emerald PUBLISHING

Journal of Services Mar

Trust and its predictors within a cyber-physical system context

Journal:	*Journal of Services Marketing*
Manuscript ID	JSM-01-2018-0007.R4
Manuscript Type:	Article
Keywords:	Internet of Things, Trust, Service systems

Trust and its predictors within a cyber-physical system context

Abstract

Purpose

This research aims to provide empirically derived insights into trust and its predictors within a cyber-physical system context of a household service.

Design/methodology

The methodology comprises an innovative mixed methods design encompassing a videographic animated film portraying a potential 'slice of life' household service system scenario that was subsequently incorporated into a quantitative survey. A total of 400 responses were then used to examine trust dimensions and their hypothesized predictors.

Findings

Findings suggest trust is two dimensional with 'online networking competency', 'perceptions of risk', 'propensity to trust technology in general' and 'concerns about security' being significant predictors. Surprisingly, 'concerns about privacy' does not have a significant effect.

Originality/value

The contribution of this research is twofold. Firstly, from a theoretical perspective, the paper offers empirical insights into trust and its predictors within a cyber-physical system context of a household service. Secondly, and from a pragmatic perspective, the model derived from this study may aid practitioners in developing trust strategies and trust management systems within such contexts.

Key words

Internet of Things (IoT), service systems, trust, cyber-physical systems (CPS)

Introduction

Contemporary research within the services marketing field continues to recognise the role that the evocation of trust plays in determining the success or otherwise of relationships between actors (e.g., Morgan and Hunt, 1994: Chesney, Chuah, Dobele and Hoffmann, 2017). However, technological advancements question the transferability and appropriateness of established models and concepts to new and emerging service contexts (e.g., Bansal, Zahedi and Gefen, 2016). The all-pervasive but inconspicuous nature of many emergent technologies creates potentially new dimensions of complexity with actors (machine and human) working collectively as adaptive socio-technical service systems (e.g., Fritsch, Groven and Schulz, 2012). Consequently, the nature of trust may differ according to the agency of human actors and machine objects within these technologically advanced service systems (Engen, Pickering and Walland, 2016). One such technologically advancing context for service systems is the Internet of Things (IoT), a term first coined in 1999 (Ashton, 2009).

The IoT comprises single 'things' each with a unique identifier that can be accessed anywhere, anytime via the internet. Things may have the capability to collect and store data as well as share data with other things (Ashton, 2009). Things connected together via the internet constitute the IoT and their coordinated actions in certain contexts become an IoT system (Minerva, Biru and Rotondi, 2015). IoT systems can also be connected together, growing into a 'cyber-physical system' (CPS). A CPS may be defined as a "*network of interacting appliances with physical inputs and outputs instead of standalone devices*" (Minerva et al, 2015:71). There is no clear technical point at which an IoT system becomes a CPS, and indeed the terms are often used interchangeably in the literature, suffice to say that the primary focus from a consumer experience perspective is the provision of services rendered possible by IoT systems as they become a CPS (e.g., Yan, Zhang and Vasilakos, 2014). Within this rapidly evolving field, Cisco predicts the global IoT market will be worth US$14.4 trillion by 2022 with the number of connected devices growing from 22.9 billion in 2016 to 50.1 billion by 2020. The majority of this expenditure will be invested in improving customer experiences and services (Mandler, Antonelli, Kleinfeld, Pedrinaci, Carrera, Gugliotta and Villares, 2013). Such services will be ubiquitous, enabling "*new ways of working; new ways of interacting; new ways of entertainment and new ways of living*" (Miorandi, Sicari, De Pellegrini and Chlamtac, 2012:1497). However, research that focuses on individuals entering relationships with IoT and CPS systems has generally been neglected (e.g., Nass, Fogg and Moon, 1996; Ng and Wakenshaw, 2017). If the enormous potential of such systems is to be fulfilled, an in-depth understanding of customer perceptions and behaviours is crucial in overcoming issues related to the effective implementation of IoT system enabled services (e.g. Wünderlich et al, 2015; Medina-Borja, 2015). Consequently, theoretically and empirically based examinations of trust within such contexts are warranted. To this end, this paper reports on an investigation that focuses on the potential nature of trust based on data collected from target consumers in an everyday home-life context: a household CPS. The contribution of this research is twofold. Firstly, from a theoretical perspective, the paper synthesizes trust predictors and constructs relevant to emergent CPS contexts. It offers empirically derived insights into trust dimensions and presents a novel approach for evaluating new service systems. Secondly, from a pragmatic perspective, the empirical model developed through the research processes may be useful for practitioners attempting to develop trust management strategies for CPS contexts.

The paper is structured as follows: initially, we provide an overview of the extant literature on CPS that leads us to question the appropriateness of traditional models of trust within such systems. The rest of the paper presents findings of a two-step research process. In the first

step, we review service systems and trust literatures, presenting a synthesis of relevant conceptual attributes and predictors of trust within CPS. The methodology is described and results of an exploratory analysis of trust dimensions are reported. Results of EFA are subsequently used to inform a second step that is then presented. In the second step, predictors of the trust factors are tested. Thereafter, findings are outlined and discussed before conclusions are drawn that highlight future directions for research and managerial implications in this domain.

Literature Review

Service Systems and CPS

Service systems may be defined as "*configurations of people, technologies, organisations and shared information able to create and deliver value to providers, users and other interested entities through service*" (Maglio and Spohrer, 2008:18). IoT systems deliver value through 'smartness', often ascribed as a consequence of the nature of software and hardware that enables 'machine generated' (algorithmic) optimized performance capability based on information shared between interconnecting devices (e.g., Abdel-Basset, Manogaran and Mohamed, 2018). The notion of 'smart everything', underpinned by IoT systems, is predicted to improve worldwide wellbeing through the development of increasingly complex service systems (e.g., Medina-Borja, 2015; Perera et al, 2014; Barile and Polese, 2010). However, the impacts of the new service systems on actors and service landscapes are yet to be fully explored particularly given their "*interactive, contextual, systemic, experiential and relational nature*" (e.g., Gustafsson et al., 2016:10; Royal Society, 2017). Interpretations of service and its provision may need to evolve so as to align with the blurring boundaries between physical objects and services provided to the extent that *"every static and discrete object could have the opportunity of becoming a pseudo-provider*" (Medina-Borja, 2015:ii), aligning with the computer science perspective of a CPS. From a consumer perspective, everyday devices will exhibit what may be increasingly interpreted as agency through perceived smartness (Bandura, 2001; Rose and Truex, 2000; Engen *et al*, 2016). Washing machines, ovens and toasters become 'active' partners in evolving service systems through the information the devices generate and share with other agents (Hoffman and Novak, 2016). Consequently, illusions of self-awareness, flexibility, transformability and self-decisiveness may be evoked (Atzori, Iera and Morabito, 2010; Gubbi, Buyya, Marusic and Palaniswami, 2013; Yang, Yang and Plotnick, 2013). 'Smart homes' consisting of such devices will be increasingly viewed as a CPS, leading to significant changes in the way that consumers experience everyday activities (Hoffman and Novak, 2016) and how they manage their lives, homes and social environments.

As IoT systems become CPS, the services they enable will increasingly involve relationships between a diversity of actors (Gummesson and Grönroos, 2012). These include a growing number of household devices as outlined above with other customers, businesses, public services and software (e.g., Frow *et al*., 2014). Actors will collectively coordinate their behaviour as a complex adaptive system (e.g., Mele and Polese, 2011; Chandler and Lusch, 2015; Engen *et al*., 2016) where new 'entities' (human and non-human actors) will be continually joining and leaving the CPS to ensure service and experiential optimization (Ng and Wakenshaw, 2017:6). From a networked actor's perspective (e.g., a customer), they will likely be unaware of the full extent of their role or the range or scope of activities encompassed within the CPS they are interacting with that delivers their service experiences. This may have significant consequences on the appropriateness of established trust models within such contexts. Thus, trust and its likely role is now considered.

Theoretical foundations of trust for CPS

Within traditional exchange perspectives of marketing, trust is an antecedent of calculative commitment (e.g., Morgan and Hunt, 1994). As a result, structural bonding between a firm and customer is composed of financial (price), social (communications) and structural (value-in-use) constituents (Chou, 2009). If positive cognitive and emotional outcomes are realized (Park, Jaworski and MacInnis, 1986), satisfaction with the value proposition and subsequent relational commitment may be attained (see Seppänen, Blomqvist and Sundqvist, 2007, for a summary of the literature in this area). However, within a CPS context there may no singular service provider (human or machine) on which consumers may focus trust decisions (Bao and Chen, 2012). Instead, such service systems comprise closely linked and distally networked businesses, public services, customers, devices, objects, machines and software (Frow *et al*., 2014) all interacting collectively to provide an integrated service experience. To add to this complexity, the boundaries between interpersonal and technological characteristics, attributes and interactions become blurred for a customer. For example, data derived from interactions are simultaneously used and re-used in real-time by multiple actors (devices, objects, third parties, etc.). These extend and bind customers to relationships within the CPS beyond the initial touchpoint with whom the customer believes they are interacting. Ultimately, there is simply too much information for an individual consumer to physically process (Lobler, 2014) and so they have limited ability to evaluate the performance of the CPS, its actors or indeed, any potential alternatives that may exist. Trust is thereby an essential constituent of the consumer's engagement with a CPS context.

Within the technology literature, McKnight, Carter, Thatcher and Clay (2011) suggest that trust situations *"arise when one has to make oneself vulnerable by relying on another person or object, regardless of the trust object's will or volition*" (p.123). In conceptualizing trust in CPS contexts, we draw on McKnight *et al.'s* (2011) framework that synthesizes interpersonal and technology based trust constructs relating to contextual conditions and the nature of trustor expectations and object attributes. Extrapolating this, a trust-based CPS is one where the interactive context is complex and involves multiple actors in simultaneous and/or coordinated actions, each interdependent upon the others in the system (Skopik, Schall and Dustdar, 2010; Su, Zhang, Mu and Bai, 2013; Yan, Zhang and Vasilakos, 2014; Harwood and Garry 2017). Thus, a further dimension to McKnight et al's (2011) framework is added that relates to an object of dependence within a CPS context (see Table 1). Within social sciences literature, trust is frequently posited in terms of "*accepted vulnerability to another's ill will (or lack of good will)*" (Friedman *et al.,* 2000). As such, different service contexts may involve risk and uncertainty that contribute towards varying degrees of control over an outcome regardless of whether the object of trust is a person, device or a CPS. Consequently, levels of trust may be affected intentionally through the moral choice of a person, or through a failure by a machine or device to act as expected (McKnight *et al.*, 2011). Within a CPS that comprises multiple IoT systems and actors, failure may occur through a combination of any number of interconnections. That said, the nature of trust will vary according to the nature of the object of dependence.

While interpersonal trust comprises moral dimensions (e.g., Berscheid, 1993), with technological trust there is a lack of any moral agency (McKnight *et al.*, 2011). As a result, trust reflects perceptions of the attributes of the technology (McKnight *et al.*, 2011). However, given the potential nature of a CPS context and the multiplicity of objects involved, there may be no obvious central or identifiable object on which to base trust decisions. By way of example, consider a service touchpoint that may be a smart mobile device-based app that provides information about energy consumption and predicted use. The data is derived

from a range of technologies and services embedded into third party devices around the home, with data collected and analyzed by multiple monitoring services, possibly compared to other service providers' datasets before information is ultimately provided to the app service firm. Within such a complex CPS, it is easy to suggest that trust is attributed to the app firm or even the smartphone manufacturer, but these are clearly just two of many actors in the CPS that provide coordinated actions upon which the consumer's trust decisions are based. In turn, decisions made are a consequence of different priorities, perceptions and expectations of objects as a CPS (Mayer, Davis and Schoorman, 1995; McKnight *et al.*, 2011).

Insert Table 1 about here

Reflecting on the breadth of theories of trust, usefully summarised in Seppänen, Blomqvist and Sundqvist (2007), this research draws on those relevant theories of trust identified in the preceding discussion (e.g., Skopik, Schall and Dustdar, 2010; McKnight *et al*., 2011; Su, Zhang, Mu and Bai, 2013; Yan, Zhang and Vasilakos, 2014; Harwood and Garry, 2017). Relevant trust constructs for a CPS context are identified as familiarity and understanding of the CPS by consumers; the reliability, predictability and consistency of the system; security of the CPS; its integrity; the competence, expertise and functionality required to interact with the CPS; the benevolence and helpfulness of the CPS for consumers; the extent to which it can be personalized; and, the faith and belief consumers have in the service delivered. Each of the constructs is now discussed in relation to the CPS context.

(i) Familiarity and understandability

Familiarity and understandability of an individual's traits and a comprehension of how these may manifest themselves when interacting with them is necessary for interpersonal trust to develop (Rempel, Holmes and Zanna, 1985). Within technological contexts, it is the user's cognizance of the processes and procedures adopted by a technological entity that evoke familiarity and understanding (Madsen and Gregor, 2000). Within CPS contexts, the consumer's familiarity and knowledge of the entire system may be limited because of the complexities previously outlined. Consequently, familiarity and understandability of other service systems and technology is drawn upon to form "*a mental model of a system and consequently being able to predict its future behaviour*" (Janson *et al*., 2013:5) that enables consumers to form trust judgements (Söllner *et al*., 2014).

(ii) Reliability, predictability and consistency

Individuals, to varying degrees, are capable of acting in an impulsive and irrational manner. Reliability, predictability and consistency are the extent to which individuals are judged to act in a predictable manner (McKnight *et al*., 2011). Technology may also act in an erratic and unreliable manner (McKnight *et al*., 2011). When considering a CPS, Cho *et al*. (2015) and McKnight *et al.* (2011) propose that reliability refers to an expectation that the system will operate in a predictable and consistent manner.

(iii) Security

Security within an interpersonal context refers to the belief that information of a personal or sensitive nature that is shared with another individual is not deliberately or inadvertently disclosed to third parties (Sheppard and Sherman, 1998). Within technology contexts, security refers to protective digital privacy measures such as authentication, encryption and

non-repudiation that are applied to prevent unauthorised data access (e.g., Cheung and Lee, 2001). Within a CPS context, security refers to how secure a service consumer perceives the system to be in terms of *"collecting and transmitting sensitive information*" (Salisbury *et al*., 2001). This encompasses unauthorised disclosure or use by third parties as well as malicious access to personal data by third parties.

(iv) Integrity

Within interpersonal contexts, integrity refers to assumptions about credibility, fulfilment of promises and honesty (Sekhon, Ennew, Kharouf and Devlin, 2014). When considering technology contexts, data integrity is a consumer's belief that rules or procedures pertaining to their personal data are such that it will not be used in a particular manner or altered without their notification and consent (e.g., Pfleeger and Pfleeger, 2011). Within a CPS context, integrity is perceived to be a reasonable adherence to processes and procedures regarding the management of personal data within the system.

(v) Competence, expertise and functionality

Perceptions of competence relate to the capacity an individual is believed to possess that enables them to achieve a particular outcome (Sekhon *et al*., 2014). Within technology contexts, it is the attributes that a device is believed to possess that enhances its perceived capability to complete a particular task (McKnight et al., 2011). Thus, competence, expertise and functionality refer to the perceived ability of a CPS to achieve a particular outcome or number of outcomes for consumers.

(vi) Benevolence and helpfulness

Benevolence and helpfulness refers to the notion of 'acting in the other party's interests' (Mayer *et al.* 1995) and draws on a moral and volitional capability that culminates in a lack of opportunistic behaviour (Morgan and Hunt, 1994). However, within technology contexts these are harder to ascribe. Helpfulness becomes instrumental because of a lack of moral agency (Beatty, Reay, Dick, and Miller, 2011). As a result, help is interpreted as the propensity of a device to proffer the necessary advice to complete a task when requested usually through a 'help' function (McKnight *et al.,* 2011). From a CPS perspective, benevolence and helpfulness are the consumer's perception that the system will holistically act in their best interest and provide advice when necessary or requested to do so.

(vii) Personalization

Intimate interactions between individuals within an interpersonal context will frequently result in individualised, distinctive and reciprocal responses that are 'caring' in nature (Rempel, Holmes and Zanna, 1985). From a technology perspective, personalization refers to the extent to which an object 'interprets and represents' the personal needs of a consumer (Komiak and Benbasat, 2006). Drawing on Chen's (2012) notion of "*Only here, only me and only now*", within a CPS context, the interpretation of a service consumer's needs and the reasoning processes related to these generates a perception of personalised service provision (e.g. Söllner *et al*., 2014).

(viii) Faith/Belief

At an interpersonal level, faith refers to confidence or belief in the ability of another to perform. It is usually based on non-rational criteria (Castelfranchi and Falcone, 2010) and may be evoked by evidence, signs or experience (Cho, Chan & Aldi, 2015). From a technology perspective, Madsen and Gregor (2000) refer to confidence as the belief that an object or device will perform even in situations where it is unproven. Within a CPS context,

faith may be based on limited understanding and/or familiarity with a system but a belief that it will perform appropriately nonetheless.

In addition, potential predictor constructs of trust for a CPS context are identified. We next describe the theoretical foundations of the trust predictors.

Theoretical foundations of predictors of trust within a CPS

It has long been recognised that consumers possess different levels of ability to form expectation and performance assessments about services. When making such assessments, consumers draw on their qualifications, skills, knowledge, intuition and experiences (Hanlon, 1997). Driven by an ethos that recognises that consumers are becoming increasingly familiar with their technologically-networked worlds encompassing "*relations of collaborations, participation, dispersion and distributed expertise*" (Lankshear and Knobel, 2006:27), consumers are now "*better informed, connected, capable and empowered*" (Macdonald and Uncles, 2007:498). Drawing on the ancient Greek notion of *metis* (knowledge, cunning, know-how, practical skills and common sense), Macdonald and Uncles (2007) coined the phrase 'consumer savviness' to describe the "*array of practical skills and knowledge* [consumers apply] *to respond to a constantly changing networked environment*" (Macdonald and Uncles, 2007:499). Consequently, whilst consumers may have no direct experience of new and emerging CPS contexts, they are in a position to draw on a breadth of practical skills, knowledge and experience of technologies and devices in general to formulate risk assessment and trust decisions based on their intuitive logic (Alford and Sherrell, 1996:73). Taking this into consideration, the technology acceptance model (TAM) and its variants (eg., Davis, 1993; Venkatesh and Davis, 1996, 2000) were not deemed to be relevant to the current study: usability and acceptance of technology were considered to be embedded in the experience environment of everyday devices which form the basis of an IoT system, such as commonplace household electrical goods. Building on McKnight et al. (2011) and Harwood and Garry (2017), five constructs were identified that may predict trust decisions in CPS contexts. These are propensity to trust technology in general; a generalised perceived risk of using technology; consumers' online networking competency; consumers' concerns about privacy; and, consumers' concerns about security (see Table 2 for a summary of the key literature). We next consider each of these in relation to CPS contexts.

Insert Table 2 about here

(i) Propensity to trust technology in general

Drawing on research by Mayer, Davis and Schoorman (1995) and McKnight, *et al.* (2011), an individual's trusting stance in technology in general refers to the extent to which consumers "*are willing to depend on technology across a broad spectrum of situations and technologies*" (McKnight *et al*., 2011:6). Pertinent to this research, 'propensity' is neither trustee nor situation specific but transcends a service context and is experientially based. Thus, a consumer's disposition to trust technology in general may be applied to new and emergent technologies such as a CPS context.

(ii) Generalised perceived risk of using technology

Generalised perceived risk of using technology is experientially based and may be defined as "*uncertainty resulting from the potential for a negative outcome*" of using technology (Norberg, Horne and Horne, 2007:106). This encompasses the perceived likelihood of a

negative event occurring (Paul and Tarpey, 1975). Therefore, negative experiences of technology in general may be used to predict consumers' disposition towards new and emergent technologies such as a CPS context.

(iii) Online networking competency

Online networking competency is the ability of consumers to tap into collective knowledge in order to make better and more informed decisions. Macdonald and Uncles (2007) propose that consumers are continually exposed to new ideas and perspectives online, which may subsequently influence their '*mental states and behaviours*'. Thus, competency is likely to positively predict trust in a CPS context based on consumers' self-confidence and experience of online networking.

(iv) Concerns about privacy

Privacy is defined as control over information disclosure and use specifically in relation to the duplication and sharing of information for secondary use. Secondary is "*information provided for one purpose that is re-used for unrelated purposes without the individual's knowledge or consent*" (Culnan and Armstrong, 1999:106). Secondary use is likely to be the underpinning premise of many service innovations operating under the Open Data Initiative (www.theodi.org). Trust reflects a willingness to assume risks of disclosure (Mayer *et al*., 1995). The link between privacy and trust has long been established in both online (e.g., Mukherjee and Nath, 2007) and offline (e.g., Damschroder *et al.*, 2007) contexts. However, rapidly evolving technologies such as IoT have changed the privacy landscape (Peltier, Milne and Phelps, 2009; www.eugdpr.org). To date, most privacy-based research has focused on internet usage and direct marketing (Peltier, Milne and Phelps, 2009) and has empirically demonstrated how concerns over privacy issues impact negatively on trust in online contexts (e.g., Schlosser, White and Lloyd, 2006). The invisible and continuous nature of information exchange in relation to sensing, actuating, computational and communicative processes within IoT systems and CPS contexts is unlikely to mitigate this given privacy concerns may be a function of past experiences (Rixon, Hirani, Cartwright, Beynon, Selva, Sanders and Newman, 2013; Acquisti, Taylor and Wagman, 2016). Additionally, individual consumers differ in their general concerns about privacy (Klang, 2006; Kumaraguru and Cranor, 2005). Interestingly, computer scientists assess privacy based on stringent technology solutions and legal protocols, which are considered secondary to consumer perceived assessments (Pavlou and Chellappa, 2001). Overall, however, concerns about privacy are predicted to negatively affect trust in a CPS context.

(v) Concerns about security

Within technology contexts, security is generally accepted as referring to the safety of personal information and control over unwanted intrusions (Bart, Shankar, Sultan and Urban, 2006). Data security has been empirically proven to be of increasing concern to many individuals (e.g., Salisbury, Pearson, Pearson and Miller, 2001). Regardless of the extent to which organizations implement security measures based on technology solutions and/or legal guidelines, however, it is individual perceptions of security that are important in evoking trust (e.g., Mukherjee and Nath, 2007). Thus, concerns about security will negatively affect the trust in a CPS context.

Drawing on these theories of trust, the research aims to explore how the five predictors and eight dimensions of trust identified relate to a CPS context. The literature review led us to conceptualize the research framework in Figure 1. In the next section, we describe the

methodology used to operationalize a research design for an emergent CPS context and evaluate the relevance of the constructs and predictors identified.

Insert Figure 1 about here

Methodology

In designing the research, it was crucial that the inconspicuous but all-pervading nature of potential applications of technology within a CPS context should be captured and communicated in an appropriate and realistic way. To address this challenge, a three-phase approach was adopted: first, scoping potential IoT systems for a CPS context; second, developing and testing a scenario based on these, and third, conducting a quantitative survey using the identified trust-based constructs.

To enable respondents to visualise the characteristics and complexity of a CPS context that does not currently exist is problematic and traditional research methods into the nature of consumer behaviours are therefore inadequate. To address this, this research drew on the filmic approach of storytelling within contemporary consumer culture (e.g., Belk and Kozinets, 2005; Schembri and Boyle, 2013). A videographic process was adopted to devise projective materials with which to engage consumers in discussions (Sayre, 2001; Belk and Kozinets, 2005). Potential IoT technologies were identified from a systematic scoping of technology product developments and classified through a process of collating 'found images' (Pink, 2007; Pauwels, 2011). A CPS within a household context was selected as the evidence from this exploratory phase of the research corroborates previous research into IoT systems suggesting this will be a pioneering field in service applications (e.g., Terpening and Littleton, 2017). A storyboard and script were devised that depicted potential IoT technologies in use within a CPS household and home-based context. Next, pre-testing of the devised scenario was conducted to evaluate the relevance and realism of the CPS context identified. A focus group of 15 researchers and industry participants with different disciplinary interests (science, technology, arts and marketing) and levels of knowledge and experience of IoT developments and applications reviewed the proposed storyboards and scripts and provided feedback. An experienced film producer/director was briefed to translate the storyboard and script into a short animated film (created in Second Life®). In addition, an introductory film was made that presented the characters in the scenario to research participants. The script, together with examples of screenshots from the scenario, may be seen in Appendix 1. A link to the films was subsequently embedded as a projective tool into the survey instrument.

The research instrument comprised three key parts. The first section consisted of classification questions. The second section comprised the pre-existing and validated items for each of the trust constructs identified in the literature: understandability (Madsen and Gregor, 2006), reliability (McKnight *et al*., 2011), security (Salisbury *et al*., 2001), integrity (Mcknight, *et al*., 2002), competence (Mcknight *et al*., 2002), benevolence (Bhattacherjee, 2002), personalization (Komiak and Benbasat, 2006) and faith (Madsen and Gregor, 2006). The final section comprised pre-existing and validated items related to the proposed predictors of trust. Specifically these were: online networking competencies (Macdonald and Uncles, 2007); risks of using technologies (Yan, Zhang and Vasilakos, 2014); trust in technologies (McKnight *et al*., 2002) and concerns about privacy and security (Smith, Milberg and Burke, 1996). All items were measured using a five-point likert scale. The

survey instrument may be seen in Appendix 2. Employing a market research agency, a quota sampling process was used to ensure a representative sample was recruited in terms of age and gender (over 18s only). The data were collected using an online interface (Deutskens, De Ruyter and Wetzels, 2006). In total, 400 usable responses were collected and analysed.

Analysis and results

Preliminary analysis of respondents' perceived realism of the projective films and scenario identified 88.3% of participants considered '*Introduction to the Walker Family*' to be 'realistic' or 'very realistic' and 88.5% of participants considered the Household Management System film to be 'realistic' or 'very realistic'. These values were considered sufficiently high to undertake further detailed analyses. Given the unique nature of the CPS context and the fact that these constructs had never been explored together within such a context, an examination of the nature of the relationships between them was considered necessary. The bivariate correlation table suggested a number of items to be moderately or highly correlated with a significant number of *r* values of .50 or higher (Cohen, 1988). This suggested issues with discriminant validity (Bagozzi *et al*., 1988) (see Appendix 3). Alpha tests conducted on the original scales ranged from .644 to .88. Consequently, an Exploratory Factor Analysis (EFA) was conducted to identify potential underlying dimensions within the data. Prior to this, checks were carried out to ensure the appropriateness of the data for EFA. An examination of the correlation matrix identified the presence of a significant number of coefficients of .3 or above. Bartlett's Test of Sphericity (Bartlett, 1954) was statistically significant and the Kaiser-Meyer-Olkin (KMO) value (.955) exceeded the recommended value of .6 (Kaiser, 1970). The EFA resulted in a two-factor solution accounting for 61.3% of the variance. All items loaded significantly. However, one item cross-loaded ('*The HHM system would be honest'*) and this item was removed from further analysis. Factor 1 accounted for 55.0% of variance and Factor 2 accounted for 6.3% of the variance (see Appendix 4). The reliability was checked using Cronbach's alpha. Factor 1 and Factor 2 alpha scores were 0.912 and 0.847 respectively. As these are above 0.7, they may be considered reliable for this sample.

Discussion of EFA findings

The two-factor result was surprising given the literature review had identified eight constructs for trust relevant to CPS contexts. That said, within unfamiliar contexts, consumer understanding decreases and imperfect knowledge exists albeit the majority of household devices portrayed within the scenario were familiar. However, they are familiar as stand-alone devices performing specific functions such as fridges, dishwashers, washing machines and vacuum cleaners, not as IoT connected devices that provide additional functionality through their interaction with third parties, or as interconnected devices that may provide a collective service. At one level, respondents are comfortable with the notion of how these devices operate and how they should perform as well as the criteria they would use to assess their performance. However, at another level, participants are unfamiliar with how such devices would function as part of a wider CPS. This gives rise to the perceived complexity of a service system that comprises a range of human and machine actors that are continually interacting with each other. Thus, the criteria by which the participants assessed such a system's performance is uncertain. For this reason, we believe that familiarity and understanding are no longer separate trust dimensions. Understandability and familiarity, together with the ability to gauge the performance of the system, are therefore perceived as being interrelated and so load together on to one factor. We have labelled this trust dimension 'Experiential Based Performance Assessment' or EBPA to reflect the notion that familiarity and understanding derive from experience. The second factor is characterised by items

related to acceptance, commitment, security, truth and honesty, and reflects a generalized confidence or faith that the holistic household service system will perform appropriately. We have labelled this dimension 'Constancy' to reflect the notion that the system will be trustworthy in terms of being '*unchanging or unwavering as in purpose, loyalty or faithfulness*'. In effect, we believe the Constancy dimension reflects a perception of the persistence of the CPS that continues to provide service to consumers even when it is not demanded - it simply exists. However, there is also a simultaneous recognition that without consumer data it would be less able to meet consumer needs when required. , The more data the system contains, the more 'truthful' its perceived interactions would be from a consumer perspective.

Research hypotheses

Having explored and considered how the trust-based constructs identified from the literature review loaded into factors, labelled EBPA and Constancy, we next sought to evaluate how well the predictor constructs identified in the literature above related to these new trust dimensions. In order to achieve this, the conceptual framework was developed into a model with a series of research hypotheses (see Figure 2). The hypotheses are stated as follows.

H1a: Propensity to trust technology in general will positively affect the trust dimension of experiential based performance assessment (EBPA).
H1b: Propensity to trust technology in general will positively affect the trust dimension of constancy.

H2a: Generalised perceived risk of using technology will negatively affect the trust dimension of experiential based performance assessment (EBPA).
H2b: Generalised perceived risk of using technology will negatively affect the trust dimension of constancy.

H3a: Online networking competency will positively affect the trust dimension of experiential based performance assessment (EBPA).
H3b: Online networking competency will positively affect the trust dimension of constancy.

H4a: Concerns about privacy will negatively affect the trust dimension of experiential based performance assessment (EBPA).
H4b: Concerns about privacy will negatively affect the trust dimension of constancy.

H5a: Concerns about security will negatively affect the trust dimension of experiential based performance assessment (EBPA).
H5b: Concerns about security will negatively affect the trust dimension of constancy.

Insert Figure 2 about here

Analysis and results of hypotheses

The evaluation of the proposed model followed a two-step approach (e.g., Anderson and Gerbing, 1988). The initial stage used confirmatory factor analysis (CFA) to evaluate the measurement model and to examine the reliability and validity of criteria associated with the latent variables. An evaluation of the structural model follows.

A seven factor and 41-indicator CFA was conducted. An examination of each item's loading on its corresponding construct was used to assess the convergent reliability of items. Barclay, Thompson and Higgins (1995) suggest that, as a rule of thumb, item loadings should exceed 0.70. The results demonstrated that a number of standardized regression weightings were of values less than the recommended cut off and were deleted (Barclay *et al.,* 1995; Hulland, 1999). These comprised EBPA1 (.51), SC5 (.57), ONC2 (.57), PTT1 (.58), PC3 (.65), EBPA2 (.67) and C5 (.69). Additionally, convergent reliability was assessed using average variance extracted (AVE). All values for AVE were above 0.50 and therefore acceptable (Bagozzi and Yi, 1988). Finally, a Cronbach alpha test revealed all values to be above .7 so the scales may be considered reliable with this sample (see Appendix 5). Next, we assessed discriminant validity. An initial examination of the absolute values of the factor inter-correlations identified all values as being below 1, providing some evidence of discriminant validity of the constructs (Kumar *et al.*, 1993). Discriminant validity was further assessed by examining the relationship between correlations among the constructs and the square root of AVEs (Chin, 1998; Fornell and Larcker, 1981). The results indicate the square root of the AVEs is greater than any of the correlations among the constructs indicating satisfactory discriminant validity for all constructs (see Appendix 6).

The second stage involved analyses of the structural model (Salisbury, Pearson, Pearson and Miller, 2001). Reported values for the model fit indices (RMSEA=.064; RMR=.085; CFI=.876; NFI=.815 and GFI=.812) are marginally above or below recommended cut off values (Hooper, Coughlan and Mullen, 2008). An attempt to improve fit by means of examining the first-order parameters was adopted (Reisenzein, 1986). This analysis involved an examination of the modification indices (MI) (Bryne, 1987). Model refinement may take place provided there is a robust theoretical and empirical justification for such an approach and adjustments that make no substantive sense are avoided (Silvia and MacCallum, 1988). Based on this premise, a path from EBPA to Constancy (MI=157.95) was added. This may be theoretically justified insofar as EBPA is predicted by participants' experience of using existing service systems and is used to complete potential gaps in knowledge so as to make assessments about the Constancy of an unfamiliar system.

Model fit improved significantly with reported values for the re-specified model ranging from a 'well-fitting' or 'good' model (χ^2/df= 2.2, p< 0.00; RMSEA=.052; RMR=.039 and CFI=.923) (Hu and Bentler, 1999; Steiger, 2007, Byrne, 1998; Diamantopoulos and Siguaw, 2000 in Hooper *et al.,* 2008) to a 'marginal' fitting model (NFI=.863, and GFI=.861) (Hair *et al.,* 1995). The re-specified structural model may be seen in Figure 3.

Insert Figure 3 about here

A summary of hypothesized results may be seen in Table 3.

Insert Table 3 about here

Discussion

H1a is accepted but H1b is rejected. The propensity to trust technology in general has a significant and positive effect on EBPA (experientially based performance assessments) about the service system but not on its Constancy. H2a is accepted but H2b is rejected. The perceived risk of using technology in general has a significant and negative effect on EBPA about the service system but not on its Constancy. H3a is accepted but H3b is rejected. Participants' level of competency in networking online has a significant and positive effect on EBPA about the service system but not on its Constancy. Both H4a and H4b are rejected. Concerns about privacy do not have a negative significant effect on either EBPA or Constancy. Both H5a and H5b are accepted. Concerns about security have a significant and negative effect on both EBPA and Constancy.

Interpretation

This research has identified trust dimensions and their predictors within a CPS: a household context. From a theoretical perspective, EFA findings indicate the novel ways that trust is evoked by consumers. Traditional constructs drawn from extant literature within the social science and technology fields merge into two factors. These new factors intimate the impact of the potential complexity of CPS contexts on consumers' ability to make judgments *experientially* (EBPA) and how the system's continuity becomes the focus of trust (Constancy). The path model (Figure 3) findings indicate the strongest relationship is between experiential based performance assessment (EBPA) and generalised confidence or faith-based assessment of its Constancy of performance. Within such CPS contexts as that depicted in this research, vast amounts of data are collected and information exchanged between actors (human and machine) continuously and ubiquitously (Shand, Dimmock and Bacon, 2004) and results suggest that consumers find it cognitively prohibitive to process the volume of exchanges and the accompanying need for moment-to-moment trust judgments and decisions (Sillence and Briggs, 2008). Consequently, consumers 'pass on' decisions to the system, having faith that it will act in their best interest by demonstrating Constancy (or persistence) (Roussos and Moussouri, 2004). A contribution of this research is that within such multi-partite service environments (CPS contexts), findings indicate that trust becomes a fundamental component of the value proposition itself, residing within and across the network of actors and objects. Hence, hypotheses relating to predictors of trust in H1b, H2b, H3b and H4b are unsupported and the null hypotheses accepted.

The findings imply how consumer experiences of current service systems may be used to predict the likelihood for trust in new systems, such as emergent CPS contexts. Constructs such as more generalised trust in technology, perceived risks of using technology, consumer competency in networking online and concerns about the security of personal information are important. Hence, hypotheses in relation to predictors H1a, H2a, H3a and H5a are supported. This suggests that the *entity of reference* used in making a judgment about the trustworthiness of a CPS context is not fixed to any extraneous cue(s) related to the service system (ie., a touchpoint, device, etc.) but to an *idiosyncratic customer experience* of the service context (Denning, 2015). The lack of significance of generalised trust in technology as a predictor of Constancy (H1b) highlights that, at the present time, consumers rely on their general experience to make judgments about the stability of the CPS context. Whilst this relationship between the constructs is not surprising, it does indicate an interesting challenge: if general trust in technologies does not transfer directly to faith-based confidence (Simmel, 1978) in the pervasiveness of the system but is mediated by experience (e.g., McKnight *et al.,* 2011), how might consumers gain the necessary experience to adapt within a rapidly evolving system? Indeed, consumers' general propensity to trust technology and, to a lesser degree, engage in social networking activity, positively relates to their experiential performance

assessment of the system. The former is not situation specific but derived from their general attitude to technology and desire to extrapolate their experiences between different technology-enabled situations. These findings contrast with traditional theories of trust that focus on interactions, say, with products, services or actors (e.g., Morgan and Hunt, 1994; Seppanen et al., 2007) in that the touchpoint is no longer defined or bounded by its branding.

The findings also indicate that an increase in perceived risks of being part of a CPS (H2a) is coupled with concerns over data security (H5a), and may lead to lower experiential performance assessment of the system (e.g., Norberg et al, 2007; Paul and Tarpet, 1975). Again, this is an unsurprising finding but its impact on consumer experience ultimately has important implications for the future adoption of IoT technologies that will comprise a CPS in the home, as highlighted above. A particularly interesting finding in the analyses is also the lack of significance of privacy on either the EBPA (experiential based performance assessment) of the household CPS or consumers' general confidence or faith in its Constancy of performance (H4a and H4b). This contrasts with contemporary rhetoric on the importance of data privacy in the adoption of IoT technologies (e.g., Peltier et al 2009; Rixon et al 2013; Acquisti et al 2016). Whilst acknowledging this needs further investigation, in the context of this study it is possible that consumers perceived the data needed to ensure such household systems are trustworthy is already within the system, of little value to them, or beyond their ability to control the system's access to it.

Future scenarios and research directions

What is likely to distinguish CPS contexts is that service systems dynamically *evolve* as actors (machines, devices and consumers) adapt *intelligently* to the context – it is not simply a case of the volume of data or information but its *dynamic performance* across the system that is unknowable to actors. Based on the findings of this research, consumers may be willing to set personal automated behavioural controls for data and information flows (privacy) within the system in order to manage the levels of digital identity they are comfortable with in order to receive the trusted service they desire. This may align well to theories of an emergent category of actor within IoT systems: the *trust manager* (Cho *et al*., 2015). Trust managers (TM) are typically automated reputation management technologies that provide consumers with estimates of the reliability of behavioural responses within a system for particular operations under conditions of imperfect knowledge and risk. In effect, the TM provides a level of assurance (*soft security*) for consumers. This may be by limiting the use of certain devices or modifying interactive and transactive behaviours in relation to the consumption patterns for those devices[1] (e.g., Lazarus, Averill and Opton, 1970; Castelfranchi and Falcone, 2010).

Social networking is evidently one way in which consumers may increase their understanding of the system. This implies technology-savviness over a broad range of devices, including those that connect people together for social purposes through networks, and technology-enabled systems such as CPS is important to the future adoption of the household system, effectively encompassing nested layers of a complex system. For example, to render a service at home, say, serving a nutritional meal that maximizes use of available resources (financial constraints, perceived wellbeing benefits, food stock stored in household cupboards, meal planning activities, etc.), typical information may draw upon a range of data. This may include data from an individual's personal environment, such as their psychophysical

[1] This is different to what consumers often see badged as *security* or *privacy settings* associated with individual components within an IoT system (software, devices, objects).

(emotional/cognitive) behaviours, their social environment (including behaviours, interactions, profiles of each social context), the interface or application used (such as its usage, interactions, transactions and context of use) the device (its usage, context of use, interactions, transactions and connected transactions), and the machine object such as a refrigerator (including its transactions and connected transactions with other machines). The findings into the relationships between the constructs identified may therefore usefully contribute to the future development of constructs on the role of social cognition theory (Bandura, 1986) that considers environmental influences on consumer behaviour. In turn, this theory may also further support development of TAM-based theories of specific technology adoption (e.g., Davis, 1993; Venkatesh and Davis, 1996).

Taken holistically, these findings suggest trust within CPS consumption contexts is not determined by interactions with a single device or touchpoint nor by a brand that bounds a service context but is embedded within it indicating the nature of trust in such systems. Such *embedded trust* is neither a consequence of nor antecedent to the service experience per se but incorporates agent-based trust and trust *acquired* from the behaviours of other similar service systems. Consumers use their experience of service performance to *fill in the gaps* of their knowledge. This then raises interesting questions as to how and under what optimal conditions experience of technologies is transferred to new consumption contexts. Embedded trust is focussed on CPS services 'in the round' and consumers are unable to identify specific roles of individual actors within the complex networked environment. This implies that whilst immediate attention of consumers may be on the most salient components (touchpoints), any failures by actors (eg., firms, devices, etc.) will affect perceptions of the entire system to varying levels, and possibly other systems. In such circumstances, trust may be subject to extraneous influences, positive or negative, at both macro and micro market levels. Influences may be media, personal social networks or firms, suggesting collective marketing communication strategies are required to ensure trust remains embedded (e.g., Giddens, 1990; Lobler, 2014) but levels of tolerance to system adaptations are not well understood within CPS contexts - at what level of influence does embedded trust become distrust? Interestingly, blockchain, as an emergent cryptographic method, may be useful in embedding trust by attaching a non-transferable cypher (block) to each micro-level transaction across a system. Blockchain produces a form of distributed digital ledger such that authenticity is irrefutable because it is confirmed collectively by members in the system (chain). The ways in which CPS use blockchain is a matter of ongoing technological development but its usefulness as a signification to consumers of system trustworthiness requires investigation.

Implications for research

An important area for future investigation is to understand how actors operationalize and effectively manage their roles in emerging CPS contexts in order to optimize trust across the system. This may be from a strategy, relationship marketing, technology (AI), policy or transdisciplinary perspective that encompasses the breadth of the system. This adds an exponential and multidimensional level of complexity to undertaking research that builds on extant work which has previously focussed primarily on defined interactions, say, at brand or firm level (e.g., Komiak and Benbasat, 2006; Hong, 2015). Approaches to research investigation need to be explored and developed, potentially aligning with Gummesson, Mele and Polese's (2018) view of synergies that complexity theory has with service-dominant logic, systems theory and service science.

Findings intimate consumers may potentially become constructive in their performance of trust in a CPS in order to exert influence over data and information flows, effectively managing their privacy and identity. Currently, however, very little is known about how actors may adapt their behaviour beyond the contractual and legal obligations that organizational actors specify (e.g., types and amount of data and information about individual users, related to general terms and conditions of service use and data protection). This will be an important area of future research in light of emerging legal frameworks on how data may be used (e.g., the EU's General Data Protection Regulation). Whilst consumers may adapt their privacy levels, however, there is no *hard security* within an autopoietic system (see e.g., Sicari, Rizzardia, Griecob and Coen-porisinia, 2015). Thus, data and information flow is persistent – for an individual actor there is ultimately only one way to have any control over this and that is to disengage with the entire system. This may be challenging if not impossible since system decisions based on historical data in a dynamically adaptive context such as CPS remains in circulation. The adaptations consumers overtly make to control the flow of personal data within a persistent system would therefore be an interesting direction in which to take future research into CPS.

Implications for practitioners

The challenge from a practitioner perspective is how to optimize trust through the predictors identified in this study, particularly when a firm level proposition (product, device, etc.) is an invisible component of the CPS context. One approach may be the adoption of CPS level agreements between system-wide members, potentially implemented through technologies such as blockchain. In such a way, and by revealing the [artificial] intelligence behind processes employed, system members as well as individual consumers may be assured, and even insured, against specific failures or negative influences. This immediately highlights the need for clarity in the roles and adaptive use of machine learning algorithms across CPS, as well as a need for a platform that pinpoints system failures as they occur (i.e., in 'real' time) including pathways for remedial action that consumers may take. In the current evolutionary climate of piecemeal adoption of IoT, however, this kind of systemic approach to relational attribution and remedy is both under-researched and undeveloped. For example, it may be argued that firms need to use mechanisms that enable consumers or their proxies to intervene and establish control parameters over CPS as they evolve. This is unlikely to happen at firm level, and may well require policy intervention in much the same way that data protection regulation has been implemented.

Findings highlight the role of knowledge transfer between CPS contexts (IoT applications) intimating that consumers who have limited experience of technologies in general, lack social mobility online or have minimal opportunities for exposure to technologies and social networks may increasingly be left behind in the development of future service contexts. It should therefore be a priority for service designers to ensure that consumers remain actively engaged in the development of systems that are based on their own performance through *embedded trust* within it, and more broadly, that access to experiences of new technologies is provided. This is likely to have societal as well as firm level implications that necessitate a coordinated strategy to promote the value of technologies-in-use and educate consumers about their evolving forms, functions and [dis]benefits. Such a strategy reflects United Nations' sustainable development goals for implementing policy on human rights and corporate social responsibility that 'leaves no one behind' (e.g., G4 quality education; G10 reduced inequality; G12 responsible consumption and production, etc.).

Limitations of Research

This research was exploratory and reflects a contemporary view of trust for a novel technological advancement. Whilst the theoretical model is based on an extensive review of literature it does not use the range of constructs that previous trust literature has identified in traditional consumer-firm contexts, thus our approach may have missed some aspects that may yet inform development of a model. The study adopts a novel research design using a videographic approach to depict development of a CPS and IoT applications that may ultimately evolve in unanticipated ways, despite the extensive review of literature and technologies in the current study to accurately reflect the context. The study is based on a sample population, but this is representative of one country presenting a Westernized view of digital culture. The adoption and use of IoT may evolve and embedded trust may apply differently in contexts such as Eastern cultures. The findings may therefore have limited application to countries with different rates of adoption of IoT technologies.

Conclusions

The study presented in this paper has developed and tested a novel model of predictors and constructs of trust in a CPS context: a household system. IoT technologies interconnect to create complex cyber-physical systems rendering services that are idiosyncratically determined by consumers. The paper discusses implications of research findings and potential areas for future research development at theoretical and practitioner levels. The findings suggest it is consumer experience of technologies *in general* that determines trust at a system-wide level, where trust is embedded into the system's continual performance simply by their presence in the system. Findings intimate that consumers do not explicitly relate to the potential pervasive constancy of the household system and may be unable to transfer their understanding of trust in this context. It is possible that even at this early stage of evolution of IoT systems, there is already too much complexity in the interrelational data exchanges within a CPS context for consumers to fully comprehend (eg., Giddens, 1990; Luhmann, 1995; Lobler, 2014).

At the firm and brand level, some innovating firms that collect data from IoT devices appear now to have determined there is little they can actually do with it themselves whilst simultaneously recognizing the significant hardware and software [cyber-] security issues that have arisen with their use (e.g., McKinsey). In the context of findings from this study, the nature of *embedded trust* highlights the need for a system-wide approach to improving the integrity of CPS performance to address perceived (and presumably commercially real) security issues (e.g., Salisbury et al, 2001). Moreover, when a CPS context provides value to stakeholders that transcend individual brands, then new types of service-on-service provision will emerge. This could, for example, pertain to public services for city-wide resource management (smart cities), general household and personal insurance (fintech) and health services: it is at this point that CPS and IoT applications become a matter of local and national government interest.

References

Acquisti, A., Taylor, C. and Wagman, L. (2016), "The Economics of Privacy", *Journal of Economic Literature*, Vol. 52, No. 2, Sloan Foundation Economics Research Paper No. 2580411.

Alford, B. L. and Sherrell, D. L. (1996), "The role of affect in consumer satisfaction judgments of credence-based services", *Journal of Business Research*, Vol. 37, No.1, pp. 71-84.

Anderson, J. C. and Gerbing, D. W. (1988), "Structural equation modelling in practice: A review and recommended two-step approach", *Psychological Bulletin*, Vol. 103, No. 3, pp. 411.

Ashton, K. (2009), That 'Internet of Things' thing, The RFID Journal, available at https://www.rfidjournal.com/articles/view?4986 [accessed 30 Nov 2018].

Atzori, L., Iera, A. and Morabito, G. (2010), "The Internet of things: A survey", *Computer networks*, Vol. 54, No. 15, pp. 2787-2805.

Bagozzi, R. and Yi, Y. (1988), "On Evaluation of Structural Equation Models", *Journal of the Academy of Marketing Science,* Vol. 16, No. 1, pp. 74-94.

Bandura*, A. (*2000*),* "Psychological aspects of prognostic judgments", In R. W. Evans, D. Baskin, & F. M. Yatsu (Eds.), *Prognosis of neurological disorders*, (2nd ed., pp.11-27).

Bansal, G., Zahedi, F.M. and Gefen, D. (2016), "Do context and personality matter? Trust and privacy concerns in disclosing private information online", *Information and Management*, Vol. 53 No. 1, pp. 1-21.

Bao F. and Chen, I.R. (2012), "Dynamic trust management for Internet of Things Applications" in *2012 International Workshop on Self-Aware Internet of Things*, San Jose, CA, US, Sept.

Barclay*,* D., Higgins C. and Thompson*,* R. (1995), "The Partial Least Squares (PLS) Approach to Causal Modelling Personal Computer Adoption and Use as an Illustration," *Technology Studies, Special Issue on Research Methodology*, Vol. 2, No. 2, pp. 285-309.

Barile, S. and Polese, F. (2010), "Smart service systems and viable service systems: Applying systems theory to service science", *Service Science*, Vol.2, No.1-2, pp. 21-40.

Bart, Y., Shankar, V., Sultan, F. and Urban, G.L. (2005), "Are the drivers and role of online trust the same for all web sites and consumers? A large scale exploratory empirical study", *Journal of Marketing*, Vol. 69 No. 4, pp. 133-52.

Beatty, P., Reay, I., Dick, S., & Miller, J. (2011). "Consumer trust in e-commerce web sites: A meta-study". *ACM Computing Surveys (CSUR)*,Vol. 43, No. 3, p. 14.

Belk, R. and Kozinets, R.V. (2005), "Videography in marketing and consumer research", *Qualitative Market Research: An International Journal*, Vol. 8, No. 2, pp. 128-141.

Berscheid, E. (1993) *Emotion. In Close Relationships*, H. H. Kelley et al. Eds., W. H. Freeman, New York, 110–168.

Bhattacherjee, A. (2002), "Individual trust in online firms: Scale development and initial test", *Journal of management information systems*, Vol. 19, No. 1, pp. 211-241.

Byrne, B. M. and Shavelson, R. J. (1987), "Adolescent self-concept: Testing the assumption of equivalent structure across gender", *American Educational Research Journal*, Vol. 24, No.3, pp. 365-385.

Castelfranchi, C. and Falcone, R. (2010), *Trust Theory: A Socio-Cognitive and Computational Model*, M. Wooldridge (Ed.). Series in Agent Technology. Wiley.

Chandler, J.D. and Lusch, R.F. (2015), "Service Systems: A Broadened Framework and Research Agenda on Value Propositions, Engagement, and Service Experience", *Journal of Service Research*, Vol. 18, No. 1, pp. 6-22.

Chesney, T., Chuah, S., Dobele, A. and Hoffmann, R. (2017), "Information richness and trust in v-commerce: implications for services marketing", *Journal of Services Marketing*, Vol. 31 Issue: 3, pp.295-307

Cheung, C. & Lee, M., (2001), "Trust in Internet Shopping: Instrumental Development and Validation through Classical Modern Approaches", *Journal of Global Information Management,* Vol. 9, No. 3, pp. 25-39

Chin, W. (1998), "The Partial Least Squares Approach for Structural Equation Modelling", in Ed: Marcoulides*, G., Modern Methods for Business Research,* Mahwah, New Jersey.

Cho, J.-H., Chan, K. and Adali, S. (2015), "A survey on trust modelling", *ACM Computing Surveys*, Vol. 48, No. 2, Article 28.

Chou, H.J. (2009), "The effect of experiential and relationship marketing on customer value: a case study of international American casual dining chains in Taiwan", *Social Behaviour and Personality Journal*, Vol. 37, No.7, pp. 993-1008.

Culnan, M. and Armstrong, P. (1999), "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation", *Organization Science,* Vol.10, No. 1, pp. 104-115.

Damschroder, L., Pritts, J., Neblo M., Kalarickal, R., Creswell, J. and Hayward, R. (2007), "Patients, privacy and trust: Patients' Willingness to Allow Researchers to Access their Medical Records", *Social Science and Medicine,* Vol. 64, pp. 223-235.

Davis, F. D. (1993), "User acceptance of information technology: system characteristics, user perceptions and behavioral impacts", *International Journal of Man-Machine Studies*, Vol. 38 No. 3, pp. 475-487.

Denning, S. (2015), "Customer pre-eminence: the lodestar for continuous innovation in the business ecosystem", *Strategy and Leadership*, Vol. 43, No.4, pp. 18-25.

Deutskens, E., De Ruyter, K., & Wetzels, M. (2006), "An assessment of equivalence between online and mail surveys in service research", *Journal of Service Research*, Vol. 8, No.4, pp. 346-355.

Engen, V., Pickering, J. B. and Walland, P. (2016), "Machine Agency in Human-Machine Networks; Impacts and Trust Implications", *arXiv preprint arXiv:1602.08237*.

Fornell, C. and Larcker, D., (1981), "Evaluating Structural Equation Models with Unobserveable Variables and Measurement Error", *Journal of Marketing Research,* Vol. 18, No.1, pp. 39-50.

Friedman, E.J., Resnick, P. and Sami, R. (2007). Manipulation-resistant reputation systems, in Nisan, N., Roughgarden, T., Tardos, E., Vazirani, V.V. (eds.), *Algorithmic Game Theory*, pp. 677-697, Cambridge: Cambridge University Press.

Fritsch, L., Groven, A. and Schulz, T. (2012), "On the Internet of Things, Trust is Relative", *AML Workshops,* CCIS 277, pp. 267-273.

Frow, P. McColl-Kennedy, R.R., Hilton, T., Davidson, A., Payne, A. and Brozovic, D. (2014), "Value propositions: a service ecosystems perspective", *Marketing Theory*, Vol. 14, No.3, pp. 327-351.

Giddens, A. (1990), *The consequences of modernity*, Cambridge, UK, Polity Press.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013), "Internet of things (IoT): A vision, architectural elements, and future directions", *Future Generation Computer Systems*, Vol. 29, No.7, pp. 1645-1660.

Gummesson, E. and Grönroos, C. (2012), "The emergence of the new service marketing: Nordic School perspectives", *Journal of Service Management*, Vol. 23, No.4, pp. 479-497.

Gummesson, E., Mele, C. and Polese, F. (2018). Complexity and viability in service ecosystems, *Marketing Theory*, May, available online at https://journals.sagepub.com/doi/pdf/10.1177/1470593118774201 [accessed 6 Dec 2018].

Gustafsson, A., Högström, C., Radnor, Z., Friman, M., Heinonen, K., Jaakkola, E. and Mele, C. (2016), "Developing service research–paving the way to transdisciplinary research", *Journal of Service Management*, Vol. 27, No.1, pp. 9-20.
Hair, J., Anderson, R., Tatham, R. and Black, W. (1995), *Multivariate Data Analysis,* Maxwell MacMillan International.
Hanlon, G. (1997), "A profession in transition?—Lawyers, the market and significant others" *The Modern Law Review*, Vol. 60, No. 6, pp.798-822.
Harwood, T. and Garry, T. (2017). "Internet of Things: understanding trust in techno-service systems", *Journal of Service Management,* Vol. 28, No. 3, pp. 442-475.
Hoffman, D. and Novak, T. (2016), "Consumer and Object Experience in the Internet of Things: An Assemblage Theory Approach" (August 21, 2016). Available at SSRN: https://ssrn.com/abstract=2840975
Hong, I. (2015), "Understanding the Consumer's Online Merchant Selection Process: The Roles of Product Involvement, Perceived Risk, and Trust Expectation", *International Journal of Information Management,* Vol. 35, pp. 322-336
Hooper, D., Coughlan, J. and Mullen, M. (2008). Structural equation modelling: Guidelines for determining model fit. *Articles*, 2.
Hu, L. and Bentler, P. (1999), "Cutoff criteria for fit indices in covariance structure analysis: conventional criteria versus new alternatives", *Structural Equation Modeling*, Vol. 6, pp. 1-55.
Hulland, J. (1999), "Use of Partial Least Squares (Pls) in Strategic Management Research: A Review of Four Recent Studies", *Strategic Management Journal,* Vol. 2, No. 2, pp. 195-204.
Klang, M. (2006), "Disruptive Technology: Effects of Technology Regulation on Democracy", unpublished thesis, University of Gothenburg, available at http://hdl.handle.net/2077/9910
Komiak, S. Y. and Benbasat, I. (2006), "The effects of personalization and familiarity on trust and adoption of recommendation agents", *MIS quarterly*, pp. 941-960.
Kumaraguru, P. and Cranor, L. (2006), "Privacy Indexes: A Survey of Westin's Studies, *CMU-ISRL-5-13", Institute for Software Research International*, Carnegie Mellon University.
Lankshear, C. and Knobel, M. (2006), *New literacies: Everyday practices and classroom learning*, Berkshire, UK: McGraw-Hill.
Lazarus, R.S., Averill, R.R. and Opton, E.M. (1970), "Towards a cognitive theory of emotion" in *Feelings and Emotions*, M.B. Arnold (Ed.). Academic Press, New York, pp. 207–232, The Loyola Symposium.
Lobler, H. (2014), "When Trust Makes It Worse—Rating Agencies as Disembedded Service Systems in the U.S. Financial Crisis", *Service Science*, Vol. 6, No. 2, pp. 94–105
Luhmann, N. (1995). *Social Systems*. Stanford, CA, Stanford University Press.
Macdonald, E. K. and Uncles, M. D. (2007), "Consumer savvy: conceptualisation and measurement", *Journal of Marketing Management*, Vol. 23, No.5-6, pp. 497-517.
Madsen, M. and Gregor, S. (2000), "Measuring Computer Trust", *11th Australasian conference on information systems*.
Maglio, P. P. and Spohrer, J. (2008), "Fundamentals of service science", *Journal of the Academy of Marketing Science*, Vol. 36, No. 1, pp.18-20.
Mandler, B., Antonelli, F., Kleinfeld, R., Pedrinaci, C., Carrera, D., Gugliotta, A. and Villares, C.V. (2013, March), "COMPOSE--A Journey from the Internet of Things to the Internet of Services", *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on* (pp. 1217-1222), IEEE.
Marsh, S. and Briggs, P. (2009). Examining trust, forgiveness and regret as computational concepts, in *Computing with Social Trust*, J. Golbeck (Ed.), Springer, pp. 9–43, Human-

Computer Interaction Series.
Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995), "An integrative model of organizational trust", *Academy of management review*, Vol. 20, No. 3, pp. 709-734
Mcknight, D. H., Carter, M., Thatcher, J. B. and Clay, P. F. (2011), Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS)*, *2*(2), 12.
McKnight, D. H., Choudhury, V. and Kacmar, C. (2002), "Developing and validating trust measures for e-commerce: An integrative typology", *Information systems research*, Vol. 13, No. 3, pp. 334-359.
Medina-Borja, A. (2015), "Smart Things as Service Providers: A Call for Convergence of Disciplines to Build a Research Agenda for the Service Systems of the Future" (Editorial Column), *Service Science*, Vol. 7, No. 1, pp. ii-v.
Mele, C. and Polese, F. (2011), Key dimensions of service systems in value-creating networks, in Demirkan, H., Spohrer, J.C. and Krishna, V. (Eds), *The Science of Service Systems*, Springer, New York, NY, pp. 37-59.
Minerva, R., Biru, A. and Rotondi, D. (2015), Towards a definition of the Internet of Things (IoT), *IEEE Internet Initiative*, available at https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf [accessed 30 Nov 2018].
Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012), "Internet of things: Vision, applications and research challenges", *Ad Hoc Networks*, Vol. 10, No. 7, pp. 1497-1516.
Morgan, R.M. and Hunt, S.D. (1994), "The Commitment - Trust Theory of Relationship Marketing", *Journal of Marketing*, Vol. 58(July), pp. 20-38.
Mukherjee, A. and Nath, P. (2007), "Role of electronic trust in online retailing: A re-examination of the commitment-trust theory", *European Journal of Marketing*, Vol. 41 Issue: 9/10, pp.1173-1202
Nass, C., Fogg, B. and Moon, Y (1996), "Can Computers be Teammates?", *International Journal Human Computer Studies,* Vol. 45, No. 6, pp. 669-678.
Ng, I. and Wakenshaw, S. (2017), "The Internet-of-Things: Review and Research Directions", *International Journal of Research in Marketing*, Vol. 34, pp. 3-21.
Norberg,P., Horne D. and Horne, D. (2007), "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors",*The Journal of Consumer Affairs,* Vol. 41, No. 1, pp. 100-126.
Park, C.W., Jaworski, B.J. & MacInnis, D.J. (1986), "Strategic brand concept-image management", *Journal of Marketing*, Vol. 50(Oct), pp. 135-145.
Paul, P. and Tarpey, L. (1975), "A Comparative Analysis of Three Consumer Decision Strategies", *Journal of Consumer Research,* Vol 2 (June), pp. 29-27.
Pauwels, L. (2011), "Integrated conceptual framework", in Margolis, E. and Pauwels, L., *The Sage Handbook of Visual Research Methods*, London: Sage Publications.
Pavlou, P.A. and R.K. Chellappa (2001), "The Role of Perceived Privacy and Perceived Security in the Development of Trust in Electronic Commerce Transaction", *Ebizlab Working paper*, 39 p., January 2001.
Peltier, J., Milne, G. and Phelps, J., (2009), "Information Privacy Research: Framework of Integrating Multiple Publics, Information Channels, and Responses", *Journal of Interactive Marketing,* Vol. 23, pp. 191-205.
Perera, C., Zaslavsky, A., Christen, P. and Georgakopoulos, D. (2014), "Sensing as a service model for smart cities supported by internet of things", *Transactions on Emerging Telecommunications Technologies*, Vol. 25, No. 1, pp. 81-93.
Pfleeger, C.P. & Pfleeger, (2011), *Analyzing Computing Security: A Threat/ Vulnerability / Countermeasure Approach,* Prentice Hall, Upper Saddle River

Pink, S. (2007), *Doing visual ethnography*, London, Sage.
Reisenzein, R. (1986), "A structural equation analysis of Weiner's attribution—affect model of helping behaviour". *Journal of Personality and Social Psychology*, Vol. 50, No. 6, p. 1123.
Rempel, J., Holmes, J. and Zanna, P. (1985), "Trust in Close Relationships", *Journal of Personality and Social Psychology,* Vol. 49, No. 1, pp. 95-112.
Rixon, L., Hirani, S. P., Cartwright, M., Beynon, M., Selva, A., Sanders, C. and Newman, S. P. (2013), "What influences withdrawal because of rejection of telehealth - the whole systems demonstrator evaluation" *Journal of Assistive Technologies,* Vol. *7*, No. 4, pp. 219-227.
Rose J. and Truex D. (2000), "Machine Agency as Perceived Autonomy: An Action Perspective". In: Baskerville R., Stage J., DeGross J.I. (eds) *Organizational and Social Perspectives on Information Technology*. IFIP — The International Federation for Information Processing, vol 41. Springer, Boston, MA
Roussos, G. and Moussouri, T. (2004), "Consumer perceptions of privacy, security and trust in ubiquitous commerce", *Personal and Ubiquitous Computing*, Vol. 8, No. 6, pp.416-429.
Royal Society (2017), "The Internet of Things: opportunities and threats", Conference Report, 3 Oct, available at https://royalsociety.org/~/media/events/2017/10/tof-iot/iot-conference%20report-final.pdf, accessed 27 Dec.
Salisbury, W.D., Pearson, R.A., Pearson, A.W. and Miller, D.W. (2001), "Perceived security and World Wide Web purchase intention", *Industrial Management and Data Systems*, Vol.101, No. 4, pp. 165-177.
Sayre, S. (2001), *Qualitative Methods for Marketplace Research*, London: Sage.
Schembri, S. and Boyle, M.V. (2013), "Visual ethnography: achieving rigorous and authentic interpretations", *Journal of Business Research*, Vol. 66, pp. 1251-1254.
Schlosser, A., White, T. and Lloyd, S., (2006), "Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions", *Journal of Marketing,* Vol. 70, No. 2, pp. 133-148.
Sekhon, H., Ennew, C., Kharouf, H. and Devlin, J., (2014). "Trustworthiness and trust: Influences and implications", *Journal of Marketing Management*, Vol. 30, No.3-4, pp. 409-430.
Seppänen, R., Blomqvist, K. & Sundqvist, S. (2007), "Measuring inter-organizational trust – a critical review of the empirical research in 1990–2003", *Industrial Marketing Management*, Vol. 36, pp. 249-265.
Shand, B., Dimmock, N. and Bacon, J. (2004), "Trust for ubiquitous, transparent collaboration", *Wireless Networks*, Vol. 10, No. 6, pp. 711-721.
Sheppard, B. & D. Sherman. "The grammars of trust: A model and general implications." *Academy of management Review,* 23, no. 3 (1998): 422-437.
Sicari, S., Rizzardia, A., Griecob, L.A. and Coen-porisinia, A. (2015), "Security, privacy and trust in Internet of Things: The road ahead", *Computer Networks*, pp. 146-164.
Sillence, E. and Briggs, P. (2008), "Ubiquitous computing: trust issues for a 'healthy' society", *Social Science Computer Review*, Vol. 26, No. 1, pp. 6-12.
Silvia, E.S.M. and MacCallum, R.C. (1988), "Some factors affecting the success of specification searches in covariance structural modelling", *Multivariate Behavioral Research*, Vol. 23, pp. 297–326.
Simmel, G. (1978). *The philosophy of money*, London, Routledge.
Skopik, F., Schall, D. and Dustrdar, S. (2010). "Modeling and mining of dynamic trust in complex service-oriented systems", *Information Systems*, Vol. 35, No. 7, pp. 735-757.
Smith, H.J., Milberg, S.J. and Burke, S.J. (1996), "Information Privacy Measuring Individuals' Concerns about Organizational Practices", *MIS Quarterly*, Vol. 20, pp. 167-196.

Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A. and Leimeister, J. (2014), "Chapter 3: Understanding the Formation of Trust", In: David et al. (Eds), *Socio-technical Design of Ubiquitous Computing Systems*, Springer International Publishing, Switzerland, pp. 39-57.
Steiger, J.H. (2007), "Understanding the limitations of global fit assessment in structural equation modelling", *Personality and Individual Differences*, Vol. 42, pp. 893-898.
Su, X., Zhang, M., Mu, Y. and Bai, Q. (2013). "A robust trust model for service-oriented systems", *Journal of Computer and System Sciences,* Vol. 79, No. 5, pp. 596-608.
Terpening, E. and Littleton, A. (2017), "The State of Internet of Things in the Home", *Research Report: Altmeter Prophet,* (August, 2017).
Venkatesh, V. (2000), "Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model", *Information Systems Research*, Vol. 11 No. 4, pp. 342-365.
Venkatesh, V. and Davis, F. D. (1996), "A model of the antecedents of perceived ease of use: Development and test", *Decision Sciences*, Vol. 27 No. 3, pp. 451-481.
Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003). User acceptance of information technology: towards a unified view, *MIS Quarterly*, Vol. 27, pp. 425-478.
Wünderlich, N.V., Heinonen, K., Ostrom, A.L., Patricio, L., Sousa, R., Voss, C. and Lemmink, J.G.A.M. (2015), "Futurizing smart service: implications for service researchers and managers", *Journal of Services Marketing*, Vol. 29, No. 6/7, pp. 442-447.
Yan*, Z.,* Zhang*, P. and* Vasilakos*,* A.V. (*2014*), "A Survey on Trust Management for Internet of Things", *Journal of Network and Computer Applications*, Vol. 42, pp. 120-134.
Yan, Z., Zhang, P. and Vasilakos, A.V. (2014). A survey on trust management for Internet of Things, *Journal of Network and Computer Applications*, Vol. 42, pp. 120-134.
Yang, L., Yang, S. H. and Plotnick, L., (2013), "How the Internet of things technology enhances emergency response operations", *Technological Forecasting and Social Change*, Vol. 80, No. 9, pp. 1854-1867.

Appendices

Appendix 1: Film Script

Film 1: Introduction to the Walker Family

Two couples, John and Jane and Harry and Maddy, are part of a connected family network. John and Jane are in their mid-50s, and parents of Harry, who is cohabiting with Maddy, both in their mid-20s and beginning their busy careers in the city. John and Jane live in a rural environment, over an hour away from Harry and Maddy by public transport. Jane has recently undergone surgery for breast cancer and is recovering well, following an ongoing programme of treatment. John is a keen runner, and with their son, Harry, regularly participates in marathons. Maddy has a broad social network of friends with whom she likes to keep in touch with via social networks and participation in virtual games. All four are wearing biometric trackers that capture data about their individual health, wellbeing and whereabouts status. The data is shared and used in conjunction with a range of people, devices and environments.

Film 2: The Household Manager Service System

Harry and Maddy have very busy work and home lives. They both participate in sport three nights a week and spend some time over their weekend also in sports activities, although this tends to be more social and together. During the week, Harry and Maddy like to plan their meals so they can focus on their activities, both are health conscious and like to ensure they have nutritious meals according to their lifestyle. Harry is in preparation for a marathon and is following a strict diet to maximize his performance according to his training regime. Maddy also enjoys cooking although has little time to spend planning exotic meals. Using the parameters of their respective fitness and health programmes as well as social plans, they select and upload meal ideas each week to their kitchen programme manager. The programme manager evaluates the data and ensures the appropriate foods are available for meals. This involves the freezer and refrigerator coordinating which items are defrosted and when; appropriate stock levels in the store cupboards for dried, tinned and fresh produce are maintained; and the oven heated to the correct temperature at the best time, ready for when food will be cooked. The programme manager is connected to the couple's favourite grocery retailers and automatically coordinates orders to make use of retailer offers and optimized deliveries, which it dovetails to the availability at home of either Harry or Maddy. After meals, crockery and utensils are put into the dishwasher ready for switching on in alignment with the energy consumption target the couple has set for their home. The washing machine along with other automated household equipment, such as the robotic cleaner, also align with this target, typically overnight whilst they sleep, or are out at work during the day.

Appendix 2: Survey instrument for the Household CPS

(All items were measured using a 5-point likert scale (5=agree strongly/1=disagree strongly)

Trust Dimensions

Understandability (Source: Madsen & Gregor, 2006)
U1 Overall, I understand how the Treatment manager system would work.
U2 Overall, it would be easy to follow what the Treatment manager system does.
U3 Overall, I understand how the Treatment manager system would assist me with decisions I would have to make

Integrity (Source: Mcknight *et al*., 2002)
I1 Overall, I believe the Treatment manager system would be honest.
I2 Overall, the Treatment manager system would keep its commitments.
I3 Overall, the Treatment manager system would be truthful in its dealings with me.

Personalisation (Komiak & Benbasat, 2006)
P1 Overall, the Treatment manager system would understand my needs
P1 Overall, the Treatment manager system would know what I want.

Competence (Source: McKnight, et al., 2011)
C1 Overall, the Treatment manager system would always have the skills and expertise to make the correct decisions
C2 Overall, the Treatment manager system would correctly use the information I would provide to it

Security (Source: Salisbury *et al*, 2001)
S1 Overall, I would feel secure with sensitive information about myself being collected and fed back to me by the Treatment manager system
S2 Overall, the Treatment manager system would be a safe place to collect and receive sensitive information about myself
S3 Overall, I believe the Treatment manager system would be concerned about my personal privacy.

Reliability (Source: McKnight et al., 2011)
R1 Overall, the Treatment manager system would perform reliably
R1 Overall, the Treatment manager system would be dependable

Benevolence (Source: Bhattacherjee, 2002)
B1 Overall, the Treatment manager system would do its best to help me.
B2 Overall, I believe the Treatment manager system would be open and receptive to my needs
B3 Overall, I believe the Treatment manager system would act in my best interest.

Faith (Source: Madsen & Gregor, 2006)
F1 If I was not sure about a decision, I would have faith that the Treatment manager system would provide the best advice.
F2 If I was uncertain about a decision to take, I would accept the advice of Treatment manager system rather than make it myself.

Predictors of Trust

Online networking competency (Source: Adapted from Macdonald and Uncles, 2007)

ONC1 I often check-out chatrooms and bulletin boards to find out about the latest products and services

ONC2 I'll often see if there is an on-line community that can help me when I'm looking for a product or service recommendation

ONC3 I'll often seek the opinions of other customers by posting a query about a product or service on an online bulletin board or chatroom

ONC4 I enjoy sharing points of view with online acquaintances via bulletin boards and chatrooms

ONC5 My best contacts for new product and service information often include people online that I've never met face-to-face

Propensity to trust technology in General (Source: Adapted from McKnight et al., 2009)

PTT1 I usually trust a technology until it gives me a reason not to trust it.

PTT2 Most technologies are reliable

PTT3 Most technologies have the features needed to do what they are meant to

PTT4 Most technologies enable me to do what they are meant to

Perceived risk of using technology (Source: McKnight et al., 2002)

PR1 Using technologies can be risky

PR2 Using technologies can entail uncertainty.

PR3 There can be negative outcomes from using technologies.

Privacy concerns (Source: Adapted from Smith, Milberg and Burke, 1996))

PC1 I'm concerned that organisations are collecting too much personal information about me

PC2 It concerns me to give my personal information to so many organisations

PC3 It concerns me how organisations identify me as an individual

PC4 I'm concerned about how organisations use personal information they collect about me

PC5 It concerns me when organisations ask me for personal information

Security concerns (Source: Adapted from Smith, Milberg and Burke, 1996)

SC1 Organisations should devote considerable time and effort to preventing unauthorised third party access to my personal information

SC2 Organisations should have efficient procedures to correct errors in personal information they collect and hold about me

SC3 Organisations should ensure that unauthorised third parties cannot access personal information that they hold about me

SC4 Organisations should not use my personal information for any purpose unless it has been authorised by me

SC5 Organisations need to ensure that personal information collected and held about me is accurate

Appendix 3: Bi-variate correlation table for the Household CPS

Item	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1 Would perform reliably	1																			
2 Would understand my needs	**.684****	1																		
3 Would correctly use the information provided	**.641****	**.599****	1																	
4 Would do its best for me	**.558****	**.571****	**.652****	1																
5 Feel secure with sensitive info. being collected	.444**	**.556****	.471**	.496**	1															
6 Understand how work	.339**	.278**	.288**	.397**	.264**	1														
7 Concerned about my personal privacy	.430**	.472**	.418**	.385**	**.551****	.275**	1													
8 Easy to follow what does	**.519****	.462**	.478**	.489**	.402**	.494**	.410**	1												
9 Would know what I want	**.567****	**.680****	**.502****	**.555****	**.558****	.334**	.492**	**.525****	1											
10 Would be honest	**.533****	**.521****	**.574****	**.633****	.485**	.313**	.469**	**.525****	**.564****	1										
11 Skills and expertise to make correct decisions	**.511****	**.551****	.485**	.471**	**.585****	.287**	**.524****	.453**	**.637****	.482**	1									
12 Understand how assist me with my decisions	.440**	**.540****	.491**	**.547****	.417**	.388**	.401**	.464**	**.505****	**.523****	.463**	1								
13 Would be open and receptive to my needs	**.550****	**.627****	**.593****	**.573****	**.613****	.354**	**.532****	**.518****	**.638****	**.562****	**.601****	**.587****	1							
14 Faith in system providing the best advice	**.523****	**.608****	**.518****	.466**	**.604****	.280**	**.569****	.459**	**.572****	**.510****	**.617****	**.505****	**.632****	1						
15 Would act in my best interest	**.542****	**.579****	**.554****	**.608****	**.635****	.250**	**.527****	.423**	**.598****	**.574****	**.546****	**.518****	**.631****	**.671****	1					
16 Truthful in its dealings with me	.468**	.490**	**.525****	**.554****	**.543****	.313**	.479**	.467**	**.514****	**.683****	.420**	**.529****	**.579****	**.590****	**.689****	1				
17 Would be dependable	**.599****	**.588****	**.582****	**.514****	**.549****	.352**	.497**	.496**	**.560****	**.590****	**.517****	**.514****	**.598****	**.634****	**.661****	**.689****	1			
18 Accept the system's advice	.481**	**.594****	.436**	.430**	**.561****	.236**	**.601****	.419**	**.575****	.497**	**.560****	.468**	**.518****	**.671****	**.576****	**.538****	**.606****	1		
19 Safe place to coll. and rec. sensitive info.	.433**	**.572****	.414**	.444**	**.714****	.234**	**.576****	.417**	**.559****	**.500****	**.536****	.425**	**.557****	**.647****	**.607****	**.537****	**.571****	**.682****	**1**	
20 Would keep its commitments	**.516****	**.540****	**.570****	**.594****	**.588****	.356**	**.507****	.488**	**.578****	**.546****	**.501****	.499**	**.638****	**.610****	**.636****	**.643****	**.623****	**.550****	**.631**.**	1

Appendix 4: Exploratory Factor Analysis results for the trust components in the Household CPS

Item	Factor 1: Constancy	Factor 2: Experiential Based Performance Assessment
Safe place to coll. and rec. sensitive info.	.945	
Accept the HHM system's advice	.880	
Feel secure with sensitive info. about me being collected	.848	
Faith in the HHM system providing the best advice	.825	
Concerned about my personal privacy	.777	
Would act in my best interest	.711	
Has the skills and expertise to make correct decisions	.671	
Would keep its commitments	.556	
Would be dependable	.574	
Would know what I want	.564	
Would understand my needs	.561	
Would be open and receptive to my needs	.550	
Truthful in its dealings with me	.527	
Understand how work		.793
Easy to follow what does		.679
Would do its best for me		.675
Would correctly use the information I would provide to it		.588
Would perform reliably		.546
Understand how assist me with my decisions		.537

Appendix 5: Confirmatory Factor Analysis

Standardised Regression Weights (p<.05 for all items)

Predictors Regression Path			Loading	Alpha	AVE
Online networking competency				0.817	0.60
Online networking competency	→	ONC3 Seek opinions online	0.78		
Online networking competency	→	ONC4 Share opinions online	0.83		
Online networking competency	→	ONC5 Online sources for new products	0.71		
Propensity to trust technology in general				0.831	0.62
Propensity to trust technology in general	→	PTT2 Most technologies are reliable	0.70		
Propensity to trust technology in general	→	PTT3 Have features to do what meant to	0.82		
Propensity to trust technology in general	→	PTT4 Enable me to what meant to	0.84		
Perceived risk of using technology			0.854	0.67	
Perceived risk of using technology	→	PR1 Can be risky	0.81		
Perceived risk of using technology	→	PR2 Entails uncertainty	0.87		
Perceived risk of using technology	→	PR3 Negative outcomes	0.77		
Privacy concerns				0.889	0.67
Privacy concerns	→	PC1 Collecting too much information	0.86		
Privacy concerns	→	PC2 Give information	0.81		
Privacy concerns	→	PC4 How use information	0.86		
Privacy concerns	→	PC5 Ask me for information	0.75		
Security concerns			0.885	0.67	
Security concerns	→	SC1 Devote time and effort	0.84		
Security concerns	→	SC2 Efficient procedures	0.77		
Security concerns	→	SC3 Unauthorised third parties	0.86		
Security concerns	→	SC4 Authorised use	0.79		
Trust Dimensions					
Constancy (R^2 =.86)				0.946	0.59
Constancy	→	C1 Safe place	0.79		
Constancy	→	C2 Accept advice	0.77		
Constancy	→	C3 Feel secure	0.77		
Constancy	→	C4 Have faith	0.82		
Constancy	→	C6 Act in my interest	0.81		
Constancy	→	C7 Skills and expertise	0.71		
Constancy	→	C8 Keep commitments	0.77		
Constancy	→	C9 Be dependable	0.77		
Constancy	→	C10 Know what I want	0.76		
Constancy	→	C11 Understand my needs	0.75		
Constancy	→	C12 Open and receptive	0.78		
Constancy	→	C13 Truthful	0.74		
Experiential Based Performance Assessment (EBPA) (R^2=.23)				0.883	0.58
Experiential Based Performance Assessment	→	EBPA3 Do its best	0.79		
Experiential Based Performance Assessment	→	EBPA4 Correctly use information	0.78		
Experiential Based Performance Assessment	→	EBPA5 Perform reliably	0.72		
Experiential Based Performance Assessment	→	EBPA6 Assist with decisions	0.75		

Appendix 6: Assessment of Discriminant Validity

Construct	1	2	3	4	5
1. Online networking competency	**.77**				
2. Propensity to trust technology	.28	**.78**			
3. Perceived risk of using technology	-.11	-.04	**.82**		
4. Privacy concerns	-.14	-.17	.46	**.82**	
5. Security concerns	-.28	.11	.47	.61	**.82**

*Diagonal values in bold are the square roots of the AVEs and off-diagonal values are correlations of the latent values

Table 1: Conceptual comparisons of trust between interpersonal, technological and CPS literatures

Object Attribute	Interpersonal	Technology	CPS
Familiarity and Understandability	Knowledge and understanding of dispositional attributions and traits of partner (e.g. Rempel, Holmes & Zanna, 1985).	Employing procedures, terms and cultural norms that are familiar and understandable (e.g. Madsen & Gregor, 2000).	Users forming mental models to predict future behaviour of smart service system
Reliability Predictability and Consistency	Acting in a predictable manner whilst exercising volition or freedom to choose (e.g. Sekhon, Ennew, Kharouf & Devlin, 2014)	Recognition that technology has no volition but may still function properly and on a consistent basis (e.g. McKnight *et al*., 2011).	Whether the smart service system may be relied on to perform its key tasks
Security	Refers to notions of the risk of indiscretions and the assumption that sensitive information revealed through intimate disclosures will not deliberately or inadvertently be shared (e.g. Sheppard& Sherman, 1998).	Perceived ability to fulfil security requirements such as authentication, encryption and non-repudiation (e.g. Cheung & Lee, 2001).	Refers to feelings of security specifically related to issues of information management when interacting with another entity within a smart service system
Integrity	Adhering to a set of established norms or procedures perceived as being 'fair and reasonable'. Generally referring to notions of 'honesty', 'credibility', 'fulfilment of promises' (e.g. Killinger, 2010).	Refers to the notion of 'data integrity' and covers users' perceptions that personal data will not be changed without users being given notice (e.g. Pfleeger & Pfleeger, 2011).	Related to issues of procedural fairness and adherence to processes regarding the management of personal information within the smart service system
Competence/expertise and functionality	Generally signals the ability or power to achieve an outcome. Frequently associated with experience and expertise (e.g. Moorman, Zaltman & Deshpande, 1992).	Technology has the attributes to deliver the functionality promised to complete a task (e.g. McKnight et al., 2011).	Refers to the ability of the smart service system to complete a task
Benevolence and Helpfulness	Acting in the other party's interest and offering help when needed. Implicit within this is a lack of opportunistic behaviour (e.g. Mayer *et al.*, 1995)	No sense of emotive caring but users may consider the 'help' function will provide necessary advice to complete a task (e.g. Beatty, Reay, Dick & Miller, 2011)	User's perception that the smart service system will act according to the user's best interest
Personalization	Dyadic interactions between intimates resulting in understanding and 'caring responses' from partners (e.g. Rempel, Holmes & Zanna, 1985).	The extent to which an object understands and represents the personal needs of the user (e.g. Komiak & Benbasat, 2006).	Understanding user needs and the generation of relevant and personalised recommendations "Only here, only me and only now"
Faith/Belief	Belief based on non-rational but may be triggered by evidence, signs or experience (e.g. Castelfranchi & Falcone, 2010)	Belief that technology will perform in situations in which it is untried (e.g. Madsen & Gregor, 2000)	Belief that a smart service system will perform appropriately even when there is limited understanding and/or familiarity

Table 2: Predictors of trust within CPS contexts

Trust Predictor	*Sources*	*Interpretation for CPS contexts*
Online networking competency	Macdonald and Uncles (2007)	the ability of consumers to draw on their experiences of collective online knowledge and interaction to make more informed trust decisions
Propensity to trust technology	Mayer *et al*. (1995) McKnight *et al.* (2011)	the extent to which users are willing to depend on technology across a broad spectrum of situations and technologies
Perceived risk of using technology	Norberg, Horne and Horne (2007) Paul and Tarpey (1975)	uncertainty resulting from the potential for a negative outcome and the perceived likelihood of a negative event occurring when interacting with technology
Privacy concerns	Acquista *et al.* (2016) Rixon *et al.* (2013)	consumers perceived control of information disclosure and secondary use
Security concerns	Bart *et al.* (2006) Mukherjee and Nath (2007)	consumer perception of the safety of personal information from unwanted third party intrusions

Table 3: Summary of hypothesised results

Hypotheses	**Path**	**Supported?**
H1a	Propensity to Trust Technology → (+) EBPA	Yes
H1b	Propensity to Trust Technology → (+) Constancy	No
H2a	Perceived Risk of using Technology → (-) EBPA	Yes
H2b	Perceived Risk of using Technology → (-) Constancy	No
H3a	Online Networking Competency → (+) EBPA	Yes
H3b	Online Networking Competency → (+) Constancy	No
H4a	Concerns about Privacy → (-) EBPA	No
H4b	Concerns about Privacy → (-) Constancy	No
H5a	Concerns about Security → (-) EBPA	Yes
H5b	Concerns about Security → (-) Constancy	Yes

Figure 1: Research framework: predictors and constructs for trust in CPS contexts

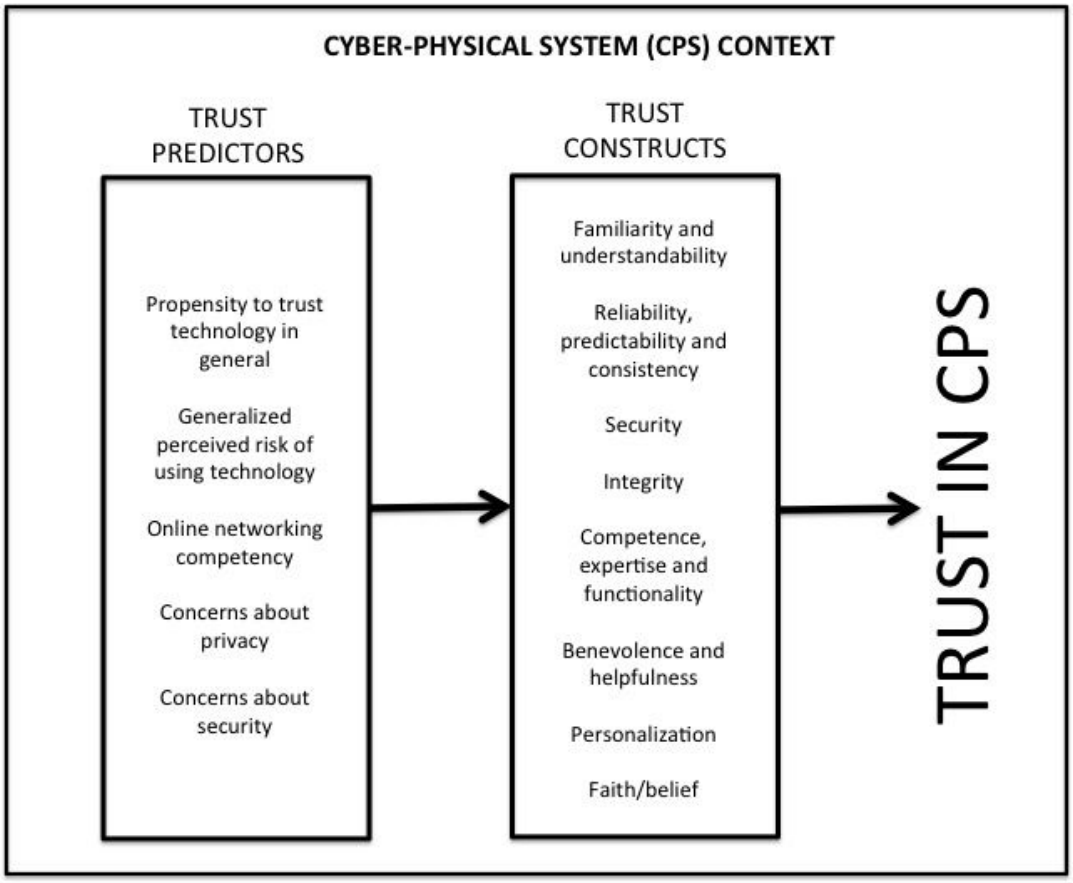


Figure 2: Proposed Path Model and Hypotheses

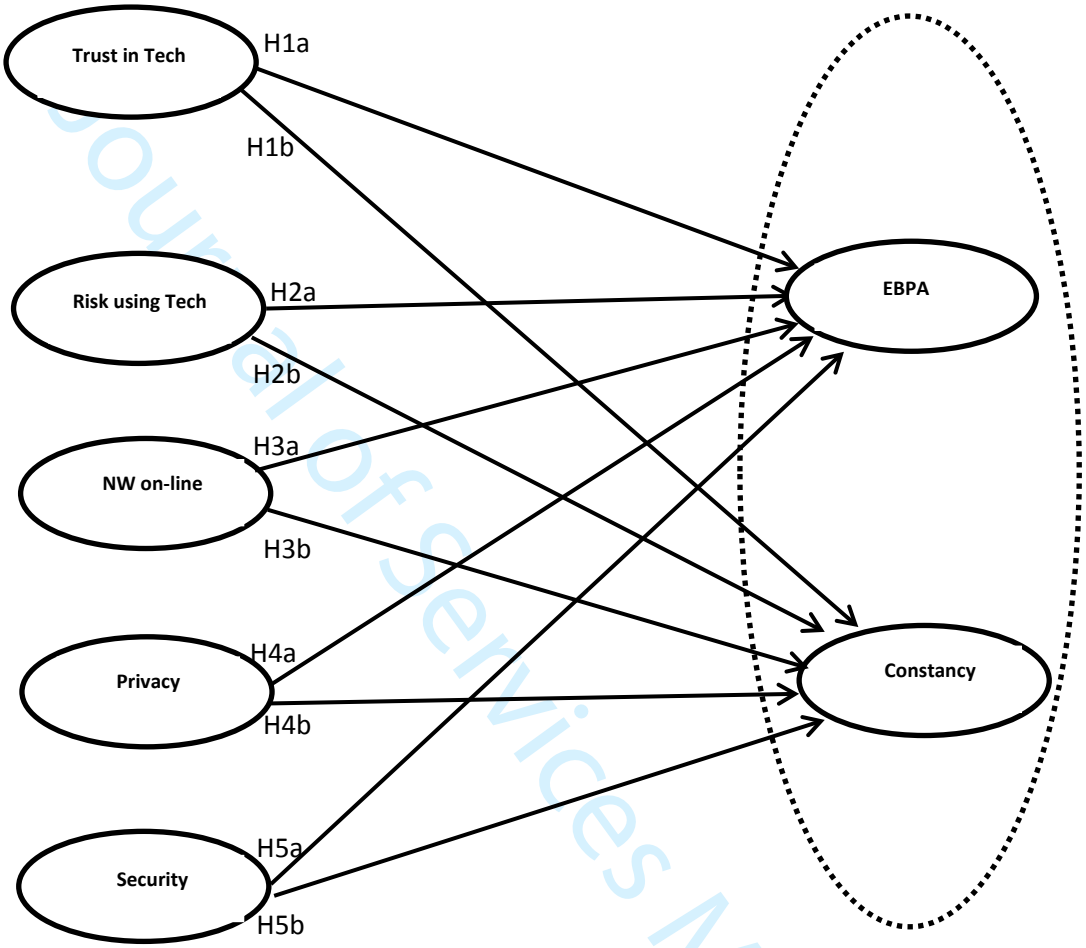
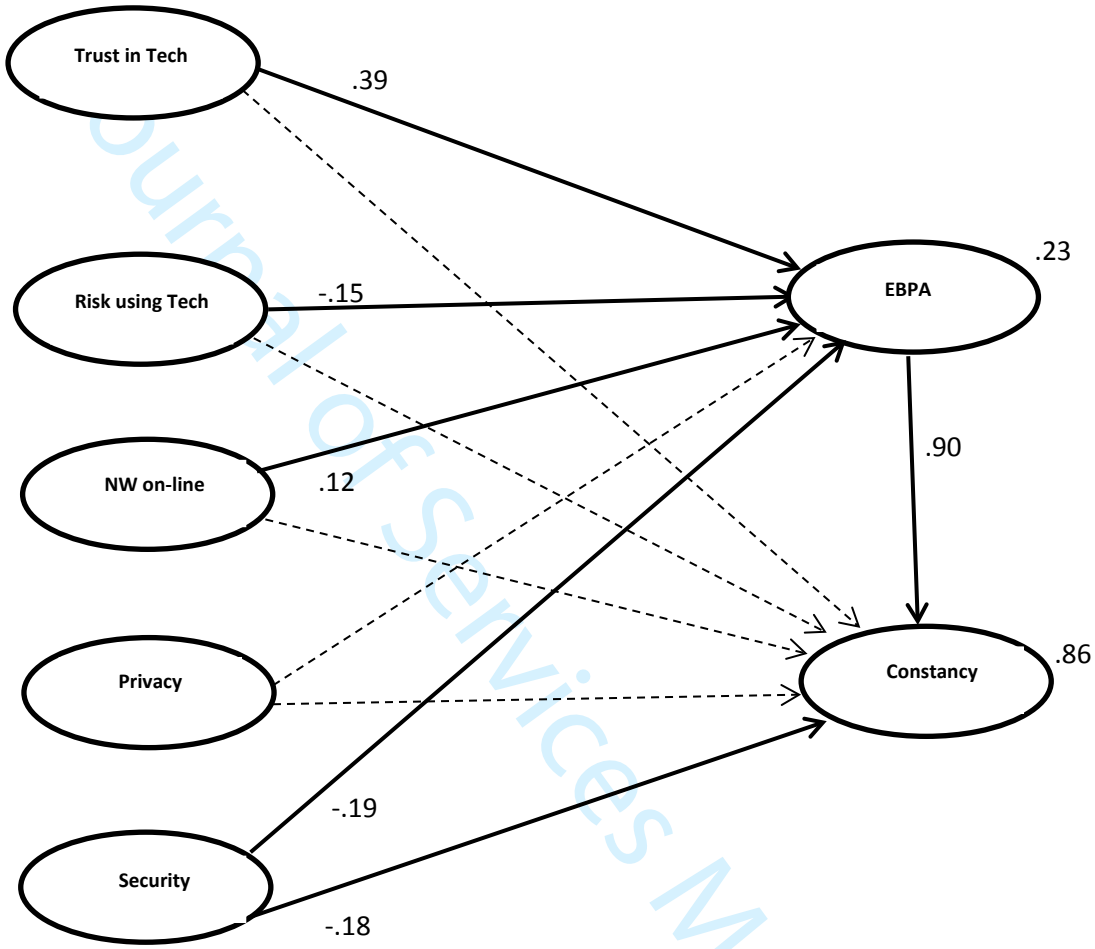


Figure 3: Path model with Significant Paths



Note: Fit Measures: RMSEA=.056; RMR= .036; CFI=.931; GFI= .861, NFI=.883, ——▶ $p < 0.05$, - - - -▶ means path not significant.