Chapter 13
"*All my mates have got it, so it must be okay*": Constructing a Richer Understanding of Privacy Concerns—An Exploratory Focus Group Study

Anthony Morton

13.1 Introduction

In a 2010 UK survey[1], 76.4 % of respondents were either *very concerned* or *somewhat concerned* about their privacy while using the Internet. In the same survey, 44 % had experienced an invasion of their privacy[2] *very frequently* or *somewhat frequently*. A 2011 survey by the European Commission on attitudes towards data protection and electronic identity found that although three out of four respondents accepted the need to provide personal information as part of everyday life, 70 % were concerned about how organisations use their personal information, believing they had "*only partial, if any, control of their own data*".[3] Although privacy surveys have attracted some criticism[4], they highlight a genuine concern amongst people of the impact of technology-underpinned services on their privacy. This concern is not misplaced. In the last five years, services as diverse as street-level mapping[5], smartphones and smartphone applications[6], video-gaming[7], social networking[8], targeted advertising[9] and peer-to-peer file-sharing[10] have attracted adverse publicity

[1] Coles-Kemp et al. 2010.

[2] For this survey question, an invasion of privacy included offline intrusions, e.g. unsolicited telephone calls, in addition to online intrusions, e.g. e-mails.

[3] European Commission (EUROPA) 2011.

[4] Harper and Singleton 2001.

[5] Barnett 2008; BBC 2008; Mills 2007.

[6] Sarno 2010; Panzarino 2011; Leavitt 2011.

[7] Quinn and Arthur 2011.

[8] BBC 2010, 2011.

[9] Fiveash 2007; Ashford 2011.

[10] Mennecke 2007; NBC 2009; Federal Trade Commission 2010.

A. Morton (✉)
Department of Computer Science, University College London,
Gower Street, London WC1E 6BT, UK
e-mail: anthony.morton.09@ucl.ac.uk

S. Gutwirth et al. (eds.), *Reloading Data Protection,*
DOI 10.1007/978-94-007-7540-4_13, © Springer Science+Business Media Dordrecht 2014

or criticism, for collecting or leaking personal information. Such services, although offering benefits such as easier navigation and travel, entertainment, social contact, relevant advertising and access to media content, may explicitly request personal information, collect it covertly or accidentally[11], or distribute it without the user's knowledge.[12]

Investigation of an individual's privacy concerns has traditionally focused on their general level of privacy concern, or their perception of organisations' collection, use, management, control and securing of personal information, by asking them to respond to a selection of statements about government and/or organisations' information handling practices. However, responding to statements about information handling practices in the abstract is problematic. When asked to consider one of Westin's statements—"*Most businesses handle the personal information they collect about consumers in a proper and confidential way*"[13]—a survey participant may reasonably think, "*It depends on the organisation. I trust organisation X, but not organisation Y, as I don't believe it will look after my personal information carefully*". Furthermore, when providing personal information to an organisation, the nature of the technology platform involved is omitted from most general privacy concern surveys. For example, a customer may be comfortable conducting financial transactions using a bank's website, but not using a smartphone application—even when interacting with the same bank. Finally, such surveys do not take into account environmental influences, such as the experiences of an individual's friends, or media stories concerning similar technology-underpinned services. Peoples' attitudes to disclosing their personal information is complex, as they may state they value their information privacy, but are usually prepared to trade personal information for benefits.[14]

A more holistic approach to the construction of privacy concern is required, which encompasses the technical, organisational and environmental factors individuals take into account when choosing to use a technology-underpinned service requiring the provision of personal information. Existing privacy concern indexes, such as Westin's, only provide measurement of an individual's general level of privacy concern. An individual's privacy concern is likely to be constructed from their concerns about the technology-mediated interaction they are having with a specific organisation, others' views of the organisation and/or technology, and their personality, life experiences and innate desire, or otherwise, to protect their privacy.

To emphasise the importance of considering a broad range of factors in determining privacy concern, this paper henceforth refers to the socio-technical construct of

[11] Farrell 2010.

[12] Johnson 2008; El Emam 2010.

[13] This statement was one of those used by Westin to derive his Privacy Segmentation Index, and Core Privacy Orientation Index used in his studies between 1995 and 2003—quoted in Kumaraguru and Cranor (2005).

[14] Beldad et al. 2011.

a *technology service*—proposed by Morton & Sasse[15]—in place of the more cumbersome phrase *technology-underpinned service*. A *technology service* consists of a technology platform[16] and the organisation providing it. The use of the *technology service* construct emphasises the need, when attempting to understand peoples' privacy concerns, of not only considering the hardware and software in the technology platform, but the motivation, principles, culture and privacy practice of the organisation providing the *technology service*.

When deciding to use a technology service[17], an individual's desire to achieve their goal(s) usually results in them having to balance relinquishing some aspect of their information privacy in exchange for benefits[18] (e.g. saving credit card details on an e-commerce website to achieve their goal of saving time). In essence, "[. . .] *individuals will exchange personal information as long as they perceive adequate benefits will be received in return—that is, benefits which exceed the perceived risks of information disclosure*" (p. 327).[19] However, individuals do not always rationally consider the risks and consequences—including long-term ones—of information disclosure[20], and are often unable to predict the nature of the information to be managed.[21] Nevertheless, the phrase, "*perceived risks of information disclosure*" does encapsulate the meaning of privacy concern. If an individual believes the party requesting the information is not capable of looking after their personal information properly, they will perceive a high degree of risk. Privacy concern—in the context of a technology-mediated interaction—can therefore be thought of as an individual's perceived risk of disclosing personal information; the higher the perceived risk, the higher the individual's level of privacy concern. Beldad views online information privacy as a response to the risks of disclosing personal data, influenced by the amount and type disclosed.[22] This suggests privacy concern, like privacy, is highly contextual, depending, in part, on an individual's expectations of the privacy behaviour of the technology service under consideration—it cannot be measured in the abstract.

An individual's privacy-sensitive decision making process is likely to affected by incomplete information, bounded rationality (their ability to understand the available information and use it to make a rational privacy-sensitive decision), and psychological factors.[23] However, an individual will usually make some effort to consider

---

[15] Morton and Sasse 2012.

[16] Morton and Sasse use the term *technology lens* for the technology platform to highlight that a poorly implemented or designed technology platform may lead an individual to have a distorted view of the organisation, no matter how benign its motivation.

[17] For simplicity it is assumed an individual actively makes a decision to use a technology service, rather than its use being mandatory or unavoidable (e.g. closed-circuit television), or it existence being unknown.

[18] Sheehan and Hoy 2000.

[19] Culnan and Bies 2003.

[20] Acquisti 2004; Acquisti and Grossklags 2005.

[21] Laufer and Wolfe 1977.

[22] Beldad et al. 2011.

[23] Acquisti and Grossklags 2005.

information about a technology service to assist, or justify, their privacy-sensitive decision making, unless they are solely focused on the benefits it offers. Generally speaking, levels of risk increase when there is insufficient information to assess the true level of risk. Similarly, an individual's level of privacy concern will rise if there is incomplete information about a technology service's ability to safeguard the personal information they need to provide. To reduce the discomfort with a lack of information about the collection and usage of their personal data, people will engage in '*information-seeking behaviours*'[24], with Beldad suggesting "[a]*n online privacy statement is often the only source of information*" (p. 222).[25] However, people are also likely to seek information from other sources, such as the attributes of the technology service which are important to them (e.g. security mechanisms, brand name, professionalism of website design etc.) and the advice of friends and colleagues.

Perfect information about a technology service is not possible, and even if it was available, bounded rationality would be likely to prevent an individual from correctly processing it. Fortifying notice-and-consent, such as clearer privacy policies—although welcome—assumes "[i]*ndividuals can understand all facts relevant to true choice at the moment of pair-wise contracting between individuals and data gatherers*" (p. 32).[26] An individual is therefore likely to look for certain attributes of the technology service they are considering using, which they consider to be important. These may include: its professionalism; design; ease of use; perceived security protections; nature of the information requested; perceived ethics of the providing organisation; evidence of sound information handling practices; and links to trusted third parties (e.g. online payment systems). Environmental cues, such as friends' experiences, reviews by existing users and changing social privacy norms[27] are also likely to influence an individual's privacy concern.

The absence of, or incomplete information about, the technology service attributes or environmental cues an individual seeks for reassurance in their decision to engage with it, are likely to lead to an increase in privacy concern. For example, a missing or unclear privacy policy on a website may cause an individual's level of privacy concern to increase, fearing the providing organisation will sell their personal information to a third-party without their permission. Similarly, a lack of information from friends and colleagues about their experiences with a particular technology service may also increase an individual's level of privacy concern.

If it is assumed the technology service attributes and environmental cues an individual seeks for reassurance are underpinned by their innate level of privacy concern, it can be seen that an individual's privacy concern when engaging with a technology

[24] Beldad et al. 2011.

[25] Beldad et al. 2011.

[26] Nissenbaum 2011.

[27] Mark Zuckerberg, the CEO of Faceboook's observation that "*People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time"* is a good example of this—TechCrunchTV 2010.

service can be constructed from: (1) their innate level of privacy concern; (2) environmental cues, which may be general or related to the technology service under consideration; and (3) attributes of the technology service under consideration. The last of these components (attributes of the technology service) will be highly contextual (i.e. relevant to a particular technology service), with the second one partially influenced by context (i.e. media stories about technology services similar to the one under consideration). Furthermore, each of the three privacy concern components is also likely to be influenced by an individual's personality and attributes (e.g. age, gender, educational level, computer experience etc.). For example, an individual may have been told by friends of their negative privacy experiences with a technology service, but discounted these views because they believe their friends are "*not particularly Internet-savvy*" and "*probably didn't tick the right boxes*".

As the first stage in developing this richer approach to the construction of peoples' privacy concern, the rest of this chapter describes an exploratory study—using focus groups and an online survey—to explore what people consider when deciding to use a technology service offering benefits, but requiring personal information. Section 13.2 situates the proposed approach to constructing privacy concerns in the context of existing work in trust, and the measurement of peoples' privacy concerns, and proposes a hypothetical model based on this work. Sections 13.3, 13.4 and 13.5 describe the research objectives addressed by the study, and provide a description of the research method used. The results from the qualitative and quantitative analyses of the focus group transcripts are discussed in Sects. 13.6–13.9. The paper concludes in Sects. 13.10 and 13.11 with a discussion of the limitations of the study and the next steps for the research, which is to create a richer representation of individuals' privacy concerns, linking this with organisational privacy practice and privacy by design.

13.2 Related Work

Westin—who defines *privacy* as, "*the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about themselves is communicated to others*" (p. 7)[28]—categorised people in his surveys of their privacy concern as: (1) *Privacy Fundamentalists*—who are protective of their privacy, distrustful of organisations collecting personal data, and believe in privacy regulation; (2) *Privacy Pragmatists*—who consider the consequences of providing private information *vs*. the benefits received; and (3) *Privacy Unconcerned*—who are least protective of their privacy, believing any benefits they receive for disclosing personal information outweigh its potential misuse.[29]

---

[28] Westin 1967.

[29] Kumaraguru and Cranor 2005. Perri 6 observes a fourth group is now also recognised—*privacy fatalists*—"*who believe that there is little that they or anyone else can do to ensure proper use of personal information*" (p. 2)—6 et al. 1998.

One-dimensional measurements of peoples' general level privacy concern, such as Westin's categorisation, do not explain the specific dimensions of that concern.[30] To address this, Smith et al. (1996) created a multidimensional scale called, concern for information privacy (CFIP), constructed from individuals' concerns about organisations' information handling practices in the context of offline direct marketing. CFIP is constructed from four factors relating to the handling of information by organisations: (1) collection; (2) errors; (3) unauthorised secondary use; and (4) improper access to information. Stewart & Segars observed, "[. . .] *the theoretical and operational assumptions underlying the structure of constructs such as CFIP should be reinvestigated in light of emerging technology, practice, and research*" (p. 37)[31], and empirically validated CFIP. They concluded that CFIP was a second-order factor mediating the relationship between computer anxiety and behavioural intention. They also suggested that growing awareness amongst consumers of explicit and implicit information collection and processing by organisations are likely to impact the nature of CFIP—in essence, the effect of environmental cues, such as media stories and the experiences of friends and colleagues.

Using CFIP as the foundation, Malhotra et al. (2004) created the more parsimonious Internet Users' Information Privacy Concerns (IUIPC) scale, specifically aimed at the Internet environment. IUIPC consists of ten items measuring three factors: (1) information collection—identified by Smith et al. (1996); (2) control over personal information; and (3) awareness of an organisation's privacy practices. Although these privacy concern scales recognise an individual's perception of an organisation's information handling practices is an important constituent in their level of privacy concern, they do not explain the influence of external factors, an individual's innate privacy concern, and the specific attributes of the technology service (e.g. perceived security protections, professionalism, design, ease of use, perceived brand and ethics of the providing organisation, service etc.), which an individual seeks for reassurance.

If, as posited earlier, privacy concern is assumed to be the "*perceived risks of information disclosure*"[32], trust in the technology platform and providing organisation's privacy behaviour is key to people feeling comfortable disclosing personal information, as '[t]*rust is only required in situations that are characterized by risk and uncertainty*' (p. 384).[33] Social exchange theory posits that if the benefits of a social transaction with another party outweigh the perceived costs (or risks), an individual will enter into it; trust therefore plays a critical role in this process as it reduces perceived costs and is a precondition for self-disclosure.[34]

The relationship between privacy concern, trust and behavioural intention were explored by Liu et al. in the context of e-commerce, who found that "*privacy has a strong influence on whether an individual trusts an EC* [(e-commerce)] *business.*

[30] Malhotra et al. 2004.

[31] Stewart and Segars 2002.

[32] Culnan and Bies 2003, p. 327.

[33] Riegelsberger et al. 2005.

[34] Metzger 2004.

In turn, this will influence their behavioral intentions to purchase from or visit the site again" (p. 300).[35] Privacy, in their *privacy–trust–behavioural intention model* consists of the dimensions of notice, access, choice and security, matching the Fair Information Practices set out by the US Federal Trade Commission for e-commerce.[36] This suggests a technology service implementing and following fair information practices, and making this behaviour visible to an individual considering using it, is more likely to engender trust than one which does not.

Like privacy, trust's multi-dimensional nature makes it impossible to arrive at a unitary definition. To address this, McKnight & Chervany[37] developed a typology of three trust constructs: (1) *dispositional trust*; (2) *interpersonal trust*; and (3) *institutional trust*. *Dispositional trust* is essentially the general level of trust an individual has, consisting of *faith in humanity* and *trusting stance*.[38] Rotter[39] was the first to develop a scale for this construct of an individual's generalised trust in others[40]—effectively an innate level of trust—which an individual carries with them and applies to each situation. An individual's upbringing and culture will mould their persona and hence their disposition to trust.[41] Peoples' disposition to trust has been found to be positively related to their enthusiasm to embrace new technology[42]—their *Personal Innovativeness with respect to Information Technology* (*PIIT*)—a construct developed by Agarwal & Prasad, which they define as, "*the willingness of an individual to try out any new information technology*".[43]

Tan & Sutherland[44] include dispositional trust in their multidimensional model of trust, to emphasise the importance of this personality-based trust on consumers' trusting behaviour. They suggest that interpersonal trust and institutional trust are founded upon dispositional trust, observing, "[i]*f the individual typically finds it hard to trust in general, they are not likely to find the internet a comfortable place to conduct business* [. . .]" (p. 47)[45] Similarly, it is likely an innately private person will not feel comfortable providing personal information to technology services. An organisation making its privacy policy available will have little impact on the views of Privacy Fundamentalists, or those who believe any information disclosure is risky.[46]

Institutional trust is split into: (1) *situational normality*—things appear normal; and (2) *structural assurances*—contracts, regulations and warranties are in place and

---

[35] Liu et al. 2005.

[36] Federal Trade Commission 2000.

[37] McKnight and Chervany 2001.

[38] McKnight and Chervany 2001.

[39] Rotter 1967.

[40] Rotter refers to this as *interpersonal trust*.

[41] Tan and Sutherland 2004.

[42] McKnight et al. 2002.

[43] Agarwal and Prasad 1998.

[44] Tan and Sutherland 2004.

[45] Tan and Sutherland 2004.

[46] Beldad et al. 2011.

evident.[47] In the context of a technology service, an example of *situational normality* is an e-commerce website appearing professional and following a familiar shopping basket and checkout paradigm; an example of a *structural assurance* is the website adhering to distance selling legislation.

An individual's assumptions and expectations of a technology service, which form part of their initial level of trust in it, may be influenced by *trust signals* emitted by the technology service, allowing the individual to determine if trust should be given[48], and hence whether personal information should be disclosed. Trust signals include *trust symbols* (e.g. evidence of HTTPS and trusted third-party seals) and *trust symptoms* (e.g. user reviews, usability and professionalism of web site design).[49] These trust signals originate from the technology service and mainly influence *interpersonal trust*, allowing an individual (*trustor*) to decide if trust should be given to the *trustee*. If the sources of trust signals are the attributes of a technology service related to its information privacy practice, e.g. use of technical security controls, stated privacy policy and control over personal information provided to its users, absent or weak trust signals are likely to increase an individual's level of perceived risk of information disclosure, leading to increased privacy concern and decreased trust.

In addition to the trust signals emitted by a technology service, individuals' trust in a technology service may be influenced by environmental cues, such as the experiences of friends, advertising material (e.g. television and poster advertisements) and social privacy norms. For example, an individual's level of trust in a particular technology service is likely to be increased if their friends have used it with no perceived problems—hence the quote in the title of this paper. These environmental cues may not be directly related to the technology service under consideration. Environmental cues such as media reports and experiences of using similar technology services are likely to be an important constituent of peoples' privacy concern, as individuals generalise broadly from their experiences.[50]

Gefen et al. (2003), in their study of trust and technology acceptance in the context of online shopping, suggest the decision to purchase from an e-vendor has two antecedents: (1) their trust in the technological aspects of the website interface (influenced by its perceived ease of use); and (2) the trust the consumer has in the vendor (essentially *interpersonal trust*), reflecting the two main components of a technology service, the technology platform and providing organisation. Using three terms from Riegelsberger et al.'s (2005) framework—an organisation's *internalised norms* (e.g. policies, privacy behaviour etc.), *benevolence* (e.g. an easy faulty product return process) and *ability* (e.g. professionalism of its website)—an individual may trust the *norms and benevolence* of an organisation, but not its *ability* to provide a secure technology platform to protect users' information from unauthorised intrusion.[51] For example, an individual may believe an organisation possesses strong information

[47] McKnight and Chervany 2001.

[48] Riegelsberger et al. 2005.

[49] Riegelsberger et al. 2005.

[50] Camp et al. 2002.

[51] Beldad et al. 2011.

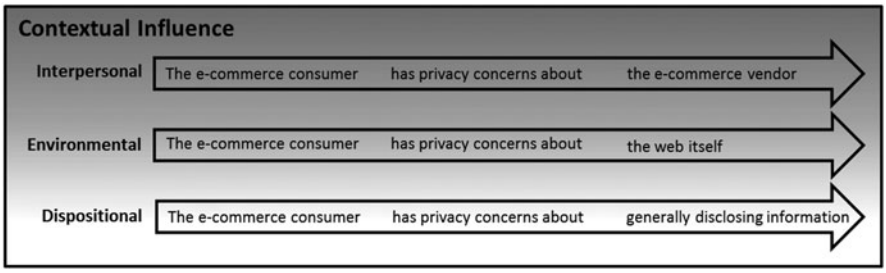

Fig. 13.1 Grammar of the privacy concern model (for an e-commerce website)

ethics and intention to safeguard collected information[52]—causing privacy concern to lessen—but may also suspect the organisation is unable to realise those ethical principles due to a poorly implemented technology platform—increasing the individual's level of privacy concern.

Research has shown a relationship between an individual's degree of *agreeableness* measured by the Five-Factor Model of personality (the Big Five) and their level of privacy concern measured by CFIP—albeit with a restricted sample of respondents.[53] Other studies have shown a relationship between an individual's personality traits and their level of privacy concern.[54] Peoples' attributes (e.g. age, gender, experience, cultural background and intellectual capability) also influence their adoption of new technology.[55]

If an individual's personality influences their level of privacy concern, trust and technology adoption, it is also likely to influence the environmental cues and technology service attributes an individual looks for to lessen their privacy concern. For example, one personality type may place a high degree of importance on technical security controls (e.g. the HTTPS browser 'padlock') and the existence of a privacy policy, whilst another may only consider the advice of friends or social norms.

McKnight & Chervany represent their trust construct using three sentences in a *grammar of trust*, with each one constructed as an action sentence with a subject, verb, and direct object.[56] If an individual's level of privacy concern is influenced by: (1) their innate level of privacy concern; (2) environmental cues; and (3) the attributes of the technology service, a *grammar of privacy concern* (Fig. 13.1) can be constructed using a similar approach, with an individual's privacy concern constructed from:

1. **Dispositional privacy concern**. An individual's innate concern about disclosing any information to other parties. *Dispositional privacy concern* is essentially the construct captured by traditional privacy surveys such as Westin's, and therefore

[52] Beldad et al. 2011.

[53] Korzaan and Boswell 2008.

[54] Iris et al. 2008.

[55] Agarwal and Prasad 1999; Venkatesh and Morris 2000.

[56] McKnight and Chervany 2001.

represents only a partial understanding of the nature of an individual's privacy concern.

2. **Environmental privacy concern**. An individual's level of privacy concern created by environmental cues, such as media reports, anecdotes from friends and family, and social privacy norms. *Environmental privacy concern* may also be lessened by structural contracts and regulations (e.g. applicable data protection legislation) being in place and evident.
3. **Interpersonal privacy concern**. An individual's level of privacy concern about the party they are transacting with. The level of privacy concern will be increased or lessened by the existence or absence of technology service attributes an individual considers important and therefore looks for.

The shading in Fig. 13.1 represents the increasing influence of context on the three components of privacy concern. The philosophy of *privacy as contextual integrity*[57] posits that the transfer of personal information between two entities (e.g. a consumer and an e-commerce website) should be tied to the widely accepted norms of particular contexts, so that information collection and dissemination is appropriate to each context and the roles of the entities, and in line with expectations. It is the violation of these norms and expectations which is one of the principal factors leading to peoples' perception that their privacy has been invaded. The collection and dissemination of personal information by increasingly powerful technologies and digital media serve to subvert these norms and expected information flows.[58] Contextual integrity is constructed from: (1) informational norms; (2) appropriateness of collection and dissemination; (3) roles of the entities involved; and (4) principles of transmission.[59] Given this construction of contextual integrity, Fig. 13.1 shows that interpersonal privacy concern will be more influenced by context (e.g. a specific transaction with a particular e-commerce website), than dispositional privacy concern.

Perri 6 describes research by Brunel University, which suggests a "*more nuanced approach to segmentation*" (p. 39) than Westin's—based on a repertoire of behaviours—and argues people take different privacy stances in different contexts, and very few can be simply categorised as fundamentalist, unconcerned or pragmatic.[60] The construction of privacy concerns shown in Fig. 13.1 addresses this by recognising that although an individual's *dispositional privacy concern* is an important factor underpinning their privacy concern, the contextual influences at the *interpersonal privacy concern* layer, and to some extent, at the *environmental privacy concern* layer, are extremely important.

Organisations may be able to influence peoples' level of interpersonal information privacy concern through information handling practices which avoid substantive harm, and the use of trust signals[61], but are unlikely to be able to significantly, or

[57] Nissenbaum 2004.

[58] Nissenbaum 2004.

[59] Barth et al. 2006.

[60] 6 et al. 1998.

[61] Riegelsberger et al. 2005.

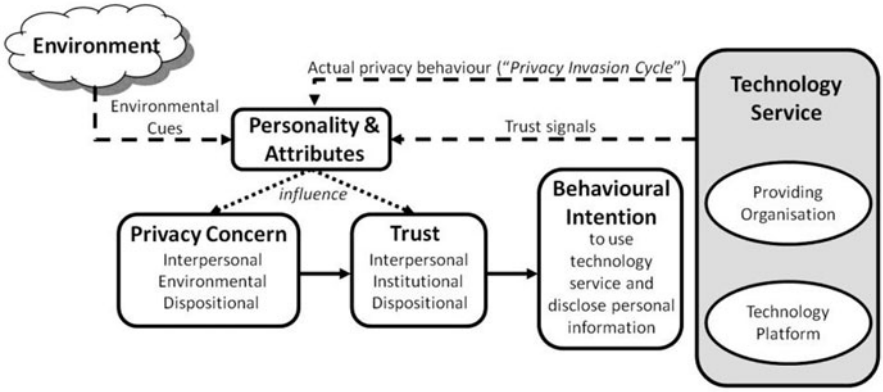

Fig. 13.2 Hypothesised extended model of privacy concern, trust and behavioural intention

quickly, influence an individual's dispositional privacy concern. Pragmatically, this approach to privacy concern seems reasonable. An individual with a very high level of dispositional privacy concern is unlikely to provide their personal information, irrespective of the experiences of others, or the perceived privacy behaviour of the other party. Similarly, an individual with a moderately high level of dispositional privacy concern may be dissuaded from providing their personal information by the experiences of friends who have had their information passed to third parties—increasing the individual's environmental privacy concern.

Using the *privacy–trust–behavioural intention model* of Liu et al. (2005) and the idea of trust signals proposed by Riegelsberger & Sasse[62], a hypothesised extended model of privacy concern, trust and behavioural intention is proposed (Fig. 13.2). The model illustrates how trust signals emitted by a technology service—albeit modified by an individual's personality and attributes—influence interpersonal trust (e.g. trust in the ability of the technology service to provide the products ordered) and interpersonal privacy concern (e.g. the level of concern about the technology service's privacy practices). Similarly, environmental cues will be modified by an individual's personality and attributes, influencing their environmental privacy concern.

An individual will have assumptions and expectations of a technology service's likely privacy behaviour, with their "*privacy perceptions often reflect*[ing] *their trust in the organisation, technology and thus expectations for privacy protection*" (p.52) (also please add superscripted reference to footnote 64). If an individual's experience of the technology service's actual privacy behaviour does not match these expectations and assumptions, because of a malicious or incompetent organisation, error, or a badly designed technology platform leaking sensitive information, the individual is likely to feel their privacy has been invaded, have an emotive reaction, and reject the technology and providing organisation—Adams & Sasse call this the *Privacy Invasion Cycle*[63], and this concept has been included in the hypothesised model

[62] Riegelsberger et al. 2005.

[63] Adams and Sasse 2001.

shown in Fig. 13.2. The invasion of an individual's privacy is likely to result in a decrease in their trust as a result of an increase in their privacy concern about the technology service, suggesting the construction of peoples' privacy concern is likely to be a dynamic process.

13.3 Research Objectives & Method

The principal aim of this exploratory study was to understand the factors—organisational, technological and environmental—which people consider when deciding to use a technology service. More specifically, it was to explore the factors which increase or decrease their *interpersonal privacy concern* and *environmental privacy concern* (Fig. 13.1). The secondary aim was to investigate if peoples' attributes (age, computer experience, gender etc.) influence the organisational, technological and environmental factors they consider to be important (Fig. 13.2). These aims resulted in two research objectives:

1. To investigate the organisational, technological and environmental factors people consider when deciding to use a technology service.
2. To investigate if there is a relationship between individuals' attributes (e.g. age, gender, computer experience etc.), willingness to adopt new technologies and general privacy concern (e.g. their Westin category), and the organisational, technological and environmental factors they consider.

If people look for very disparate organisational, technological and environmental factors when faced with different types of technology services, the hypothesised model (Fig. 13.2) is unlikely to be feasible. Therefore a third research objective was defined:

3. To investigate if the factors individuals consider are broadly common to all technology services.

To address these three objectives, a research method was required—richer than online surveys—which facilitated open-ended investigation of these factors, without unduly influencing study participants. Focus groups were selected as the research method as they are suited to the investigation of complex behaviours and motivations[64], such as technology adoption and privacy-sensitive decision making. Focus groups also allow participants to query each other, explain themselves and comment on each other's experiences.[65] There has been some use of focus groups in understanding privacy concerns about technologies, and acceptance of new technologies[66]; this latter area being focused on informational privacy in healthcare.[67] There has however, been

[64] Morgan and Krueger 1993.

[65] Kitzinger 1995; Morgan 1996.

[66] Zhang et al. 2010; Hundley and Shyles 2010; 6 et al. 1998.

[67] Skinner et al. 2003; Snell et al. 2012.

Table 13.1 Focus group scenarios and composition

Focus group no	Scenario	Group composition
G1	Photograph sharing web site	Technical PhD students and postdoctoral researchers
G2	Social networking discounts	Undergraduate students
G3	Supermarket RFID ordering	Technology outsourcing business development and administrative staff
G4	Smartphone assistant	Postgraduate students
G5	Smart metering	IT support and development, IT business development, IT project management, retirees and administrative staff
G6	Landmark identification web site	Extended family group consisting of retirees, middle managers, administrative staff and tradesmen

promising work by the VOME project[68], which has run interactive sessions with users discussing citizen-centric privacy by design.[69]

In addition to the focus groups, an online survey was used to collect quantitative data prior to participants' attendance at each focus group, although completion of the survey was not a pre-requisite for attendance. The principal objective of the survey was to provide data for quantitative analysis to investigate research objective 2. The survey was split into four sections: (1) eight questions concerning the participant; (2) one question to ascertain the participant's willingness to adopt new technologies; (3) three questions to ascertain the participant's general level of privacy concern; and (4) two questions based on Sheehan's study of privacy concerns[70], which were not used in the study.

13.4 Focus Group Procedure

Six focus groups—considered to be an adequate number[71]—took place, capturing the views of 35 individuals. To ensure participants represented a broad range of experiences and ages, opportunistic sampling with participant peer recruitment was used for four of the groups, with the other two groups consisting of volunteers from a UK university's participant pool (Table 13.1).

At the start of each focus group the researcher provided an overview of the objectives of the session and briefly described the concept of a technology service. This

[68] Visualisation and Other Methods of Expression (VOME) is a project involving researchers from the Information Security Group at Royal Holloway, University of London, Salford and Cranfield Universities. It has explored how users engage with the concepts of information privacy. For further information about VOME see http://www.vome.org.uk.

[69] VOME 2012.

[70] Sheehan 2002.

[71] Morgan 1996.

was to encourage participants to think more widely than the technology described in the scenario, and also consider the organisation providing it.

Once the focus group had read the scenario randomly allocated to it (see Appendix for the six scenarios), it was shown the following three questions:

1. What things would you consider when deciding to use, or not use, this technology service?
2. How would you go about deciding if the benefits offered by this technology service were worth the potential loss of some of your privacy?
3. How would you decide whether to trust this technology service to look after your privacy?

Each focus group lasted approximately one hour, with 15–20 min spent discussing each question. Use of the same questions and procedure for each focus group facilitated investigation into the similarity of the themes discussed across the focus groups. The groups were designed to encourage participants to interact with each other, rather than the researcher, allowing "*structured eavesdropping*" (p. 301).[72] The researcher attempted to restrict their contribution to reading the three questions out aloud, and asking further probing questions when required.

13.5 Qualitative Analysis of Focus Groups

A thematic analysis—similar to that described by Braun & Clarke[73], albeit without producing a thematic map—was undertaken for the qualitative analysis of the focus group transcripts.

Each focus group was recorded by the researcher, and transcribed by a professional typing agency. The researcher listened to the audio recording of each session twice, correcting any errors in the transcripts, and ensuring anything in the transcript which identified the focus group or its members was redacted. This ensured the data was "*transcribed to an appropriate level of detail, and the transcripts* [. . .] *checked against the tapes for 'accuracy*"' (p. 96).[74] This process of active reading and re-reading, and becoming familiar with the data, assisted with generating initial ideas for base-level codes.

Once the transcripts had been checked they were loaded into ATLAS.ti, and participants' comments—*quotations* in ATLAS.ti—coded by the researcher in a systematic fashion with an initial set of base-level codes. The entire transcript from each focus group was coded to ensure '[e]*ach data item has been given equal attention in the coding process*.' (p. 96).[75] At the end of the initial coding phase 39 base-level codes had been created, excluding the ATLAS.ti super-codes and non-substantive codes used to facilitate subsequent quantitative analysis. The 39 base-level codes

[72] Powney J., quoted in Kitzinger 1995.

[73] Braun and Clarke 2006.

[74] Braun and Clarke 2006.

[75] Braun and Clarke 2006.

Table 13.2 Demographic profile of online survey participants

Demographic characteristic		Percentage of respondents
Gender ($n = 27$)	Male	51.9
	Female	48.1
Age (years; $n = 27$)[a]	Under 18	3.7
	18–24	7.4
	25–34	33.3
	35–44	25.9
	45–54	14.8
	55–64	11.1
	Over 65	0.0
	Rather not say	3.7
Education level[a] ($n = 26$)[b]	Doctoral	7.7
	Postgraduate	19.2
	Undergraduate	38.5
	Diploma level	19.2
	School leaver	15.4

[a] The total of the percentages in Table 13.2 for this survey item does not equal 100 % because of rounding

[b] $n = 26$ as one online survey participant was still attending school

were then collated into candidate themes by considering whether a code could be combined with others into an overarching theme.

Although Braun & Clarke suggest quotations may be coded '[. . .] *in as many different 'themes' as they fit into* [. . .]' (p. 89)[76], the researcher coded each quotation to a single base-level code, and hence theme. This encouraged the researcher to consider carefully what each participant was actually alluding to in their comment, and also facilitated the reconciliation of totals during quantitative analysis. Each quotation was also coded with a non-substantive reference for the participant who spoke it, e.g. G5P7, for participant 7 in group 5. This enabled cross-referencing of focus group quotations with the results from the online survey, during the quantitative analysis.

13.6 Online Survey Results

13.6.1 Survey Participant Demographics

Prior to attending the focus groups, 27 of the 35 focus group participants completed the online survey, with response rates ranging from 56 to 100 % within each focus group. Table 13.2 shows the demographic profile of online survey participants, and Table 13.3 their level of computer experience and daily computer use.

[76] Braun and Clarke 2006.

Table 13.3 Computer experience and use profile of online survey participants

Demographic characteristic		Item statistics ($n = 27$)
Computer experience (years)	Mean	19.9
	Standard deviation	6.8
Computer use at home and work per day (hours)	Mean	6.7
	Standard deviation	3.1

13.7 Survey Participants' General Attitude to Technology and Privacy

Four of the questions in the online survey were asked to determine participants' general level of privacy concern, and their attitude towards adopting new technologies, the results of which are discussed briefly below:

- **Technology Privacy Concern**: Participants were asked to respond to two statements concerning their perception of the impact on their privacy of: (1) existing technology, which had been around for at least three years; and (2) emerging technology, which had appeared in the last year. These two statements represented a survey participant's *technology privacy concern* (TPC), which can range from 2 to 8, where 2 represents two '*Not concerned at all*' responses and 8 represents two '*Very concerned*' responses. Ignoring the results from the two survey participants who selected '*Don't know*', resulted in a sample size of 25, with a mean TPC score of 6.0 ($\sigma = 1.55$), suggesting a relatively high level of TPC amongst survey participants, which may be caused by the relatively high percentage (40.7 %) of Privacy Fundamentalists in the survey group.
- **Westin's Privacy Segmentation Index**: Survey participants were asked to respond to the same three statements used by Westin between 1995 and 2003 to determine peoples' Privacy Segmentation Index/Core Privacy Orientation Index[77], with their responses used to place them into one of three privacy categories using the same criteria as Westin (Table 13.4). In Westin's surveys from 1996 to 2003, between 55 and 64 % of participants were categorised as Privacy Pragmatists, with the remaining participants split approximately equally between Privacy Fundamentalists and Privacy Unconcerned.[78] The high percentage of Privacy Fundamentalists (40.7 %) amongst survey participants in this exploratory study may be caused by the large percentage (65.4 %) educated to undergraduate degree level or above. Previous studies have found a relationship between higher levels of education and increased privacy concern.[79]

[77] This index was called the *Privacy Segmentation Index* for Westin's surveys between 1995 and 1999, and the *Core Privacy Orientation Index* for the surveys since mid-2000 (Kumaraguru and Cranor 2005).

[78] Kumaraguru and Cranor 2005.

[79] Phelps et al. 2000; Sheehan 2002.

Table 13.4 Percentage of online survey participants in each Westin category ($n = 27$)

Westin category	Percentage of online survey participants
Privacy fundamentalists	40.7
Privacy unconcerned	18.5
Privacy pragmatists	40.7

The total of the percentages in Table 13.4 does not equal 100 % because of rounding.

Table 13.5 Responses to: "Here are some predictions about how technology will impact peoples' privacy in the next five years. Which of the following statements comes closest to the way you feel?" ($n = 27$)

Statement	Percentage of survey participants	Coding
Technology will make peoples' privacy worse	59.3	3
Technology will make peoples' privacy better	7.4	2
Despite advances in technology, peoples' privacy will remain about the same as it is today	18.5	1
Don't know	14.8	N/A

- **Future Impact of Technology on Privacy**: Table 13.5 shows the percentages for the responses from survey participants to the same question used by Westin in 1996.[80] Almost 60 % of survey participants believed technology would make people's privacy worse over the next five years.

To test if survey participants' responses to this question were consistent with their responses to the TPC statements, they were coded as shown in the far right-hand column in Table 13.5, and a Pearson two-tailed correlation test (with '*listwise*' exclusion, so $n = 22$) performed between these and the TPC scores. Correlation was significant at 0.599 ($p = 0.003$), indicative of consistency between the responses from each participant to these two survey questions about privacy concern in relation to technology.

- **Willingness to adopt new technologies**: To assess survey participants' willingness to adopt new technologies, a score for each participant was calculated by taking the mean of scores for the four statements in Agarwal & Prasad's PIIT scale.[81] A mean score of 7 represented someone with the highest level of willingness to adopt new technologies, and a mean score of 1 represented someone with the lowest. The overall mean PIIT score for focus group survey participants was 4.82 ($\sigma = 1.18$), suggesting a reasonable level of comfort using new technology. To assess the reliability of the measure, Cronbach's α was calculated to be 0.825—indicating good internal consistency.

[80] Kumaraguru and Cranor 2005.

[81] Agarwal and Prasad 1998.

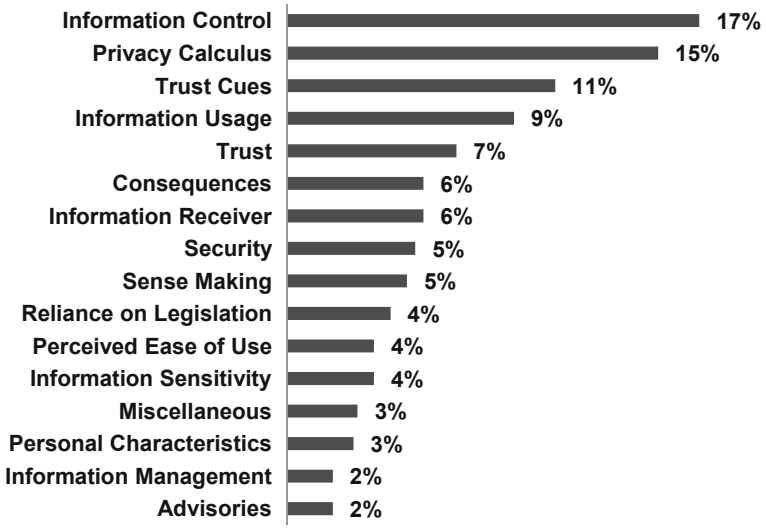

Fig. 13.3 Percentage of coded quotations from focus groups for each identified theme ($n = 599$)

13.8 Focus Groups—Qualitative Analysis

From the analysis of the six focus group transcripts, 599 quotations were coded and allocated to one of 39 base-level codes, grouped into 16 themes.[82] Fig. 13.3 shows the percentage of coded quotations allocated to each of the 16 themes.

Quotations from the focus group transcripts not directly related to the research objectives, such as copyright, peoples' desire for an online presence, the societal impact of technology and general criminal activity, were placed in a *Miscellaneous* theme—representing 3 % of coded quotations. The three themes most frequently discussed in the groups: (1) *Information Control*; (2) *Privacy Calculus*; and (3) *Trust Cues*—representing 43 % of all coded quotations—are discussed in the next three sections.

13.8.1 Information Control

The *Information Control* theme includes four base-level codes used for quotations relating to: (1) organisations passing personal information to third parties (34 %); (2) the ability to opt-in or opt-out of aspects of a technology service (27 %); (3) individual control over access to personal information (24 %); and (4) information control provided by a technology service (15 %).

Organisations passing personal information to third parties was the most common concern within the *Information Control* theme. This was either because of a perception that some organisations act unethically, or individuals being unaware

[82] See Appendix for a description of the types of quotations covered by each theme.

they had given permission to share personal information. Passing of information to third parties without notice, and the secondary use of that information, is an important factor in people feeling their privacy has been invaded.

In common with the three out of four of the respondents in the European Commission survey[83], focus group participants recognised organisations' commercial objective to collect and sell consumers' personal information. One focus group participant observed, "*Well, they're probably selling the data to the retailers, aren't they? It's a revenue stream from that*" (G5). A participant in another group remarked, "*Well obviously the company wants to get as much money as they possibly can, and this site would be for free, would be free sign up, so they have to get the money through the links we share*" (G2).

As two of the groups' discussions progressed (G3 & G4), participants became aware of the potential consequences—collated under the *Consequences* theme—of information being passed to third parties for secondary use. A participant in the group discussing the Smartphone Assistant scenario said:

> So how would that affect insurance companies for example? Because I've thought about that as well, so if there's all this data about what I'm buying, where I'm going, you know, let's say I have diabetes and I went and bought sweets all the time that would get recorded and then I'd have an issue with my diabetes, and insurance would go like, 'Well, you know, she's doing all of that stuff and she's not helping herself.'

The ability to opt-in or opt-out of aspects of a technology service was discussed in all groups, particularly in the context of passing information to third parties. Under the UK Data Protection Act 1998, if a data holder wishes to pass a data subject's information to a third-party, permission must be sought from the data subject. Three of the groups referred to the framing of such questions[84] (G1, G5 & G6); with participants generally suspecting commercial pressures lead organisations to offer consumers the choice to opt-out, rather than the more acceptable opt-in. Many in the group discussing the Photograph Sharing Web Site scenario felt organisations deliberately obfuscated the opt-in/opt-out process, with one participant expressing anger about having to opt-out of receiving e-mails from third parties: "[. . .] *when it's a little tiny little tick that you have to find it in some buried place within the website that actually really annoys me*." Individuals' effort to control their privacy and their selection of services—particularly with respect to opting out—was also raised in the group discussing the Smart Metering scenario, with one participant remarking, "*Now you have to actively protect your privacy by, you know, looking for the boxes of 'I don't want to be contacted'*, [. . .] *'I don't want my details to be sent out'*".

Individual control over access to personal information, which relates to the control people wish to exercise over access by others to their personal information, was touched upon by five groups (G1, G2, G4, G5 & G6). Unsurprisingly, the group discussing the Landmark Identification Website scenario contributed the majority (63 %) of the quotations within this base-level code, as this scenario was potentially the most personally invasive. One participant in this group reflected the group's

[83] European Commission (EUROPA) 2011.

[84] Bellman et al. 2001.

consensus, stating, "*I wouldn't be altogether comfortable knowing that other people can just take a photograph of you and find out all sorts of information about you.*"

Information control provided by a technology service relates to the amount of control a technology service provides a user—specifically the data subject—to manage the disclosure of personal information. Participants raised concerns about technology services requesting: unnecessarily mandatory data items (G4); information perceived as irrelevant by the user (G5); and information considered sensitive or intrusive by the user during initial interaction with a technology service (G1 & G4). Three groups (G1, G3 & G6) stressed their need for a technology service to notify them about which information was being shared, and with whom. One participant (G1) observed:

> You don't really know what you are going to be sharing. They never really say, 'If you join the service we will then take all of these eight items'. That doesn't really exist.

Providing users with accurate feedback about which information is being collected, was taken further by a participant in another group (G4) who said:

> It's always you're in or you're out, [it's] never the option to, 'I would still like to join your service providing these things are not recorded or done for me' and then put them all back in the other person's court. 'Do you still think I'm valuable enough to be a customer for you?'

This approach would allow users to decide which personal information they are comfortable to provide, given the context and benefit received—leaving the organisation to determine if they still wish to provide them with the benefits offered.

13.8.2 Privacy Calculus

Westin's Privacy Pragmatist, who is someone prepared to forgo some of their privacy in exchange for some sort of benefit, exemplifies the concept of *privacy calculus*. Pragmatically, privacy calculus is the cost/benefit[85] analysis in which an individual considers the benefits against the potentially unforeseen consequences of information disclosure. The privacy calculus concept is founded on Laufer & Wolfe's idea of a "*calculus of behaviour*", in which people consider the consequences of engaging in a particular behaviour.[86] They cite the example of an individual submitting to personality testing, and disclosing personal information, in the belief the outcome will be beneficial—this individual will not consider this as an invasion of privacy.[87] However, they are likely to consider it privacy-sensitive, and ask themselves, "*Can I trust this person to safeguard the personal information I have passed to them?*"

---

[85] Dinev and Hart (2006) refer to these polarities as '*risk beliefs'* and '*confidence and enticement beliefs*' respectively.

[86] Laufer and Wolfe 1977.

[87] Laufer and Wolfe 1977.

The notion of privacy calculus is therefore effectively a trade-off in which an individual weighs up the cost to their privacy against the benefits of disclosing private information; Beldad et al. (2011) observe:

> [w]hen the expected benefits from the information disclosure do not outweigh the value attached to the personal data to be disclosed, information withholding or incomplete information disclosure could be forthcoming (p. 226).

The *Privacy Calculus* theme includes two base-level codes: (1) the benefits received by an individual for using a technology service (72 %); and (2) an individual's thought processes when considering the benefit offered by a technology service, against the amount and type of personal information requested (28 %). During coding it was often difficult to decide which of these two base-level codes a quotation should be coded against; this was mitigated by including both within the *Privacy Calculus* theme.

The benefits received by an individual for using a technology service were placed on a continuum by the focus groups, with tangible benefits at one end: cash payments (G1 & G2); cheaper products and services (G3 & G6); and cost savings (G3 & G5). At the other end of this continuum are intangible benefits: recommendations (G1 & G4); removal of the effort of visiting shops (G3 & G4); assistance with lifestyle (G3); ability to save credit card details (G1 & G4); social benefits (G5); and socialising (G1 & G2). Beldad et al. also categorise benefits as *tangible* or *intangible*, with tangible benefits (e.g. cash, vouchers or gift items), and intangible benefits (e.g. convenience, joining a social networks and personalised services).[88] However, focus group participants differentiated between discount vouchers or credits, and cash payments, when considering their privacy. One participant in the group discussing the Social Networking Assistant scenario—which offered credits which could only be spent with participating companies—stated:

> [. . .] if they gave me cash, physical cash, I wouldn't mind, but because I don't have the choice of where I spend the credits, it has to be targeted on certain sites, my privacy concerns would be dominant in a situation like this.

This suggests certain benefits, such as discount vouchers and two-for-one offers (G1, G2 & G6) are actually situated in the middle of the benefits continuum, with their relevance to an individual's goal(s) at a particular point in time increasing their attractiveness. For example, the group discussing the Landmark Identification Web Site scenario initially rejected the idea, but one participant observed:

> I think if I was at a landmark that costs thirty, forty pounds each to get into, and all of a sudden I was offered two-for-one tickets, but by accepting that offer and using that offer, there isn't an opt-out button to receive mailings, for example, from a company. At the time I'd probably take it.

An individual's thought processes when considering the benefit offered by a technology service against their perceived loss of privacy accounted for 28 % of the coded quotations under the *Privacy Calculus* theme. However, all groups at some point during their discussions referred to the privacy-sensitive decision making

[88] Beldad et al. 2011.

process they adopt. The relevance of a technology service's benefits to an individual's goals has already been alluded to, and this appeared to be a particularly important factor in participants' privacy calculus. One participant in the group discussing the Landmark Identification Web Site scenario exemplified this by observing:

> The tipping point for me would be, would I get benefit, do I think I would use this enough? [. . .] I'd make a conscious decision, 'Will I use this software, is it of benefit to me, are there savings there, generally across the board? Yes or no?' Yes, I would use it, and, to a certain extent, take this on board.

Another participant in the same group explicitly referred to the degree of privacy invasion versus the benefit received:

> For me it comes back to a decision about trade-off. So, am I happy to be bombarded with emails? Yes. Am I happy to be bombarded with emails, but any stranger could identify me? Probably not. And if I'm not willing then I don't want the offer, because it's not worth it.

13.8.3 Trust Cues

Although the focus groups referred to the importance of *trust symptoms*, such as other users' reviews (G2 & G6), findings from personal research (G1 & G2), friends' recommendations (G1, G2, G3, G4 & G6), and magazine reviews (G4), the groups' discussions also highlighted the importance of other prompts from the wider environment—*environmental cues*—in the construction of an individual's trust in a technology service and therefore a willingness to provide it with personal information. The *Trust Cues* theme therefore encompasses not only coded quotations relating to *trust symbols* and *trust symptoms* (45 %)[89], but also environmental cues, which account for the remaining 55 % of coded quotations in this theme.

Environmental cues include: (1) social privacy norms—specifically participants perception of peoples' information sharing behaviour; (2) technology norms—particularly the increasing capabilities of technology to collect and process information; and (3) other external cues, such as advertisements (G1), media stories of hacking and loss of credit card details (G1, G2 & G5), payment for goods and services through recognised methods, e.g. Verified by Visa (G1), and use of the technology service by other people (G6). With reference to this last cue, participants admitted there was comfort in 'following the crowd', with a participant in the group discussing the Landmark Identification Website scenario admitting:

> [. . .] you hear of more and more people using it, so you think, 'Well it must be okay.' So, it goes back to the fear of the unknown, and whilst you don't know much about it, the more people that use it, the more comfortable you become with it.

Social privacy norms and technology norms appear to define a 'privacy floor' for participants in terms of acceptable levels of information sharing behaviour. One participant in the group discussing the Landmark Identification Website scenario observed:

[89] Riegelsberger et al. 2005.

> So, it's just a totally different world now, and I think people are more willing to accept it, if they've come through that generation. I think there's much more willingness to accept what's out in the public domain and what you're going to share with people [. . .]

Examples from the focus groups of societal and technology norms used by participants in their privacy-sensitive decision making were:

- **Societal norms**—the need to share information as part of modern life (G2 & G6); peoples' apparent comfort with sharing personal information (G1 & G6); increasing availability of personal information (G2); and the need to enter personal details to gain access to discounts and services (G3 & G6).
- **Technology norms**—the increasing levels of surveillance, e.g. CCTV (G1 & G4); behavioural tracking by websites and supermarket loyalty cards (G1, G3 & G6); unsolicited e-mails and targeted advertising (G4 & G6); and the relentless progress of technology (G3).[90]

13.9 Focus Group Theme Similarity

There was insufficient data across all theme/focus group combinations to perform a statistical test to determine if there was a broad similarity between the focus groups, in terms of the number of times each theme was discussed (research objective 3 in Sect. 13.3). An approach was therefore required to facilitate visual inspection of the qualitative data in the transcripts.

The percentages for each of the 15[91] themes were calculated as the number of quotations for that theme, divided by the total number of quotations in each focus group. A frequency table was created, and the 25 and 75 % percentiles calculated to define three categories based on the percentage of a focus group's coded quotations relating to each theme: (1) *H*—between 9 and 22 %; (2) *M*—between 3 and 9 %; and (3) *L*—less than 3 %; these categories were used to label each theme/focus group combination in Table 13.6. Table 13.6 is divided into three sections—shown by the outlined cells—based on the number of *H*, *M* and *L* categories, so that the most common category in each section—reading from left to right—is *L*, *M* and *H*. This overview grid suggests a broad degree of communality of themes raised and discussed across the focus groups despite the use of different scenarios.

The two most popular themes—*Information Control* and *Privacy Calculus*—have an *H* category in all six focus groups. Despite the broad commonality of the remaining 13 themes across the focus groups—there are some exceptions—most noticeably the *H* categories in five of the scenario/theme combinations in the *Somewhat Discussed* group, and the single *L* category in the *Frequently Discussed* group. Transcripts from focus groups where there were unexpected *H* or *L* categories in the scenario/theme combinations were therefore re-examined.

---

[90] In many respects this acceptance of technology norms, i.e. the inevitability of technological progress and increasing collection and processing of personal information, echoes the views of the *privacy fatalists*—6 et al. (1998).

[91] The *Miscellaneous* theme was excluded, resulting in a sample size of 582 quotations.

Table 13.6 Percentage of quotations—as a category—for each theme across all focus groups ($n = 582$ quotations)

Technology service scenario	Advisories	Information management	Personal characteristics	Information sensitivity	Perceived ease of use	Reliance on legislation	Sense making	Security	Information receiver	Consequences	Trust	Information usage	Trust cues	Privacy calculus	Information control
Photograph sharing web site (Group 1)	L	L	L	M	M	H	M	L	M	M	H	M	H	H	H
Social networking discounts (Group 2)	M	M	L	L	M	M	M	M	M	L	M	M	H	H	H
Supermarket RFID ordering (Group 3)	L	L	L	L	L	L	L	H	M	H	M	H	M	H	H
Smartphone assistant (Group 4)	M	L	L	L	M	L	M	M	L	L	M	H	M	H	H
Smart metering (Group 5)	L	L	M	M	M	M	M	M	M	M	H	H	L	H	H
Landmark identification web site (Group 6)	L	L	M	M	L	L	M	L	M	M	L	M	H	H	H
	Rarely discussed			Somewhat discussed								Frequently discussed			

75% of themes in the *Frequently discussed* section have an *H* category
58% of themes in the *Somewhat discussed* section have an *M* category
72% of themes in the *Rarely discussed* section have an *L* category

13.9.1 Photograph Sharing Web Site Scenario (Group 1)

Participants in this group discussed how they felt the law protects their data and financial transactions, along with their distrust of organisations' motives—resulting in an *H* category for the following two themes:

- **Reliance on Legislation**—The discussion in this group began with concerns about copyright of users' photographs—coded under the *Miscellaneous* theme—and frequently returned to how the law protects consumers. The group discussed terms and conditions, data protection, consumer fraud and financial protection.
- **Trust**—Like the Smart Metering scenario, participants generally mistrusted organisations' motives—with one participant observing, "*these big companies have all been shown to act in very dubious ways and that's I think that's what actually scares people the most*"—or trusted particular brands based on their experience—with another participant remarking, "*I trust Amazon, or I am happy to give them the information I have* [. . .] *given them*".

13.9.2 Supermarket RFID Ordering Scenario (Group 3)

Participants in this group discussed the collection and use of data about shopping habits, and the overall security of the system—resulting in an *H* category for the following two themes:

- **Consequences**—Participants were worried about the potential financial consequences of their shopping habits, with one participant fearing that details about products purchased could be sold to the UK National Health Service (NHS), leading them to say, "*you've got a non-healthy diet, because of that and you're more likely to develop diabetes. Therefore we're going to charge you more money in tax, because you're more likely to use our hospitals"*.
- **Security**—Participants frequently discussed their concerns regarding the security of the system, due to the sanctity of the home, concerns about the authorities (e.g. police) checking up on them, and disquiet about the security of information captured by the system.

13.9.3 Smart Metering Scenario (Group 5)

Participants in this group frequently returned to their overall mistrust of energy suppliers, resulting in an *H* category for the *Trust* theme. Two comments encapsulated the group's opinions—"*Do you know any electricity suppliers we trust?*", and "*I don't trust any of these companies really, deep down*". This appeared to be primarily caused by participants' previous experiences of incorrect utility meter readings, with one observing for estimated bills, "*they have actually estimated it for the future* [. . .] *and half the time it's wrong*". This mistrust in energy suppliers' competence appeared to be generalised to a suspicion that energy suppliers would probably misuse the detailed electricity consumption data from smart meters. Participants also mistrusted energy suppliers' motives—with one stating "*My concern would also be the likelihood is that they will benefit more than I*".

Despite this focus group's mistrust of energy suppliers this scenario was the only one to have an *L* category for the *Trust Cues* theme. This may have been because participants knew—or at least suspected—that the UK Government will make smart meter installation mandatory in the future. When asked, "*What things would you consider when deciding to use or not use this technology service?*", one participant responded, "*I think whether it's optional or not, whether you have got a choice or whether it's part of the contract to have this meter fitted*". If smart metering does become mandatory, environmental cues are likely to have minimal effect on peoples' adoption behaviour.

13.10 Personal Characteristics and Themes Discussed

A quantitative analysis of focus group transcripts was carried out to investigate the hypothesised relationship between participants' personal characteristics (i.e. their attributes and general attitudes to technology adoption and privacy) and the themes discussed in the focus groups. As this required data for each focus group participant from the online survey, only quotations made by the 27 participants who completed the survey were used in the quantitative analysis.

Where required, the personal characteristics from the online survey were converted into categorical variables[92] using the criteria shown. Pearson's chi-square (χ^2) test was used to determine if there was a relationship between the personal characteristics captured by the online survey and the themes raised in the focus groups. Pearson's chi-square test is used as a test of independence of two categorical variables (e.g. a personal characteristic and a theme discussed in the focus groups). The chi-square statistical test calculates the deviations between the actual frequencies observed in each combination of categorical variables and the frequencies which might be expected due to chance. The sum of the standardised deviations between the observed and expected frequencies for each combination of categorical variable results in Pearson's chi-square (χ^2) statistic.

An important criterion for Pearson's chi-square test to be valid is that the expected frequency in each combination of categorical variables is greater than 5. However, in thematic analysis there are likely to be themes with relatively few coded quotations attributed to them, therefore quotations relating to themes representing less than 5 % of the total 599 coded were removed, resulting in nine themes covering 477 quotations. As chi-square tests could only be carried out for participants responding to the relevant survey question used in each chi-squared test, the maximum data set size used for the chi-square test was 420 quotations—70 % of total quotations coded—across nine themes.

To transform the focus group transcript data into a format allowing quantitative analysis, it was exported from ATLAS.ti as an XML file and processed with a Microsoft Excel Visual Basic module developed by the researcher. This created a Microsoft Excel worksheet, which could be imported into SPSS, with each row

[92] These are marked with an asterisk in Table 13.7.

containing a coded quotation, its theme, and information from the survey pertaining to the participant who made the quotation, e.g. age, computer experience, Westin category, etc.

The results in Table 13.7 show the chi-square figure in six of the nine Pearson chi-square tests as significant, supporting an association between certain participant characteristics and the themes discussed in the focus groups. Conventionally, a Pearson chi-square test is considered statistically significant, i.e. two categorical variables are not independent, if the value of $p < 0.05$ (the column headed "p (sig.)" in Table 13.7). The results suggest participants' intrinsic attributes (e.g. age and gender) are not related to the number of quotations within each theme discussed in the focus groups, but there is evidence to support an association with educational level and computer experience. The one exception to this latter category was the amount of time a participant used a computer each day, which did not appear to have a significant association with the themes raised and discussed in the focus groups.

The standardised residuals for the six chi-square tests, which supported a significant association between the personal characteristic category and the theme discussed in the focus groups, were used to understand which themes contributed significantly to the overall association, thus:

- **Educational Level**—Participants in the *Lower* education level category made significantly less quotations relating to the *Trust* theme ($z = -2.1$) than expected—this was the only theme with a significant effect for this categorical variable.
- **Computer Experience (in years)**—There was no theme about which participants made significantly more or fewer quotations.
- **Personal Innovativeness in Information Technology (PIIT)**—Participants in the *Late Adopters* category (PIIT score $< \mu$) made significantly fewer quotations relating to the *Information Receiver* theme ($z = -2.1$) than expected—this was the only theme with a significant effect for this categorical variable.
- **Technology Privacy Concern**—Participants with a *High* TPC score (TPC $>= \mu + \sigma$) made significantly more quotations relating to the *Security* theme ($z = 2.5$), and significantly fewer quotations relating to the *Information Receiver* theme ($z = -2.0$) than expected. Participants with a *Low* TPC score (TPC $<= \mu - \sigma$) made significantly more quotations relating to the *Trust Cues* theme ($z = 2.5$), than expected.
- **Westin Category**—Participants in Westin's *Privacy Unconcerned* category made significantly more quotations relating to the *Trust Cues* theme ($z = 3.2$), than expected; participants in the *Privacy Fundamentalists* category made significantly fewer ($z = -2.3$). Participants in the *Privacy Fundamentalists* category also made significantly more quotations relating to the *Security* theme ($z = 2.2$) than expected.

Table 13.7 Pearson chi-square test results for personal characteristic categories and themes discussed across all focus groups

Personal characteristic category	Categorical variables and criteria	n[a]	df	Chi-square value[b]	p (sig.)	Possible assoc'n?
Gender	Male Female	420	8	12.997	0.112	No
Age*	Under 35 35 and older	420	8	9.442	0.306	No
Educational level*	Lower (< undergraduate) Higher (≥ undergraduate)	420	8	17.727	0.023	Yes
Computer experience*	Low (years $< \mu$) High (years $\geq \mu$)	420	8	17.715	0.023	Yes
Daily computer use*	Low (hours $< \mu$) High (hours $\geq \mu$)	420	8	7.742	0.459	No
Personal innovativeness in information technology (PIIT)*	Late adopter (PIIT score $< \mu$) Early adopter (PIIT score $\geq \mu$)	420	8	21.817	0.005	Yes
Technology privacy concern*	Low (TPC $\leq \mu - \sigma$) Medium ($\mu - \sigma <$ TPC $< \mu + \sigma$) High (TPC $\geq \mu + \sigma$)	411[c]	16	35.813	0.003	Yes
Westin category	Privacy unconcerned Privacy pragmatist Privacy fundamentalist	420	16	36.332	0.003	Yes
Future impact of technology on privacy (Westin)	Better Same Worse	366[c]	16	45.092	< 0.001	Yes

[a] Number of focus group quotations in chi-square analysis

[b] Pearson chi-square test

[c] This was less than the maximum possible 420 quotations as some survey participants responded with "*Don't know*" to this survey item

- **Future Impact of Technology on Privacy (Westin)**—This result should be treated with some caution, as the expected frequency in 29.6 % of the cells in the contingency table was less than 5. This was a large contingency Table (3 × 9), and "[i]*n larger tables the rule is that all expected counts should be greater than 1 and no more than 20 % of expected counts should be less than 5*" (p. 695).[93] For this chi-square test all expected counts were ≥ 4 and $p < 0.001$, suggesting the possibility of a relationship. This personal characteristic also had a significant effect on the largest number of themes. Participants who thought technology would make peoples' privacy better over the next five years made significantly fewer quotations relating to the *Trust* theme ($z = -2.3$) than expected. Participants who thought technology would make peoples' privacy worse over the next five years made significantly fewer quotations relating to the *Trust Cues* theme ($z = -2.0$) than expected. Participants who thought the effect of technology over the next five years would be about the same as it is today, made significantly more quotations relating to the *Trust Cues* theme ($z = 3.3$), and significantly fewer quotations relating to the *Information Usage* theme ($z = -2.5$), than expected.

13.11 Limitations of Study

An obvious limitation of this study was the small sample size of 35 people who took part in the focus groups. However, as this was an exploratory study involving focus groups, and the "[. . .] *common rule of thumb is that most projects consist of four to six focus groups*" (p. 144)[94], an average of six participants in each focus group is reasonable.

Although the sample size for the online survey was also small ($n = 27$), the chi-square tests used to find a relationship between participants' personal characteristics and the themes discussed across the focus groups, used up to 420 coded quotations, split across nine themes. Despite the creation of the themes being data-driven 'from the ground up', significant statistical relationships were found between specific attributes of people (e.g. computer experience, measures of general privacy concern and PIIT), and the number of times specific themes were discussed across the focus groups. However, the chi-square tests only investigated the relationship between two categorical variables—the focus group theme and personal attribute—for all quotations across all focus groups. Such a test cannot provide a probability that an individual with a particular attribute will be the one to raise a particular topic in the group. The analyses also did not differentiate between those quotations which were the first time a particular theme was discussed, and those that were related to further discussions on the same theme.

A major advantage of focus groups—their ability to encourage group level discussion—is potentially one of their major limitations. Participants may behave

[93] Field 2009.

[94] Morgan 1996.

differently if faced with the technology service assigned to their focus group in a different context (e.g. using it alone to achieve a specific goal). The *privacy paradox*, in which peoples' stated privacy behaviour is not the same as their actual behaviour, is a well-known phenomenon.[95] However, in the context of a focus group, particularly when discussing a specific technology service, people may be more truthful about their privacy behaviour in front of others who may challenge them and ask for justification of their views.

In focus group discussions people may be reminded by other participants of factors they would not normally consider, and therefore there is a danger of dominant personalities steering a group's discussion—both these biases were mitigated to some extent by the study's design. Firstly, the use of a standard set of three questions, with an approximately similar amount of time allotted to each question, ensured discussion remained focused, and was not hijacked by particular participants. Secondly, the use of an online survey gave participants the chance to provide their views of privacy in a different and solitary context—the data from these two different research methods still resulted in statistically significant relationships.

13.12 Conclusions and Further Work

Information Control was the most frequently discussed theme in the focus groups, with 17 % of all coded quotations. Not only does this lend credence to the idea that people principally seek informational self-determination when engaging with technology services, but also echoes one of the factors—control over collection and usage personal information—in the IUIPC scale.[96] When empirically validating the CFIP scale, Stewart & Segars observe[97]:

> [A] central concern that seems to underlie consumer attitudes, and is perhaps the common theme captured by the higher-order concept of CFIP, is the issue of control. Consumers desire levels of personalization and customization but also want some sense of control over how this service occurs. (p. 46)

The control-based privacy paradigm is a recurring theme in privacy literature[98], and is supported by empirical studies[99], but has attracted some criticism.[100] Furthermore, although definitions of privacy, such has Westin's[101], consider control as an important dimension of privacy, due in part to the importance of individual autonomy in Western culture[102], Laufer & Wolfe suggest "*the privacy phenomenon is conceptually different*

[95] Norberg et al. 2007.

[96] Malhotra et al. 2004.

[97] Stewart and Segars 2002.

[98] Westin 1967; Altman 1976; Fried 1968.

[99] Sheehan and Hoy 2000; Malhotra et al. 2004.

[100] Allen 2000; Tavani 2007.

[101] Westin 1967.

[102] Laufer and Wolfe 1977.

from control/choice" (p. 39), and that control/choice is actually a mediating variable in the privacy system.

An individual's information control is more than the disclosure or non-disclosure of information, but a decision making process in which an individual considers the future consequences of engaging in a particular behaviour—the "*calculus of behavior*".[103] Laufer & Wolfe suggest new technologies affect this calculus, so an "*individual is often unable to predict the nature of that which has to be managed*" (p. 37).[104] Their idea of a calculus of a behaviour underpins Culnan & Bies' observation that this "*social exchange perspective also applies to a consumer context*" (p. 327)[105], i.e. consumers carry out a similar cost-benefit analysis, or what they refer to as a "*privacy calculus*"—the second most discussed theme in the focus groups. Although this implies people consider to some degree, the risks and benefits of providing personal information, the significant percentage (72 %) of coded quotations in the *Privacy Calculus* theme relating to the benefits offered by a technology service, indicates people are principally focused on the benefits they believe they will receive for disclosing personal information.[106] The fact that the *Consequences* theme only accounted for 6 % of all coded quotations, supports the idea that people do not always consider the medium and long-term consequences of disclosing personal information.

The third most discussed theme in the focus groups—*Trust Cues*—not only included coded quotations relating to *trust symbols* and *trust symptoms*[107], but also environmental cues. Of the coded quotations within the *Trust Cues* theme, 55 % related to environmental cues, including the advice of friends, social and technology norms, and media stories, indicating the possible existence of another component of peoples' privacy concern: *environmental privacy concern*.

Although there was insufficient data to statistically support the research objective of investigating if the factors individuals consider are common to all technology services, analysis of 582 of the total of 599 coded quotations does—*prima facie*—support this. For the four most frequently discussed themes: (1) *Information Control*; (2) *Privacy Calculus*; (3) *Trust Cues*; and (4) *Information Usage*, there was a high incidence of these themes representing more than 9 % of the total coded quotations in each of the focus groups. Furthermore, cogent reasons could be found where less than 9 % of coded quotations in each focus group were related to these particular themes. There was also a reasonably evident grouping of the themes into the other two groups: (1) *somewhat discussed* (i.e. between 3 and 9 % of the coded quotations in each group); and (2) *infrequently discussed* (i.e. between 0 and 3 % of the coded quotations in each group). These exploratory findings suggest it may be feasible to abstract the technology service attributes and environmental cues people typically look for—across disparate technologies.

---

[103] Laufer and Wolfe 1977.

[104] Laufer and Wolfe 1977.

[105] Culnan and Bies 2003.

[106] Acquisti 2004.

[107] Riegelsberger et al. 2005.

Table 13.8 Relationship between significant residuals and personal characteristic categories

	High level of privacy concern		Low level of privacy concern	
	High technology privacy concern[a]	Privacy fundamentalists	Low technology privacy concern[a]	Privacy unconcerned
Trust cues		Less	More	More
Trust	*Less*		Less	
Information usage		*More*	Less	*Less*
Information receiver	Less		Less	*Less*
Security	More	More		

[a] In Table 13.8 those in the *High technology privacy concern* category includes participants who believe privacy will get worse in response to Westin's question on the future impact of technology on privacy, and those whose TPC score was $\geq \mu + \sigma$; all other participants were placed in *Low technology privacy concern* category. The two categories in Table 13.8 use the highest standardised residuals for the Westin and TPC categories

Significant statistical relationships were found between the themes raised and discussed in the focus groups and: (1) the attributes of educational level and computer experience; (2) personal innovativeness in information technology (PIIT)[108]; and (3) general privacy concern (including those measured using Westin's categories). For those cases where a significant statistical relationship was found, examination of the standardised residuals helps to explain the relationship. For example, those in the Westin's Privacy Fundamentalists category made significantly more quotations relating to the *Security* theme than expected, but significantly fewer quotations relating to *Trust Cues* theme than expected. Those categorised as Privacy Unconcerned made significantly more quotations relating to the *Trust Cues* than expected.

Table 13.8 shows the relationship between five themes where there were significantly more or less comments made in the focus groups than expected (i.e. $z > \pm 1.96$)[109], and two different types of users: (1) those with a high level of privacy concern; and (2) those with a low level of privacy concern. The results in Table 13.8 suggest there is potentially a type of person with a high level of general privacy concern, who will attach more importance to a technology service's security, and how their personal information might be used, than the advice of friends. Similarly there may be people who are generally unconcerned about privacy and likely to be influenced in their adoption of technology by social privacy norms or the advice of others.

This suggests it may be feasible, with further research, to identify a richer set of *privacy concern types* for groups of people, representing the technology service attributes and environmental cues which each group consider important and therefore look for. This will assist in understanding how *interpersonal privacy concern* and *environmental privacy concern* are constructed.

[108] Agarwal and Prasad 1998.

[109] Table 13.8 also shows those relationships where there is standardised residual between 1.7 and 1.96 in *faint text*. As this table is the result of quantitative analysis of qualitative data it is considered unrealistic to have an absolute cut-off at 1.96.

The exploratory study did not explore the impact of individuals' personality on their level of privacy concern, i.e. *dispositional privacy concern*. However, the significant statistical relationships between peoples' innovativeness and general level of privacy concern, and the themes raised and discussed in the focus groups suggests certain aspects of peoples' personality is likely to determine the technology service attributes and environmental cues they consider important.

Morton & Sasse[110] propose a layered approach—the Privacy Security Trust (PST) Framework—to assist practitioners with effective privacy practice for both the technology platform and providing organisation within a technology service. The layers within their framework are: (1) information security; (2) information management; (3) information principles; (4) information use; and (5) information privacy culture. It is trust signals from each of the PST Framework layers in a technology service's privacy practice, which will be contextual and assist in the construction of an individual's *interpersonal privacy concern*. For example, the *Information Principles Layer* in the PST Framework should encapsulate fair information practices, echoing the CFIP scale of privacy concern with its emphasis on peoples' concerns about organisations' information privacy practices.[111]

Morton & Sasse suggest the trust signals originating from the organisation's privacy practice may become distorted by a badly designed or implemented technology platform leaking personal information. The fact information control was the most commonly discussed topic in the focus groups, highlights the importance of providing users with feedback and control of their personal information, implemented in the technology platform using the tenets of *privacy by design*[112], and seamlessly linked to the organisation's *Information Management Layer* as defined in the PST Framework.

The qualitative analysis of the focus group transcripts suggests individuals are likely to seek out specific technology service attributes, whose absence, or inadequate implementation, will increase their level of *interpersonal privacy concern*. Similarly, the focus group results suggest individuals also take environmental cues into account, which may increase or decrease their level of *environmental privacy concern*. Finally, the quantitative analysis of the focus groups transcripts and survey data suggest certain individual characteristics influence the technology service attributes and environmental cues people consider important.

Acknowledgements Special thanks are owed to all participants who took time to participate in the focus groups, which formed part of this study. Anthony Morton is funded by a PhD scholarship—part of a UK Engineering and Physical Sciences Research Council (EPSRC) grant (EP/G034303/1)—awarded to the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast.

[110] Morton and Sasse 2012.

[111] Smith et al. 1996.

[112] Cavoukian 2009.

Appendix

Focus Group Technology Service Scenarios

Photograph Sharing Web Site (discussed by Group 1) A photograph sharing web site continually runs a software application, which uses facial recognition technology coupled with information from popular social networking sites, to label ('tag') people in all uploaded photographs. If the picture contains a landmark that the software recognises by searching images on the Internet, this is also labelled. For example, if the picture contains identifiable people and a landmark, the picture will be labelled as '*Mr. Fred Smith and Mrs Jane Jones by Big Ben in London*'. If the picture has meta-data within it, the date and time are extracted and appended to the picture's title, e.g. '*Mr. Fred Smith and Mrs. Jane Jones by Big Ben in London on June 21st at 2:30pm*'.

Organisations that manage landmarks, such as Legoland, Woburn Abbey, Tower Bridge, and Edinburgh Castle etc., can subscribe to a service to be sent photographs of people visiting their landmarks, which they show on their web sites. Users registered with the photograph sharing web site, can sign up to a service to get '*2 for 1*' offers on landmarks similar to the one they have been photographed at, with the coupon being e-mailed to all of the people identified by the software application in the photograph who are registered with the photograph sharing web site (whether they have signed up for the '*2 for 1*' offer or not).

Social Networking Discounts (discussed by Group 2) A social networking site for which users must register and create a profile containing their personal information. Registered users can:

- Link to each other by sending invitations.
- Post status messages about themselves.
- Post messages on other users' pages.
- Send private messages to each other.
- Upload photographs.
- Create and join groups with other users.
- Link to content on the Internet they consider worth looking at.

Users can gain 'social networking credits', which they may use as discounts on products sold on affiliated web sites. The amount of credits is based on a user's amount of use of the social networking site, the number of links with other users they have, and the amount of information about themselves they have entered into their profile.

Supermarket RFID Ordering (discussed by Group 3) A supermarket uses RFID (radio frequency identification) chips, which are not disabled at the supermarket checkout, in the product tags on their food goods.

The supermarket is trialling a new automatic ordering service for shoppers who are registered on their home delivery web site. For a single payment of £ 25 the

registered customer is given a small RFID reader unit, which is placed near their food cupboards and wirelessly connects with the household's broadband router.

This RFID reader unit continually scans the product tags of goods in the cupboards and e-mails a message to the customer, at a selected frequency (monthly or weekly), containing a list of items no longer in the cupboard (and therefore assumed to be used). The customer can click the *Buy Now* button in the e-mail and replacement goods are delivered to the house at the customer's chosen delivery time. Goods purchased using this e-mail automatically attract a discount and also get priority for delivery times.

Smartphone Assistant (discussed by Group 4) A smartphone assistant software application, which monitors an individual's location and provides information about things nearby which may be of interest, including:

- Events (e.g. concerts, theatre, films etc.)
- Places to visit (e.g. museums, parks etc.)
- Shops selling products an individual might be interested in
- Restaurants
- Clearance sales

To ensure the application provides relevant content, individuals must register and enter information about themselves, their interests and lifestyle. The developers of the application provide these details to other companies to allow them to provide targeted advertisements to the registered users' smartphones. If an individual visits a retail outlet, which is part of the scheme, a coupon code flashes up on the screen that can be used to receive a discount at that retail outlet. If an individual has clicked on an advert on their smartphone and ordered goods online they also receive a discount.

Smart Metering (discussed by Group 5) An electricity company offers its customers the opportunity to have a smart meter installed, which sends back details of electricity consumed by taking readings of electricity consumption every half-hour. The readings are sent via the customer's broadband connection to both the electricity infrastructure provider and the electricity supplier. Customers who have a smart meter installed are given a discount on their electricity bill, every quarter.

If a customer has agreed to have a smart meter installed, they are sent updates via e-mail telling them which appliances are inefficient and therefore costing money to run. The electricity supplier, through its relationship with retailers, can offer discounts on household appliances with better energy efficiency. Customers are sent e-mails with adverts offering these appliances.

Landmark Identification Web Site (discussed by Group 6) A smartphone software application which allows individuals to use the camera built into their mobile phone to take a picture of a landmark and request identification of it.

The software uses images from the Internet to identify the landmark, its name being displayed on the smartphone, along with links to relevant web sites providing more information (e.g. opening hours, special events). This information may also include special offers relating to the landmark, such as 2-for-1 tickets, discounted food, private 'behind the scenes' tours etc.

Table 13.9 Types of focus group quotations covered by each theme

Theme name	Types of quotations coded under theme
Advisories	Information and warnings provided by a technology service concerning privacy and data handling
Information management	Individual's perception of how an organisation manages peoples' information once they are in possession of it
Personal characteristics	How an individual's age and personal experience is perceived to affect their use of technology, views on privacy, trust etc
Miscellaneous	General quotations not related to the research questions
Information sensitivity	An individual's view of the information they consider sensitive within the context of a technology service
Perceived ease of use	The effort an individual has to make to use a technology service; design; and whether use is mandatory
Reliance on legislation	An individual's reliance on legislation to protect them, e.g. data protection, consumer protection etc
Sense making	How individuals avoid/minimize privacy invasion, and use previous experiences or similar situations to understand a technology service
Security	The technology service's security, and organisations' physical and information security
Consequences	The impact on an individual's personal security, finances or behavior of using a technology service
Information receiver	Organisations' ability to provide the technology service, its objectives and its characteristics
Trust	Technological and organisational trust
Information usage	Use of information by organisations for location tracking, behavior profiling, and targeted advertising
Trust cues	How individuals use news stories, reviews, third parties etc. to aid their decision to engage with a technology service; social and technological norms; and trust symbols and trust symptoms
Privacy calculus	Individuals' views of the benefits a technology service offers, and the decision process individuals undertake when considering the potential benefits *vs*. private information that has to be provided
Information control	The information control offered by a technology service (e.g. opt-in/opt-out, feedback and control), organisations passing information to third parties without authorisation, and how individuals control information disclosure

The software is free, but to download it and continue using it, you must register and provide links to your profile on social networking sites you use such as Facebook, LinkedIn etc.

This same smartphone software also allows individuals to take a picture of a person on the street, and using facial recognition technology coupled with information from popular social networking sites, provide the name of the person in the picture.

A link is provided to the web site(s) so the user can find out any other publicly available information about the person, such as address, job title etc. (where this can be found).

Qualitative Analysis Themes

During qualitative analysis of focus group transcripts 39 base-level codes were created—grouped into 16 themes—shown in Table 13.9 with a description of the types of quotations coded within each theme.

References

6, Perri, Kristen Lasky, and Adrian Fletcher. 1998. *The future of privacy—Public trust and the use of private information*. Vol. 2. 2 vols. Demos. http://www.demos.co.uk/files/thefutureofprivacyvolume2.pdf.

Acquisti, Alessandro. 2004. Privacy in electronic commerce and the economics of immediate gratification. Presented at the Proceedings of the 5th ACM conference on Electronic commerce—EC '04, New York, NY, USA, 2004, 21, doi:10.1145/988772.988777.

Acquisti, A., and J. Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine* 3 (1): 26–33. doi:10.1109/MSP.2005.22.

Adams, A., and M. Angela Sasse. 2001. Privacy in multimedia communications: Protecting users, not just data. In *People and Computers XV: Interaction without Frontiers*, eds. A. Blandford, J. Vanderdonckt and P. Gray, 49–64. London: Springer.

Agarwal, R., and J. Prasad. 1998. A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information Systems Research* 9 (2): 204–215. doi:10.1287/isre.9.2.204.

Agarwal, Ritu, and Jayesh Prasad. 1999. Are individual differences germane to the acceptance of new information technologies? *Decision Sciences* 30:361–392.

Allen, Anita L. 2000. Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm. *Connecticut Law Review* 32:861.

Altman, Irwin. 1976. Privacy—A conceptual analysis. *Environment and Behavior* 8 (1): 7–29. doi:10.1177/001391657600800102.

Ashford, Warwick. US woman sues google over gmail scanning. *ComputerWeekly.com*, August 11, 2011. http://www.computerweekly.com/news/2240105327/US-woman-sues-Google-over-Gmail-scanning.

Barnett, Emma. Google street view: Survey raises privacy concerns. *Telegraph.co.uk*, March 12, 2010, sec. Technology. http://www.telegraph.co.uk/technology/google/7430245/Google-Street-View-survey-raises-privacy-concerns.html.

Barth, Adam, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. 2006. Privacy and contextual integrity: Framework and applications. In *Security and Privacy, 2006 IEEE Symposium On*, p. 15.

BBC. Google's street view under fire. *BBC News*, July 9, 2008. http://news.bbc.co.uk/1/hi/sci/tech/7498613.stm.

BBC. Google buzz 'breaks privacy laws'. *BBC News*, February 17, 2010. http://news.bbc.co.uk/1/hi/technology/8519314.stm.

BBC. Facebook sorry over tagging launch. *BBC News*, June 8, 2011. http://www.bbc.co.uk/news/technology-13693791.

Beldad, Ardion, Menno de Jong, and Michaël Steehouder. 2011. A comprehensive theoretical framework for personal information-related behaviors on the internet. *The Information Society* 27 (4): 220–232. doi:10.1080/01972243.2011.583802.

Bellman, Steven, Eric J. Johnson, and Gerald L. Lohse. 2001. To opt-in or opt-out? It depends on the question. *Communications of the ACM* 44 (2): 25–27.

Braun, Virginia, and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3 (2): 77–101.

Camp, L. Jean, Helen Nissenbaum, and Cathleen McGrath. 2002. Trust: A collision of paradigms. *Financial Cryptography* 2339:91–105.

Cavoukian, Ann. 2009. *Privacy by Design*. Ontario: Office of the Information and Privacy Commissioner. http://www.ipc.on.ca/images/Resources/privacybydesign.pdf.

Coles-Kemp, Lizzie, Lai Yee-Lin, and Margaret Ford. 2010. *Privacy on the internet: Attitudes and behaviours*. VOME (Royal Holloway—Information Security Group). http://www.vome.org.uk/wp-content/uploads/2010/03/VOME-exploratorium-survey-summary-results.pdf.

Culnan, Mary J., and Robert J. Bies. 2003. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues* 59 (2): 323–342.

Dinev, Tamara, and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17 (1): 61–80. doi:10.1287/isre.1060.0080.

El Emam, K., E. Neri, E. Jonker, M. Sokolova, L. Peyton, A. Neisa, and T. Scassa. 2010. The inadvertent disclosure of personal health information through peer-to-peer file sharing programs. *Journal of the American Medical Informatics Association* 17 (2): 148.

European Commission (EUROPA). Data protection: Europeans share data online, but privacy concerns remain—new survey. *europa.eu*, June 16, 2011. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/742&format=HTML&aged=0&language=EN&guiLanguage=en.

Farrell, Nick. Google admits it sniffed out people's data. *TechEye.net*, May 17, 2010. http://www.techeye.net/security/google-admits-it-sniffed-out-peoples-data.

Federal Trade Commission. 2000. *Privacy online: Fair information practices in the electronic marketplace—A Report to Congress*, May 2000. http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

Federal Trade Commission. 2010. Widespread data breaches uncovered by FTC probe. *Federal Trade Commission*, February 22, 2010. http://www.ftc.gov/opa/2010/02/p2palert.shtm.

Field, Andy. 2009. *Discovering statistics using SPSS*. 3rd ed. SAGE Publications Ltd.

Fiveash, Kelly. 2007. MoveOn tells facebook to stop shining beacon. *The Register*, November 21, 2007. http://www.theregister.co.uk/2007/11/21/facebook_moveon_privacy_beacon/.

Fried, Charles. 1968. Privacy. *The Yale Law Journal* 77 (3): pp. 475–493.

Gefen, David, Elena Karahanna, and Detmar W Straub. 2003. Trust and TAM in online shopping: An integrated model. *MIS Quarterly* 27 (1): pp. 51–90.

Harper, J., and S. Singleton. 2001. *With a grain of salt: What consumer privacy surveys don't tell us*. Competitive Enterprise Institute & The Cato Institute, June 2001. http://www.slis.indiana.edu/faculty/hrosenba/www/l574/pdf/harper_privacy-surveys.pdf.

Hundley, Heather L., and Leonard Shyles. 2010. US teenagers' perceptions and awareness of digital technology: A focus group approach. *New Media & Society* 12 (3): 417–433. doi:10.1177/1461444809342558.

Johnson, M. Eric. 2008. Information risk of inadvertent disclosure: An Analysis of file-sharing risk in the financial supply chain. *Journal of Management Information Systems* 25 (2): 97–124.

Junglas, Iris A, Norman A Johnson, and Christiane Spitzmüller. 2008. Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems* 17 (4): 387–402. doi:10.1057/ejis.2008.29.

Kitzinger, Jenny. 1995. Introducing focus groups. *BMJ: British Medical Journal* 311 (7000): 299–302.

Korzaan, Melinda L., and Katherine T. Boswell. 2008. The influence of personality traits and information privacy concerns on behavioral intentions. *The Journal of Computer Information Systems* 48 (4): 15–24.

Kumaraguru P. and L. F. Cranor. 2005. Privacy Indexes: A Survey of Westin's Studies. *Technical Report CMU-ISRI-05–138,* Institute for Software Research International, School of Computer Science, Carnegie Mellon University, December.

Laufer, Robert S., and Maxine Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33 (3): 22–42.

Leavitt, Lydia. 2011. Mobile app makers probed over privacy concerns. *TG Daily*, April 5, 2011. http://www.tgdaily.com/business-and-law-features/55204-mobile-app-makers-probed-in-privacy-investigation.

Liu, Chang, Jack T. Marchewka, June Lu, and Chun-Sheng Yu. 2005. Beyond concern—A privacy-trust-behavioral intention model of electronic commerce. *Information & Management* 42 (2): 289–304. doi:10.1016/j.im.2004.01.003.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15 (4): 336–355. doi:10.1287/isre.1040.0032.

McKnight, D. Harrison, and Norman L. Chervany. 2001. "What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology." *International Journal of Electronic Commerce* 6 (2): 35–59.

McKnight, D. Harrison, Vivek Choudhury, and Charles Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research* 13 (3): 334–359.

Mennecke, Thomas. 2007. Pfizer P2P security breach. *Slyck News*, June 20, 2007. http://www.slyck.com/story1496_Pfizer_P2P_Security_Breach.

Metzger, Miriam J. 2004. Privacy, trust, and disclosure: Exploring barriers to electronic commerce." *Journal of Computer-Mediated Communication* 9 (4). doi:10.1111/j.1083–6101.2004.tb00292.x.

Mills, Elinor. 2007. Google's street-level maps raising privacy concerns. *USA Today*, June 4, 2007. http://www.usatoday.com/tech/news/internetprivacy/2007–06-01-google-maps-privacy_N.htm.

Morgan, D. L. 1996. Focus groups. *Annual Review of Sociology* 22:129–152.

Morgan, David. L, and Richard A. Krueger. 1993. When to use focus groups and why. In *Successful focus groups: Advancing the state of the art*, Vol. 1. Sage Publications, Inc, pp. 3–19.

Morton, Anthony, and M. Angela Sasse. 2012. Privacy is a process, not a PET: A theory for effective privacy practice. In *Proceedings of the 2012 Workshop on New Security Paradigms*, 87–104. NSPW '12. New York, NY, USA: ACM, 2012. doi:10.1145/2413296.2413305.

NBC. 2009. New warnings on cyber-thieves. *TODAY Investigates*. United States: NBC, February 26, 2009. http://www.today.com/id/26184891/vp/29405819#29405819.

Nissenbaum, Helen. 2004. Privacy as contextual integrity. *Washington Law Review* 79 (1): 119.

Nissenbaum, Helen. 2011. A contextual approach to privacy online. *Daedalus* 140 (4): 32–48.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41 (1): 100–126. doi:10.1111/j.1745–6606.2006.00070.x.

Panzarino, Matthew. 2011. It's not just the iphone, android stores your location data too. *TNW—The Next Web*, April 21, 2011. http://thenextweb.com/google/2011/04/21/its-not-just-the-iphone-android-stores-your-location-data-too/.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing* 19 (1): 27–41. doi:10.2307/30000485.

Quinn, Ben, and Charles Arthur. 2011. PlayStation network hackers access data of 77 million users. *The Guardian*, April 26, 2011. http://www.guardian.co.uk/technology/2011/apr/26/playstation-network-hackers-data?intcmp=239.

Riegelsberger, Jens, M. Angela Sasse, and John D. McCarthy. 2005. The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies* 62 (3): 381–422.

Rotter, Julian B. 1967. A new scale for the measurement of interpersonal trust. *Journal of Personality* 35 (4): 651–665. doi:10.1111/j.1467–6494.1967.tb01454.x.

Sarno, David. 2010. Apple collecting, sharing iphone users' precise locations [Updated]. *Los Angeles Times*, June 21, 2010, sec. Business. http://latimesblogs.latimes.com/technology/2010/06/apple-location-privacy-iphone-ipad.html.

Sheehan, Kim Bartel. 2002. Toward a typology of internet users and online privacy concerns. *The Information Society* 18 (1): 21–32. doi:10.1080/01972240252818207.

Sheehan, Kim Bartel, and Mariea Grubbs Hoy. 2000. Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing* 19 (1): 62–73.

Skinner, Harvey, Sherry Biscope, Blake Poland, and Eudice Goldberg. 2003. How adolescents use technology for health information: Implications for health professionals from focus group studies. *Journal of Medical Internet Research* 5 (4). doi:10.2196/jmir.5.4.e32.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* 20 (2): 167–196.

Snell, K., J. Starkbaum, G. Lauß, A. Vermeer, and I. Helén. 2012. From protection of privacy to control of data streams: A focus group study on biobanks in the information society. *Public Health Genomics* 15 (5): 293–302. doi:10.1159/000336541.

Stewart, Kathy A., and Albert H. Segars. 2002. An empirical examination of the concern for information privacy instrument. *Information Systems Research* 13 (1): 36–49.

Tan, Felix B., and Paul Sutherland. 2004. Online consumer trust: A multi-dimensional model. *Journal of Electronic Commerce in Organizations (JECO)* 2 (3): 40–58.

Tavani, Herman T. 2007. Philosophical theories of privacy: implications for an adequate online privacy policy. *Metaphilosophy* 38 (1): 1–22. doi:10.1111/j.1467–9973.2006.00474.x.

TechCrunchTV. Crunchies Awards 2010. *Mike Arrington Interrogates Mark Zuckerberg*. Las Vegas, January 9, 2010. http://static-cdn1.ustream.tv/swf/live/viewer:55.swf?vid=3848950&vrsl=c:170.

Venkatesh, Viswanath, and Michael G. Morris. 2000. Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly* 24 (1): 115–139.

VOME. 2012. Citizen-centric privacy by design. http://www.vome.org.uk/wp-content/uploads/2012/06/citizen-centric-privacy-by-design.pdf.

Westin, Alan F. 1967. *Privacy and freedom.* [1st ed.]. New York, NY, USA: Atheneum.

Zhang, Harry, Claudia Guerrero, David Wheatley, and Young Seok Lee. 2010. Privacy issues and user attitudes towards targeted advertising: A focus group study. In *Human Factors and Ergonomics Society Annual Meeting Proceedings*, 54:1416–1420.