. What is the highest level of education you have completed?

	Response Percent	Response Count
Some school <input type="checkbox"/>	0.8%	1
High school or equivalent <input type="checkbox"/>	5.5%	7
Vocational/technical school <input type="checkbox"/>	3.9%	5
Some University <input type="checkbox"/>	3.1%	4
Bachelor's degree <input type="checkbox"/>	40.6%	52
Advanced degree (Master's, Doctoral or Professional degree) <input type="checkbox"/>	46.1%	59
answered question		128
skipped question		0

4. What is your current annual household income?

	Response Percent	Response Count
Under £20,000 (\$40,000) (€25,000) <input type="checkbox"/>	16.4%	21
From £20,000 to £30,000 (\$40,000-\$60,000) (€25,000-€38,000) <input type="checkbox"/>	12.5%	16
From £30,000 to £40,000 (\$60,000-\$80,000) (€38,000-€50,000) <input type="checkbox"/>	13.3%	17
From £40,000 to £50,000 (\$80,000-\$100,000) (€50,000-€64,000) <input type="checkbox"/>	7.0%	9
Above £50,000 (\$100,000) (€64,000) <input type="checkbox"/>	30.5%	39
Prefer not to answer <input type="checkbox"/>	20.3%	26
answered question		128
skipped question		0

5. What is your ethnicity?

	Response Percent	Response Count
White <input type="checkbox"/>	68.8%	88
Black <input type="checkbox"/>	7.8%	10
Asian <input type="checkbox"/>	13.3%	17
Mixed <input type="checkbox"/>	2.3%	3
Other <input type="checkbox"/>	7.0%	9
Prefer not to answer <input type="checkbox"/>	0.8%	1
answered question		128
skipped question		0

6. Which of the following categories best describes your employment situation?

	Response Percent	Response Count
Manager or Professional <input type="checkbox"/>	39.8%	51
Non-management employee <input type="checkbox"/>	21.1%	27
Self-employed <input type="checkbox"/>	8.6%	11
Student <input type="checkbox"/>	24.2%	31
Unemployed <input type="checkbox"/>	0.8%	1
None of the above <input type="checkbox"/>	5.5%	7
answered question		128
skipped question		0

7. How long have you lived in the UK?		
	Response Percent	Response Count
Not living in the UK	21.9%	28
Less than 1 year	12.5%	16
More than 1 year	65.6%	84
<i>answered question</i>		128
<i>skipped question</i>		0

8. Have you been a victim of fraud?		
	Response Percent	Response Count
Yes	32.8%	42
No	67.2%	86
<i>answered question</i>		128
<i>skipped question</i>		0

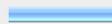
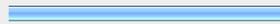
9. Do you know someone who has been a victim of fraud?		
	Response Percent	Response Count
Yes	68.8%	88
No	31.3%	40
<i>answered question</i>		128
<i>skipped question</i>		0

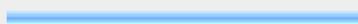
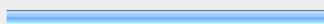
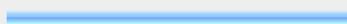
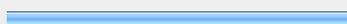
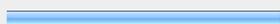
10. Have you been a victim of internet fraud?		
	Response Percent	Response Count
Yes	16.4%	21
No	83.6%	107
<i>answered question</i>		128
<i>skipped question</i>		0

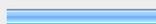
11. Do you know someone who has been a victim of internet fraud?		
	Response Percent	Response Count
Yes	39.1%	50
No	60.9%	78
<i>answered question</i>		128
<i>skipped question</i>		0

12. How long have you been using the internet?		
	Response Percent	Response Count
Less than 12 months	0.0%	0
1 to 2 years	1.6%	2
3 to 5 years	3.9%	5
5 years or more	94.5%	121
<i>answered question</i>		128
<i>skipped question</i>		0

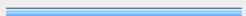
13. Where do you access the internet most frequently?						
	most	second most	second least	least	Rating Average	Response Count
From home (including home office)	58.7% (74)	40.5% (51)	0.0% (0)	0.8% (1)	1.43	126
From office, school, university	46.5% (53)	48.2% (55)	1.8% (2)	3.5% (4)	1.62	114
From public terminal (library, cafe)	1.0% (1)	2.1% (2)	56.7% (55)	40.2% (39)	3.36	97
From other places	0.0% (0)	5.2% (5)	30.2% (29)	64.6% (62)	3.59	96
answered question						128
skipped question						0

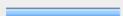
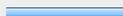
14. Do you use the internet		
	Response Percent	Response Count
All day every day 	28.1%	36
Part of the day everyday 	70.3%	90
Weekly 	1.6%	2
Monthly	0.0%	0
Very occasionally	0.0%	0
answered question		128
skipped question		0

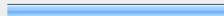
15. Do you use the internet to (check all that apply)		
	Response Percent	Response Count
Communicate 	93.0%	119
Research 	91.4%	117
Work 	82.8%	106
Read news 	87.5%	112
Shop 	87.5%	112
Social network (eg. Facebook) 	68.8%	88
answered question		128
skipped question		0

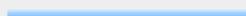
16. Have you used [or are you using] any of the following sites? (check all that apply)		
	Response Percent	Response Count
amazon.co.uk 	81.3%	104
play.com 	18.0%	23
argos.co.uk 	39.1%	50
none of the above 	14.8%	19
answered question		128
skipped question		0

17. If yes, have you read at least one of their privacy statements?		
	Response Percent	Response Count
Yes 	29.7%	38
No 	57.0%	73
Not Applicable 	13.3%	17
answered question		128
skipped question		0

18. If you have read any of their privacy statements, did they increase your trust in the sites?		
	Response Percent	Response Count
Yes 	22.7%	29
No 	18.8%	24
Not Applicable 	58.6%	75
answered question		128
skipped question		0

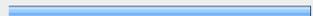
19. While on the internet, do you perceive yourself as		
	Response Percent	Response Count
More risk tolerant person 	28.1%	36
More risk adverse person 	29.7%	38
Neither of the above 	42.2%	54
answered question		128
skipped question		0

20. What is your perceived skill/experience in using the internet?		
	Response Percent	Response Count
Low 	0.0%	0
Light (mid) 	26.6%	34
Heavy 	56.3%	72
Expert (professional) 	17.2%	22
answered question		128
skipped question		0

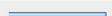
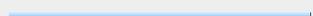
21. Do you use a third party (non-microsoft) firewall on your computer or network?		
	Response Percent	Response Count
Yes 	61.7%	79
No 	23.4%	30
Do not know 	14.8%	19
answered question		128
skipped question		0

22. Do you use virus protection software on your computer?		
	Response Percent	Response Count
Yes 	89.8%	115
No 	7.0%	9
Do not know 	3.1%	4
answered question		128
skipped question		0

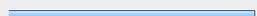
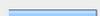
23. Do you ensure that the latest software/security patches are installed on my PC?

	Response Percent	Response Count
Yes 	75.8%	97
No 	16.4%	21
Do not know 	7.8%	10
<i>answered question</i>		128
<i>skipped question</i>		0

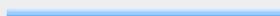
24. Have you requested a copy of your personal report from a credit rating agency (eg. Experian)?

	Response Percent	Response Count
Yes 	24.2%	31
No 	75.8%	97
<i>answered question</i>		128
<i>skipped question</i>		0

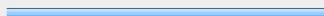
25. Have you provided your personal data to a web site that you suspected might be untrustworthy?

	Response Percent	Response Count
Yes 	16.4%	21
No 	61.7%	79
Not sure 	21.9%	28
<i>answered question</i>		128
<i>skipped question</i>		0

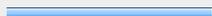
26. Have you undertaken further research on an internet company that appears to be untrustworthy in order to complete a transaction? [This could be accomplished by making a phone call to the company, researching blog comments on the company, looking at review sites etc]

	Response Percent	Response Count
Yes 	30.5%	39
No 	69.5%	89
<i>answered question</i>		128
<i>skipped question</i>		0

27. What monetary incentive would be sufficient to induce you to transact with a website that appears to be untrustworthy? Consider for example, a scenario where you are in the market to buy a large flat screen television (for approximately £1000, \$2000, or €1250)

	Response Percent	Response Count
10-25% Discount 	3.9%	5
20-50% Discount 	14.8%	19
Would not transact with the site 	81.3%	104
<i>answered question</i>		128
<i>skipped question</i>		0

28. Do you think the internet is generally a safe environment?

	Response Percent	Response Count
Yes 	51.6%	66
No 	29.7%	38
Not sure 	18.8%	24
<i>answered question</i>		128
<i>skipped question</i>		0

29. What are the most serious risks that could jeopardise or curtail your internet use? (ranked in order)							
	1 (most)	2	3	4	5	6 (least)	Response Count
Mechanical failure	15.6% (20)	7.8% (10)	9.4% (12)	15.6% (20)	19.5% (25)	32.0% (41)	128
Communication failure	7.0% (9)	15.6% (20)	11.7% (15)	18.8% (24)	37.5% (48)	9.4% (12)	128
Virus and malware attack	22.7% (29)	32.0% (41)	28.9% (37)	11.7% (15)	4.7% (6)	0.0% (0)	128
Identity theft	43.0% (55)	18.0% (23)	18.0% (23)	11.7% (15)	6.3% (8)	3.1% (4)	128
Loss of privacy	9.4% (12)	21.9% (28)	23.4% (30)	16.4% (21)	21.9% (28)	7.0% (9)	128
Spamming	2.3% (3)	4.7% (6)	8.6% (11)	25.8% (33)	10.2% (13)	48.4% (62)	128
<i>answered question</i>							128
<i>skipped question</i>							0

30. How concerned are you about the safety of your personal information on the internet?			
		Response Percent	Response Count
Not concerned		4.7%	6
Slightly concerned		45.3%	58
Quite concerned		28.9%	37
Extremely concerned		21.1%	27
<i>answered question</i>			128
<i>skipped question</i>			0

31. Does internet profiling bother you? (i.e. that someone could know more about you than you do)			
		Response Percent	Response Count
Yes		70.3%	90
No		29.7%	38
<i>answered question</i>			128
<i>skipped question</i>			0

32. Are you concerned that too much of your personal information is stored on various internet sites?			
		Response Percent	Response Count
Yes		77.3%	99
No		22.7%	29
<i>answered question</i>			128
<i>skipped question</i>			0

33. Are you aware of the function of			
	Yes	No	Response Count
Web Privacy Seals	30.7% (39)	69.3% (88)	127
Web Digital Certificates	43.8% (56)	56.3% (72)	128
<i>answered question</i>			128
<i>skipped question</i>			0

34. If you are aware of their function, does their appearance or evidence of their existence improve a site's trustworthiness?				
	Yes	No	Not Applicable	Response Count
Web Digital Certificates	39.7% (50)	4.8% (6)	55.6% (70)	126
Web Privacy Seals	25.8% (33)	10.9% (14)	63.3% (81)	128
<i>answered question</i>				128
<i>skipped question</i>				0

35. Do you know what a privacy statement is?			
		Response Percent	Response Count
Yes		88.3%	113
No		11.7%	15
<i>answered question</i>			128
<i>skipped question</i>			0

36. Do you generally read the privacy statements on the web sites that you visit?			
		Response Percent	Response Count
Yes		19.5%	25
No		80.5%	103
<i>answered question</i>			128
<i>skipped question</i>			0

37. Do you generally read a web site's privacy statement in order to trust it?			
		Response Percent	Response Count
Yes		14.8%	19
No		85.2%	109
<i>answered question</i>			128
<i>skipped question</i>			0

38. Do you generally read privacy statements before transacting with a web site?			
		Response Percent	Response Count
Yes		25.8%	33
No		74.2%	95
<i>answered question</i>			128
<i>skipped question</i>			0

39. Do you generally read privacy statements after transacting with a web site?			
		Response Percent	Response Count
Yes		10.2%	13
No		89.8%	115
<i>answered question</i>			128
<i>skipped question</i>			0

40. How often do you read the privacy statement of web sites you visit?

	Response Percent	Response Count
Always 	4.7%	6
Occasionally 	25.0%	32
Rarely 	46.1%	59
Never 	24.2%	31
<i>answered question</i>		128
<i>skipped question</i>		0

41. The presence of a privacy statement on a web site improves its trustworthiness.

	Response Percent	Response Count
Yes 	58.6%	75
No 	41.4%	53
<i>answered question</i>		128
<i>skipped question</i>		0

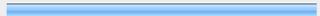
42. I do not need to read a site's privacy statement in order to trust it.

	Response Percent	Response Count
True 	64.1%	82
False 	35.9%	46
<i>answered question</i>		128
<i>skipped question</i>		0

43. I always check a site's privacy seal before registering my details on a using a web site.

	Response Percent	Response Count
Yes 	16.4%	21
No 	83.6%	107
<i>answered question</i>		128
<i>skipped question</i>		0

44. I always check the details of a site's verification certificate before transacting with a web site.

	Response Percent	Response Count
Yes 	22.7%	29
No 	77.3%	99
<i>answered question</i>		128
<i>skipped question</i>		0

45. I require an SSL lock icon to appear on my web browser before transacting with an internet site.

	Response Percent	Response Count
Yes 	37.5%	48
No 	62.5%	80
<i>answered question</i>		128
<i>skipped question</i>		0

46. Assess the factors that influence your trust in a web site (rank in order of importance).

	1 (Most)	2	3	4	5	6	7	8 (Least)	Response Count
Brand of the company	68.0% (87)	16.4% (21)	5.5% (7)	3.9% (5)	2.3% (3)	1.6% (2)	0.0% (0)	2.3% (3)	128
Previous experience of company	18.9% (24)	60.6% (77)	10.2% (13)	4.7% (6)	0.8% (1)	3.9% (5)	0.8% (1)	0.0% (0)	127
Look and feel of the site	0.8% (1)	7.1% (9)	42.5% (54)	7.1% (9)	13.4% (17)	4.7% (6)	21.3% (27)	3.1% (4)	127
Presence of a privacy statement	2.4% (3)	5.6% (7)	17.5% (22)	34.9% (44)	11.9% (15)	11.1% (14)	11.1% (14)	5.6% (7)	126
Understanding its privacy statement	0.8% (1)	3.2% (4)	6.3% (8)	16.7% (21)	31.7% (40)	17.5% (22)	18.3% (23)	5.6% (7)	126
Presence of a privacy seal	2.4% (3)	3.1% (4)	7.1% (9)	13.4% (17)	18.1% (23)	44.1% (56)	9.4% (12)	2.4% (3)	127
Presence of a verification certificate	6.3% (8)	2.4% (3)	4.8% (6)	17.5% (22)	17.5% (22)	13.5% (17)	31.7% (40)	6.3% (8)	126
Compelling commercial offer overrides any concerns	0.8% (1)	2.4% (3)	7.9% (10)	3.1% (4)	3.9% (5)	2.4% (3)	6.3% (8)	73.2% (93)	127
<i>answered question</i>									128
<i>skipped question</i>									0

47. If you generally do not read privacy statements, is this because

	Response Percent	Response Count
of a lack of time?	39.8%	51
the statements are not visible?	9.4%	12
they are typically hard to understand or are too complicated?	39.1%	50
they are not relevant?	4.7%	6
they are not trustworthy?	7.0%	9
<i>answered question</i>		128
<i>skipped question</i>		0

48. Do you think that Privacy Statements are 'fit for purpose' and are written with you in mind?

	Response Percent	Response Count
Yes	20.3%	26
No	79.7%	102
<i>answered question</i>		128
<i>skipped question</i>		0

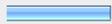
49. Do you read a web site's privacy statement to understand your legal rights?

	Response Percent	Response Count
Yes	21.9%	28
No	78.1%	100
<i>answered question</i>		128
<i>skipped question</i>		0

50. Do you believe that your personal information and privacy is adequately protected under the legal system of your country of residence?

	Response Percent	Response Count
Yes	18.8%	24
No	36.7%	47
Do not know	44.5%	57
<i>answered question</i>		128
<i>skipped question</i>		0

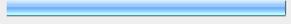
51. Do you NOT read a web site's privacy statement because you feel confident that you are adequately protected by the legal system in your country of residence?

	Response Percent	Response Count
Yes 	25.8%	33
No 	74.2%	95
<i>answered question</i>		128
<i>skipped question</i>		0

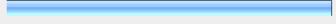
52. A prize draw for £25 of cinema tickets will be held for all participants that leave their contact e-mail at the bottom of this page. Please be assured that this address list will be SOLELY used for the purpose of the competition. Please enter your e-mail address if you would like to participate in this prize draw. Otherwise click to continue.

	Response Percent	Response Count
Email Address: 	100.0%	70
<i>answered question</i>		70
<i>skipped question</i>		58

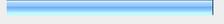
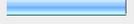
26. Have you undertaken further research on an internet company that appears to be untrustworthy in order to complete a transaction? [This could be accomplished by making a phone call to the company, researching blog comments on the company, looking at review sites etc]

	Response Percent	Response Count
Yes 	30.5%	39
No 	69.5%	89
<i>answered question</i>		128
<i>skipped question</i>		0

27. What monetary incentive would be sufficient to induce you to transact with a website that appears to be untrustworthy? Consider for example, a scenario where you are in the market to buy a large flat screen television (for approximately £1000, \$2000, or €1250)

	Response Percent	Response Count
10-25% Discount 	3.9%	5
20-50% Discount 	14.8%	19
Would not transact with the site 	81.3%	104
<i>answered question</i>		128
<i>skipped question</i>		0

28. Do you think the internet is generally a safe environment?

	Response Percent	Response Count
Yes 	51.6%	66
No 	29.7%	38
Not sure 	18.8%	24
<i>answered question</i>		128
<i>skipped question</i>		0

###