Received 11 November 2016
Revised 3 March 2017
Accepted 28 March 2017

Internet of Things: understanding trust in techno-service systems

Tracy Harwood
Institute of Creative Technologies, De Montfort University, Leicester, UK, and
Tony Garry
Department of Marketing, University of Otago, Dunedin, New Zealand

Abstract

Purpose – The characteristics of the Internet of Things (IoT) are such that traditional models of trust developed within interpersonal, organizational, virtual and information systems contexts may be inappropriate for use within an IoT context. The purpose of this paper is to offer empirically generated understandings of trust within potential IoT applications.

Design/methodology/approach – In an attempt to capture and communicate the complex and all-pervading but frequently inconspicuous nature of ubiquitous technologies within potential IoT techno-systems, propositions developed are investigated using a novel mixed methods research design combining a videographic projective technique with a quantitative survey, sampling 1,200 respondents.

Findings – Research findings suggest the dimensionality of trust may vary according to the IoT techno-service context being assessed.

Originality/value – The contribution of this paper is twofold. First, and from a theoretical perspective, it offers a conceptual foundation for trust dimensions within potential IoT applications based upon empirical evaluation. Second, and from a pragmatic perspective, the paper offers insights into how findings may guide practitioners in developing appropriate trust management systems dependent upon the characteristics of particular techno-service contexts.

Keywords Trust, Internet of Things, Risk, Ecosystem, Trust management, Techno-service system

Paper type Research paper

Introduction

This paper conceptualizes and explores relational trust within the context of the Internet of Things (IoT). The IoT is built upon the rapid development of internet, mobile, near field technologies (such as Wifi and Bluetooth) and communication networks (Schrammel *et al.*, 2011). Its foundations can be found in various works that underpin the development of artificial intelligence, where technology systems may reflect anthropomorphic reasoning based on human psychophysiological traits (Minsky, 1988, 2006). Important contributors to this are Turing and von Neumann (see Russell and Norvig, 1995; Weiss, 1999) and system control theory (see Masani, 1985 for a review of the collected works of Wiener, father of cybernetics; Kalman's, 1960 predictive algorithm; Pearl's, 2000 development of a calculus for probabilistic and causal reasoning). The interconnected technologies render new types of services to end users, albeit the technologies themselves are often ubiquitously consumed in their environment as a collective, made visible (at present) only through touchpoints such as smart devices and wearable technologies. Current predictions suggest that within a decade, IoT will consist of

This paper forms part of a special section colloqium on relationship marketing.

An earlier version of this paper was presented at the 24th International Colloquium on Relationship Marketing (ICRM) held in Toulouse, France from 6 to 8 September 2016. Dr Andreas Munzel, Associate Professor of Marketing at the IAE Toulouse School of Management, Université Toulouse 1 Capitole, France served as the Special Section Guest Editor for this paper.

Journal of Service Management
Vol. 28 No. 3, 2017
pp. 442-475
Emerald Publishing Limited
1757-5818
DOI 10.1108/JOSM-11-2016-0299

billions of objects and devices or things that have the potential to seamlessly connect people to produce services and interact and share information about themselves with each other and their environment to render services (Eloff *et al.*, 2009). Advocates of the IoT interpret its emergence as a "new industrial revolution that will boost productivity, keep us healthier, make transport more efficient, reduce energy needs and tackle climate change" (Cameron, 2014). However, the gap between recent press coverage of the potential socio-economic consequences of the IoT and empirically based research is significant. Whilst there is a considerable programme of collaborative research being undertaken across the EU and USA into IoT technologies, the primary focus of this is the development of hardware technology and the adoption of standardized platforms and protocols. That said, many potential applications of the IoT will involve relational challenges not faced within current marketing contexts including traditional (e.g. B2C and C2C) but also parasocial and machine (M) relationships (C2M and M2M). The relational consequences on users within such service contexts and the "smart environments" they inhabit have yet to be explored in the complex many-to-many networked ecosystem that encompasses the IoT environment (Wuenderlich *et al.*, 2015).

Within an IoT ecosystem, benefits are embedded within the value of products and services. Implicit within this value proposition is an agreement that the user allows service providers (and product owners) to use data generated from transactions and interactions that incorporates psychophysiological and behavioural information and its reuse at organizational-user and potentially societal levels (Bolger, 2014). Such data will increasingly be integrated with environmental data from the user's wider context (e.g. cityscape, etc.). However, an IoT ecosystem may have no cardinal or central actors on which to focus user-trust decisions (Bao and Chen, 2012). Additionally, machines may exhibit user perceived "smartness" (Bandura, 2001; Rose and Truex, 2000; Engen *et al.*, 2016) evoking an illusion of self-awareness, flexibility, transformability and self-decisiveness (Atzori *et al.*, 2010; Gubbi *et al.*, 2013; Yang *et al.*, 2013). Furthermore, they may be used to predict service demand, develop entirely new service offerings or influence behaviour at a moment in time. Such potential characteristics of the IoT have implications for the nature of user trust and how traditional models developed in interpersonal, relational marketing and virtual contexts (Taddei and Contena, 2013) may be transformed for use within an IoT context (Schrammel *et al.*, 2011).

This study aims to offer empirically generated understandings of user trust within potential IoT contexts. To this end, the contribution of this research is twofold. First, and from a theoretical perspective, it offers a conceptual foundation for trust dimensions within potential IoT applications based upon empirical evaluation. Second, and from a pragmatic perspective, the conceptual models derived from this research may aid practitioners in developing more appropriate user-trust management systems in the rapidly evolving context of the IoT. The paper is structured as follows. First, the existing literature on the nature of IoT as a techno-service system is examined before examining the potential attributes of trust within such systems. Subsequently, the methodology adopted to address the research aim is explained and the scoping of potential applications of the IoT, the development and testing of scenarios based on these and the administration of a quantitative survey is outlined. Thereafter, and reflecting the potential IoT applications identified, findings are presented in three areas: an IoT transport context, an IoT household context and an IoT health context. Our discussion of the findings elaborates on the dimensions of user-trust and the consequences of these on trust management systems within IoT environments before conclusions are drawn and directions for future research are suggested.

Literature review

Reminiscent of Vargo and Lusch's (2011) service ecosystem, the IoT is a contemporary example of a techno-service system that renders synchronized actions for end-user consumption (e.g. Hojer and Wangel, 2015). Historically the phrase "techno-service system"

was used to portray a complex system of interactions between humans and machines primarily within an intra-firm context (e.g. Emery and Trist, 1960), where emphasis was on human interaction with, and influence over, some technologically enabled system (see e.g. Mumford, 2006). More recently, however, it has been used to describe multi-actor environments, such as smart cities and homes that encompass human-machine agency across networks within IoT contexts (e.g. Engen *et al.*, 2016; Jia *et al.*, 2012). Within such contexts, machines exhibit what may be increasingly interpreted as agency by users through their perceived "smartness" (Bandura, 2001; Rose and Truex, 2000; Engen *et al.*, 2016). This perceived smartness is derived from technologies embedded into "things" that have synergistic capability in acquiring and processing data through electronics, software, sensors and network connectivity. This in turn may lead to an illusion of self-awareness, flexibility, transformability and self-decisiveness (Minsky, 1988, 2006; Atzori *et al.*, 2010; Gubbi *et al.*, 2013; Yang *et al.*, 2013). Augmenting this further, where desired outcomes cannot be achieved without human-machine interaction, perceived collective agency may result (Bandura, 1997; Engen *et al.*, 2016) leading to increased levels of efficiency, convenience and decision making (Weinberg *et al.*, 2015).

Fundamental to human-machine interactions is the notion that trust acts as a mediator (Engen *et al.*, 2016). Crucially in an IoT environment there may be no cardinal or central entity (individual human or machine) on which service users may focus trust decisions (Bao and Chen, 2012) that enables them to judge the acceptability of a system. As such, trust is not well understood or consistently defined within this context (e.g. Atzori *et al.*, 2010; Gao and Bai, 2014; Chen *et al.*, 2015). This is somewhat surprising when rhetoric suggests IoT technologies will enable firms to devise new service offerings that incorporate greater optimization, customization and autonomy (Iansiti and Lakhani, 2014; Porter and Heppelmann, 2014) leading to higher levels of engagement, satisfaction, and ultimately, stronger relationships (Neuhofer *et al.*, 2015). In an attempt to address this, this research endeavours to examine why and how trust foundations may be different within IoT contexts and, subsequently identify underlying trust dimensions.

Differentiating human-trust within the context of IoT

An exchange view of marketing suggests the underpinning bond between the firm and customer comprises financial (price), social (communications) and structural (value-in-use) components (Chou, 2009) that influence the customer at cognitive and emotional levels (Park *et al.*, 1986). Furthermore, calculative commitment, particularly in relation to structural bonds, has been found to be a reasonable measure of trust (Morgan and Hunt, 1994) and this in turn may lead to satisfaction with the value proposition and subsequently relational commitment (see Seppänen *et al.*, 2007, for a summary of the literature in this area). However, from this perspective, trust is not a part of the proposition itself but considered to be an antecedent to or consequence of the relational aspects of service delivery. As previously highlighted, in an IoT context there may exist no cardinal or central entity (human or machine) on which end users of services may focus trust decisions (Bao and Chen, 2012). Within these multi-partite environments, trust becomes a fundamental component of the value proposition itself, residing within and across a network of actors and objects. It is embedded within the data derived from interactions and behavioural responses and re-used to provide services for consumption by the provider, their personal or extended network and other beneficiaries in the wider network (e.g. Bapna *et al.*, forthcoming). This is borne out of the emergence of the ubiquity of technologies and more specifically, the embedded nature of technologies that extend and bind the relationship beyond the originating firm to include third parties in a customer focussed proposition delivery network (see Appendix 1 for an example of a wearable proposition). Interactions within IoT networks involve exchanges between different types

of agency (Gummesson and Grönroos, 2012), with relationships existing between those closely linked and distally networked in the enactment of some service experience for an end customer. In effect, the customer engages not with individuals within the network but with the service system. This system includes other customers, businesses, public services, devices, machines and software (e.g. Frow *et al.*, 2014). From an actor's perspective within the system, they will likely be unaware of the full extent of their role or the range or scope of activities encompassed within the IoT network they are interacting with to deliver a service or receive an experience. As such, user-trust may be treated as a strategic management opportunity critical to network sustainability and service development, which is separate to the technical system design aspects that may limit or control information use. Trust management may therefore refer to a declaration of credential (personalized) information, or disclosure of relevant information (customized), often decentralized across a distributed network of actors and objects.

Whilst familiarity and understanding are considered and accepted as core components of human-trust, within the IoT environment many of the interactions may be beyond the cognition of actors. Visualizing the complexity of such networks is challenging (e.g. Jaakkola and Alexander, 2014). Lataifa (2014) suggests evaluating value generated through such networks is not a "trivial task", with vast amounts of data (information) to be analysed. Such complexities are exacerbated by the all-pervasive but inconspicuous nature of the technologies within the network that create potentially new dimensions of complexity in the data generated and the flow and control of information based upon computational intelligence (e.g. Fritsch *et al.*, 2012). Consequently, human-trust as traditionally conceptualized for dyadic relationships (e.g. Morgan and Hunt, 1994) cannot be easily applied because of imperfect knowledge and/or understanding of or familiarity with the service system, its actors and their agency. Confidence in the system therefore becomes critical and is a function of limited information and limited evaluation (knowledge) of potential alternatives. In such circumstances, trust may be merely an indicator of confidence (Giddens, 1990) or indeed be faith-based and blind (Simmel, 1978). Thus, the nature of trust may differ according to the agency of human actors and machine objects within the network (Moore, 2006; Engen *et al.*, 2016). Actors and objects effectively work collectively as a complex adaptive socio-technical system, with benefits derived from the interdependencies within the networked systems (e.g. Mele and Polese, 2011; Chandler and Lusch, 2015; Engen *et al.*, 2016).

Notions of individuals (say, service consumers/users) entering relationships with IoT systems and the range of agents within them, particularly in terms of relationships with "intelligent" machines that assimilate the behaviour of other humans, has recently received increased attention (see e.g. Weizenbaum, 1966; Nass *et al.*, 1996; Ferrucci *et al.*, 2013). From an information systems (IS) perspective, research has primarily concentrated on hardware technology and the adoption of standardized platforms and protocols, where "trust management" has been developed as a risk management tool using algorithm-based ratings mechanisms that are typically incorporated into social networking sites such as eBay and Amazon (e.g. Friedman *et al.*, 2007; Aggarwal and Yu, 2008). IS research has, however, tended to ignore the human decision making and recommendation provision elements that IoT systems will potentially fulfil (e.g. Söllner *et al.*, 2014). Thus, theoretically and empirically based examinations of trust within IoT contexts are warranted. To this end, notions of trust from different disciplines were reviewed in an attempt to examine and capture the potential multi-disciplinary theoretical foundations of trust and their potential contribution to trust within a techno-service system context. These included: interpersonal (e.g. Rempel *et al.*, 1985) and organizational (e.g. Smith *et al.*, 2013) trust literatures; IS and automation literatures (e.g. Dimoka, 2010; Gefen and Pavlou, 2012; Cho *et al.*, 2015), computing and networking literatures (e.g. Janson *et al.*, 2013), virtual and online trust literatures (e.g. Hong 2015) and human-computer interface literatures (e.g. Madsen and Gregor, 2000).

Theoretical foundation

Whilst many interpretations of trust position it in terms of "accepted vulnerability to another's ill will (or lack of good will)" (Friedman *et al.*, 2000), our review identifies a much wider interpretation of trust and suggests trust has been measured in a variety of ways within a variety of disciplines. Pertinent to this research, McKnight *et al.* (2011) propose 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). Additionally, whilst recognizing that trust is an evolving and dynamic process, for the purposes of this research is to follow Söllner *et al.*'s (2014) lead and focus on initial trust when a user may be first exposed to a potential techno-service system experience. This may be justified on the grounds that when users first interact with a potentially unfamiliar techno-service system, perceptions of uncertainty and risk are particularly salient and consequently there needs to be a sufficient level of trust to overcome these perceptions (McKnight *et al.*, 2011). In attempting to identify, adapt and apply trust constructs more "palatable" to techno-service contexts, the framework proposed by McKnight *et al.* (2011) is drawn on and augmented for differentiating between interpersonal and technology-based trust constructs through the addition of a third object of dependence: techno-service systems. In doing so, three key dimensions are used: contextual conditions, the object of dependence and the nature of trustor expectations in relation to object attributes. These are now discussed in more depth followed by a theoretical justification of proposed trust constructs within a techno-service system context.

Contextual conditions

Trust situations involve risk and uncertainty. Trustors, to varying degrees, will lack control over outcomes because of the necessity to rely on another object to achieve a task. Hence, there is the notion of accepted vulnerability involving another object. Consequently, there is a risk that the trustee will not fulfil the trustors expectations. This is regardless of whether the object of trust is a person, a machine or, in this instance, a techno-service system. This may be intentionally through moral choice (by a person) or through failure to act as expected (by a machine) or a combination of the two as may be the case in a techno-service system context (McKnight *et al.*, 2011).

Object of dependence

Trust will differ depending on the nature of the object. With interpersonal trust, there is a moral and volitional dimension (Berscheid, 1993). However, McKnight *et al.*, (2011) posit that with technology there is still trust. This will focus on a specific technological object which they interpret as being a "human created artefact with a limited range of capabilities that lacks volition and moral agency" (p. 125). However, as the technological object will lack volition and moral agency, trust may reflect perceptions about the attributes of the technology rather than its motives and/or moral agency (McKnight *et al.*, 2011). Within a techno-service system context, there may be no central or individualized object (person or device) on which to focus trust decisions. Within such systems, there is potential for interpersonal and technological characteristics and attributes to be indistinguishable from each other thus making judgements about moral and volitional issues impossible.

Nature of trustor's expectations

When contemplating trust, individuals will consider different attributes and have different expectations about the object on which the trust decision is being based (Mayer *et al.*, 1995; McKnight *et al.*, 2011). An examination of the trust literature identifies common themes or threads related to such attributes which may be "abstracted from the multiplicity of trust conceptualisations across disciplines" (Bhattacherjee, 2002, p. 213). The following

discussion focusses on only those attributes that have consistently appeared when theorists within these interpersonal- and technology-related disciplines have examined trust. Drawing on this dialogue, this paper theorises their appropriateness and form within a techno-service system context. This is summarized in Table I and elaborated below.

Object attribute	Interpersonal	Technology	Posited within techno-service systems
Familiarity and understandability	Knowledge and understanding of dispositional attributions and traits of partner (e.g. Rempel *et al.*, 1985)	Employing procedures, terms and cultural norms that are familiar and understandable (e.g. Madsen and 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 *et al.*, 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
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 and 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 *et al.*, 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
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 and Sherman, 1998)	Perceived ability to fulfil security requirements such as authentication, encryption and non-repudiation (e.g. Cheung and Lee, 2001)	Refers to feelings of security specifically related to issues of information management when interacting with another entity within a smart service system
Personalization	Dyadic interactions between intimates resulting in understanding and "caring responses" from partners (e.g. Rempel *et al.*, 1985)	The extent to which an object understands and represents the personal needs of the user (e.g. Komiak and Benbasat, 2006)	Understanding user needs and the generation of relevant and personalized recommendations "Only here, only me and only now"
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 *et al.*, 2011)	User's perception that the smart service system will act according to the user's best interest
Faith/Belief	Belief based on non-rational but may be triggered by evidence, signs or experience (e.g. Castelfranchi and Falcone, 2010)	Belief that technology will perform in situations in which it is untried (e.g. Madsen and Gregor, 2000)	Belief that a smart service system will perform appropriately even when there is limited understanding and/ or familiarity

Table I. Conceptual comparisons of trust between interpersonal, technological and techno-service systems literatures

Familiarity and understandability

Within an interpersonal trust context, familiarity and understanding is widely recognized as referring to a knowledge and comprehension of the dispositional attributions and traits of a partner (Rempel *et al.*, 1985). From a technological perspective, familiarity refers to an entity employing procedures, terms and cultural norms that are "familiar, friendly and natural" (Madsen and Gregor, 2000). The potential complexities of IoT systems previously highlighted suggest the notion of "forming a mental model of a system and consequently being able to predict its future behaviour" (Janson *et al.*, 2013, p. 5) may be particularly pertinent in forming trust judgements within such contexts (Söllner *et al.*, 2014).

Reliability, predictability and consistency

From an interpersonal trust perspective, reliability, predictability and consistency relates to the degree to which an individual can be relied on to act in a predictable manner whilst exercising their volition or freedom to choose (McKnight *et al.*, 2011). Whilst recognizing that technology has no volition, it may still function in an unreliable or erratic manner (McKnight *et al.*, 2011). Hence, within this context, the work of Cho *et al.* (2015) and McKnight *et al.* (2011) is drawn on to propose that reliability refers to the belief that the techno-service system will operate properly and in a consistent manner.

Integrity

Killinger (2010) defines personal integrity as "the quality of being honest and having strong moral principles; moral uprightness". However, when referring to integrity, Bhattacherjee (2002) proposes that adhering to a set of rules or procedures is not adequate in itself. Such procedures must be perceived as being "fair and reasonable". Integrity generally refers to notions of "honesty", "credibility", "fulfilment of promises" (Sekhon *et al.*, 2014) and "doing the right thing" (Butler, 1991). Pfleeger and Pfleeger (2011) suggest integrity within technological contexts refers to notions of "data integrity" and encapsulates users' perceptions that personal data will not be changed without users being given notice. Within a techno-service system context it is proposed that integrity is related to procedural fairness insofar as there is perceived to be reasonable adherence to processes and procedures regarding the management of personal information within such systems.

Competence, expertise and functionality

Competence as an attribute is frequently associated with "experience" and "expertise" (e.g. Moorman *et al.*, 1992; Doney and Cannon, 1997) and signals the capacity to achieve an outcome (Sekhon *et al.*, 2014). Users consider whether a technological device has the attributes to deliver the functionality promised to complete a task (McKnight *et al.*, 2011). For the purposes of this research it is proposed that competence, expertise and functionality refer to the perceived ability of a techno-service system to achieve a particular outcome.

Security

Drawing on interpersonal trust literatures, Sheppard and Sherman (1998) identify security as being related to the risk of indiscretions insofar as the trustor assumes that sensitive information revealed through "intimate disclosures" will not deliberately or inadvertently be shared by a partner. Within a technology context, consensus suggests perceived security focusses on the ability to fulfil security requirements such as authentication, encryption and non-repudiation (e.g. Cheung and Lee, 2001). It is posited that within a service system context, security refers to how secure a user feels interacting with the overall system and more specifically, the extent to which they believe the system is "secure for collecting and transmitting sensitive information" (Salisbury *et al.*, 2001; Gefen and Pavlou, 2012).

Personalization

From an interpersonal trust perspective, dyadic interactions "between intimates" will result in distinctive and individualized "caring responses" (Rempel *et al.*, 1985). Within a technological context, Komiak and Benbasat (2006) posit that personalization refers to the extent to which an object interprets and represents the personal needs of the user. Within techno-service contexts it is proposed that the interpretation of user needs and the reasoning processes related to these will generate perceived personalized provision of recommendations to the user (e.g. Söllner *et al.*, 2014). From a user perspective, this may be interpreted as "Only here, only me and only now" (Chen, 2012).

Benevolence and helpfulness

Interpersonal literature generally surmises that benevolence and helpfulness are attuned to acting in the other party's interest (Mayer *et al.*, 1995). Implicit within this is a lack of opportunistic behaviour (Morgan and Hunt, 1994). However, because technology has no moral agency, there is no sense of emotive caring and helpfulness becomes a purely instrumental process (Beatty *et al.*, 2011). Hence, McKnight *et al.* (2011) posit that users may consider the "help" function on technological devices as providing the necessary advice to complete a task. From a techno-service system perspective, benevolence and helpfulness have been interpreted as the user's perception that the system will holistically act in their best interest and provide advice when necessary or requested to do so.

Faith

At an interpersonal level, faith refers to a belief based on non-rational grounds (Castelfranchi and Falcone, 2010) that may be triggered by evidence, signs or experience (Cho *et al.*, 2015). From a technological perspective, Madsen and Gregor (2000) discuss faith in terms of the belief that an object will perform even in situations where it has not previously been applied. These are reflective of our interpretation within a techno-service system insofar as faith may be based on a limited understanding and/or familiarity with a system but a belief that it will perform appropriately.

This review of the literature identifies a number of issues that question the appropriateness of trust models that draw on the extant human-technology-trust literatures to techno-service contexts. To this end, the purpose of this study is to offer empirically generated understandings of trust within such contexts. In doing so, possible trust attributes pertinent to techno-service systems are identified and theorised. Having introduced these, the next section details the processes used to "discover" (Floyd and Widaman, 1995) how these trust components interact within potentially different techno-service contexts.

Methodology

In designing the methodological approach, the imperative was to capture and communicate the potentially complex and all-pervading but frequently inconspicuous nature of ubiquitous technologies within IoT contexts. To address this challenge, a three-stage approach was adopted: first, scoping potential applications; second, developing and testing scenarios based on these; and third, conducting a quantitative survey using the identified constructs.

Scoping potential applications of the IoT

Whilst the IoT is a rapidly evolving service environment, it is as yet still piecemeal in its emergence, thus the precise nature and manifestation of service environments and how these will evolve is unclear. For this reason, traditional research methods into the nature of

consumer behaviours within such a context seem inappropriate. Visualizing the characteristics and complexity of systems that do not currently exist is problematic and may present challenges to potential respondents. To address this, this research draws on transdisciplinary techniques to help frame likely research questions that are both relevant and aligned with practice. Ozanne *et al.* (2011) propose that in order to advance consumer research, a more transformative practice should be undertaken, where transdisciplinary approaches help to frame problems and potentialities from the consumer perspective (Nicolescu, 2002). Consequently, research is conceptualized more broadly and the impact is more meaningful (Mick, 2006; Ozanne *et al.*, 2011). Arts have been suggested to be particularly helpful in thinking about consumption practices in new ways, not least because they assist in generating interesting and engaging ways to express ideas (Ozanne *et al.*, 2011). Capitalizing on the visual character of contemporary consumer culture has already been established as a methodological process in marketing research (e.g. Belk and Kozinets, 2005; Lemke, 2007; Schembri and Boyle, 2013). Despite this, a filmic approach to storytelling has received little attention as a potential contribution to marketing. It has been argued, however, that videography is useful in documenting and describing happenings, events and artefacts that disclose experiences for analysis (Sayre, 2001; Belk and Kozinets, 2005). Therefore, the research drew on the scientific, technology and artistic communities to devise visual materials with which to engage consumers in discussions that identify key issues for research.

Developing and testing scenarios

Pauwels' (2011) three-stage integrated framework of visual social research is used to structure the projective materials (origin and nature of visual; research focus and design; and, format and purpose):

(1) The origin and nature of visuals: the first stage involved identifying a breadth of emergent IoT technologies and classifying them by potential use, according to scientific and technology development intentions. This was not an exhaustive process but thematically generative in nature. During this stage, "found images" were collated (Pink, 2007; Pauwels, 2011) and descriptions of key IoT applications, noting sources and acceptable uses. Images from a range of internet sources using key search terms were generated through participation in thematically related virtual communities (social media special interest groups, often comprising early adopter consumers as well as artists, scientists and technologists). The resultant data set of images was initially grouped by practical applications of the technologies; thereafter a single image representing each different technology-in-use was identified. In some instances, this represented an imagined future use scenario or product. This material was accumulated over a period of four years.

(2) Research focus and design: content analysis (Krippendorff, 2013; Berelson, 1952) revealed cultural contexts for IoT technologies that related to three overarching areas of potential consumer application: managing personal health and well-being; social and home life; and, travel. Using these contexts, storyboards and scripts that depicted scenarios of IoT technologies in use were then developed with the intention of developing these into films. In order to visualize scenarios, and ensure films remained short, fictional idealized characters and actions were devised that could be further developed to illustrate consumption practices and patterns within an IoT context. Stories were then generated that enabled interactions between characters, extrapolating the potential of the technologies in use to connect actors across networked communities with devices with the service environment.

(3) Format and purpose: this stage involved pre-testing the devised scenarios to evaluate the relevance and realism of IoT contexts. A focus group discussion was used, involving a cross-section of 15 researchers and industry participants with different disciplinary interests (science, technology, arts and marketing) and levels of knowledge and experience of IoT development and application. The primary aim was to explore any unintended influences in the representational practices and characters within the storyboards constructed in the previous stage. Feedback was positive and receptive, resulting in minor amendments to scripts to more tightly define servicescapes of use (see Appendix 2 for final scripts of characterizations of actors and the scenarios).

In order to depersonalize characters, and minimize production costs, a machinima filmmaking technique was used to animate visuals. Machinima (machine-cinema) is a relatively low cost creative medium that uses 3D computer video games to make high definition animated films. One such game environment commonly used is Second Life®. An experienced film producer/director was selected and briefed to translate the visual and textual scenarios into short films. The producer/director was responsible for recruiting actors, designing and building sets, directing, editing and production. The researchers viewed interim stages of the process, commented on set designs, characters and enacted scenarios, including the interplay between and hierarchy of elements in each film. A voiceover describing the characterisations, scenes and actions was used to add depth and as a creative device. In all, three scenarios were created with a separate introduction to the scenarios that introduced the characters to participants. These were subsequently embedded as a projective tool into three versions of a questionnaire and cross-sectional data collected related to trust dimensions for these. The next section describes the methodology and findings related to this stage of the research.

The quantitative survey

The questionnaire comprised three key parts. The first section consisted of questions designed to collect classification information relating to age, gender, etc. The next section comprised a series of questions related to abstract attitudes to technology. These centred on behavioural and generalized attitudes in relation to trust in technologies (McKnight *et al.*, 2002) and perceived risks of using technologies (Yan *et al.*, 2014). Respondents were then required to view the film "Introduction to the Walker Family" and were asked to rate how realistic they considered the scenario depicted in the film to be (very realistic, realistic, unrealistic and very unrealistic). Subsequently, using a quota process, respondents were allocated to one of the three filmed scenarios depicting applications of IoT. Again, they were asked to rate how realistic they considered the scenario to be (very realistic, realistic, unrealistic and very unrealistic). Pre-existing indicators for the relevant trust constructs identified were used to examine trust dimensions. More precisely, indicators for reliability (McKnight *et al.*, 2011), benevolence (Bhattacherjee, 2002), faith (Madsen and Gregor, 2000), personalization (Komiak and Benbasat, 2006), security (Salisbury *et al.*, 2001), competence (McKnight *et al.*, 2002), understandability (Madsen and Gregor, 2000) and integrity (McKnight *et al.*, 2002) were employed. These were adopted and adapted to each IoT context. Details of the measurement instrument may be found in Appendix 3. To assess each item, a five-point Likert scale was used that asked respondents to "rate the extent to which you would agree or disagree with the following statements" (1 = strongly disagree and 5 = strongly agree). The questionnaire was extensively pre-tested. This was achieved by administering the questionnaire with two sets of respondents. The first set comprised of a pilot group of respondents. The second set comprised "academics knowledgeable in the field" (Bagozzi, 1994). Feedback provided by each group was subsequently incorporated in the questionnaire and appropriate amendments made.

Data collection

Data were collected in early 2016. Employing a global market research agency within New Zealand, a quota sampling process was used to ensure a sample representative of the national population in terms of age and gender (over 18s only). The data were collected using an online interface (Deutskens *et al.*, 2006). In total, 1,200 usable responses (400 per IoT scenario) were collected and analysed.

Findings

Data were analysed using SPSS (Version 22) software. Prior to conducting the analysis, it was necessary to check how realistic respondents perceived the three film scenarios and introductory film to be. In total, 88.2 per cent of all respondents considered "Introduction to the Walker Family" to be "realistic" or "very realistic". In total, 88.5 per cent of assigned respondents considered the Household Management (HHM) System scenario to be "realistic" or "very realistic". In total, 67.5 per cent of assigned respondents considered the Travel Management (TravM) System scenario to be "realistic" or "very realistic" and 75 per cent of assigned respondents considered the Treatment Management (TM) System scenario to be "realistic" or "very realistic". These values were considered sufficiently high to continue with analyses. Descriptive statistics for the sample are provided in Table II.

An analysis of the bi-variate correlation table revealed a large number of items to be moderately or highly correlated with a significant number of r values of 0.50 or higher (Cohen, 1988). This would suggest issues with discriminant validity (see Appendix 4) (Bagozzi *et al.*, 1991; McKnight *et al.*, 2002) Additionally, α tests of the original scales within each context ranged from 0.644 to 0.88. Given that these constructs had never been tested together before and given the unique nature of the contexts in which they are being applied, it was deemed appropriate to conduct exploratory factor analysis (EFA) to identify underlying dimensions within each construct.

EFA of the trust component of the survey instrument was conducted across the three scenarios. Initially, the suitability of the data for factor analysis was assessed across all three scenarios. Inspection of the corresponding correlation matrices for each scenario revealed the presence of a large number of coefficients of 0.3 and above. The Kaiser-Meyer-Olkin value exceeded the recommended value of 0.6 (Kaiser, 1970) in all three contexts (0.955 for the Travel Management System, 0.960 for the HHM System and 0.970 for the TM System). Additionally, Bartlett's test of Sphericity (Bartlett, 1954) reached statistical significance within all three scenario data sets. Preliminary findings suggested differences in the results for the dimensionality of trust across the IoT scenarios presented. These are now discussed.

The transport (TravM) system scenario

This EFA resulted in a three-factor solution accounting for 64.1 per cent of the variance. All items loaded significantly with a minimum of 0.35 for a sample of this size (Hair *et al.*, 1995). With one item there was significant cross-loading ("The TravM system would know what I want") and this item was removed from further analysis (see Table III). Loading on Factor 1 accounted for 52.8 per cent of variance, loading on Factor 2 accounted for 7.2 per cent of the variance and loading on Factor 3 accounted for 4.1 per cent of the variance. The reliability of all the scales was established by utilizing Cronbach's α. Factors 1, 2 and 3 had α scores of 0.931, 0.806 and 0.841, respectively. These values are all above 0.7, so the scales can be considered reliable for this sample with this test.

The HHM System scenario

This EFA resulted in a two-factor solution accounting for 61.3 per cent of the variance. All items loaded significantly. Again, one item cross-loaded ("The HHM system would be honest")

Overall (n = 1,200)					
Age (%)	18-25	26-40	41-55	56-70	71+
Gender (%)	Male	Female			
	46	54			
Education (%)	No formal qualifications	School leavers	Certificate or diploma	Degree	Post-graduate
	7	26	28	24	15
Living environment	Rural	Semi-Rural	Urban		
	9	15	76		
Scenario: the Transport (TravM) System scenario (n = 400)					
Age (%)	18-25	26-40	41-55	56-70	71+
	16	27	20	29	8
Gender (%)	Male	Female			
	45	55			
Education (%)	No formal qualifications	School leavers	Certificate or diploma	Degree	Post-graduate
	7	27	25	26	15
Living environment	Rural	Semi-Rural	Urban		
	10	14	76		
Scenario: the Household (HHM) System scenario (n = 400)					
Age (%)	18-25	26-40	41-55	56-70	71+
	17	27	22	25	9
Gender (%)	Male	Female			
	46	54			
Education (%)	No formal qualifications	School leavers	Certificate or diploma	Degree	Post-graduate
	7	26	27	25	15
Living environment	Rural	Semi-Rural	Urban		
	11	16	73		
Scenario: the Treatment (TM) System scenario (n = 400)					
Age (%)	18-25	26-40	41-55	56-70	71+
	16	27	20	24	13
Gender (%)	Male	Female			
	48	52			
Education (%)	No formal qualifications	School leavers	Certificate or diploma	Degree	Post-graduate
	6	26	30	20	19
Living environment	Rural	Semi-rural	Urban		
	8	14	78		

Table II.
Descriptive statistics

and this item was removed from further analysis (see Table IV). Factor 1 accounted for 55.0 per cent of variance and Factor 2 accounted for 6.3 per cent of the variance. Once again, the reliability of the scales was established by utilizing Cronbach's α. Factors 1 and 2 had α scores of 0.912 and 0.847, respectively and, being above 0.7, may be considered reliable for this sample with this test.

The TM System scenario

This EFA resulted in a one-factor solution accounting for 65.3 per cent of the variance. All items loaded significantly suggesting trust within this context is uni-dimensional (see Table V). The Cronbach's α for this dimension was 0.971 suggesting the scale can be considered reliable with this test.

Item	Factor 1: constancy	Factor 2: understandability familiarity	Factor 3: performance assessment
Safe place to coll. and rec. sensitive info.	0.943		
Concerned about my personal privacy	0.821		
Faith in the TravM system providing the best advice	0.767		
Accept the TravM system's advice	0.701		
Truthful in its dealings with me	0.700		
Would keep its commitments	0.688		
Has the skills and expertise to make correct decisions	0.675		
Feel secure with sensitive info. being collected	0.674		
Would act in my best interest	0.629		
Would be honest	0.615		
Would be dependable	0.560		
Would be open and receptive to my needs	0.499		
Understand how work		0.899	
Understand how assist me with decisions		0.787	
Easy to follow what does		0.773	
Would perform reliably			0.799
Would do its best for me			0.784
Would correctly use the information provided			0.775
Would understand my needs			0.729

Table III.
Factor analysis results for the trust component in the Transport Management (TravM) System scenario

Item	Factor 1: constancy	Factor 2: experiential-based performance assessment
Safe place to coll. and rec. sensitive info	0.945	
Accept the HHM system's advice	0.880	
Feel secure with sensitive info. about me being collected	0.848	
Faith in the HHM system providing the best advice	0.825	
Concerned about my personal privacy	0.777	
Would act in my best interest	0.711	
Has the skills and expertise to make correct decisions	0.671	
Would keep its commitments	0.556	
Would be dependable	0.574	
Would know what I want	0.564	
Would understand my needs	0.561	
Would be open and receptive to my needs	0.550	
Truthful in its dealings with me	0.527	
Understand how work		0.793
Easy to follow what does		0.679
Would do its best for me		0.675
Would correctly use the information I would provide to it		0.588
Would perform reliably		0.546
Understand how assist me with my decisions		0.537

Table IV.
Factor analysis results for the trust component in the Household Management (HHM) System scenario

Item	Factor 1: system-wide trust
Would keep its commitments	0.861
Would act in my best interest	0.860
Would be dependable	0.849
Would correctly use the information I would provide to it	0.842
Safe place to coll. and rec. sensitive info.	0.838
Would be open and receptive to my needs	0.829
Faith in the TM System providing the best advice	0.828
Would know what I want	0.824
Would understand my needs	0.811
Would be honest	0.809
Feel secure with sensitive info. about me being collected	0.805
Has the skills and expertise to make correct decisions	0.803
Would perform reliably	0.800
Accept the TM system's advice	0.800
Truthful in its dealings with me	0.795
Concerned about my personal privacy	0.784
Would do its best for me	0.784
Easy to follow what does	0.781
Understand how assist me with my decisions	0.769
Understand how work	0.642

Table V.
Factor analysis results for the trust component in the Treatment Management (TM) System scenario

To further assess discriminant validity, an analysis of the bi-variate correlation tables for each scenario was conducted (see Appendices 5-7). Within the Transport (TravM) System scenario, the majority of items demonstrate moderate to high correlations with other convergent items measuring the same or primary dimension (see Appendix 5). However, there are issues of discriminant validity with the "reliability" and "would understand my needs" items that demonstrate moderate correlations with a number of items other than their primary dimension. Similarly, within the HHM System, the majority of items demonstrate moderate to high correlations with convergent items measuring the same or primary dimension (see Appendix 6). However, with the "reliability", "understand my needs" "correctly use information", "would do its best for me" and "understand how to assist me with decisions" items, moderate correlations with a number of items other than their primary dimension is demonstrated. With the TM System, all items demonstrate moderate to high correlations with other items suggesting discriminant validity (see Appendix 7). Since this research has been exploratory in nature, these results suggest further development is required into the validation, measurement and refinement of instruments measuring trust within differing contexts.

Discussion

In the Travel Management System scenario, respondents have the ability to understand and consequently form a mental model of the system (Janson *et al.*, 2013) based upon the widespread ownership and hence familiarity and understanding of current GPS technology. This has resulted in a separate loading of items related to understandability on a factor that has been labelled "Understandability-Familiarity". Similarly, criteria used to assess the performance of the Travel Management System and its optimization of journey parameters, such as time and distance, will also be familiar and understandable to most respondents. This has resulted in items related to performance assessment (e.g. reliability, correct use of information provided, etc.) loading as a separate trust factor that has been labelled "Performance Assessment". However, whilst understanding and familiarity are considered core components of trust, there may be new or unfamiliar situations where there is

decreased familiarity on which to base understanding and hence imperfect knowledge exists. This may be the case with the HHM System scenario. It is posited that whilst respondents are familiar with the majority of the devices portrayed in this scenario as stand-alone "things" (e.g. washing machines, vacuum cleaners, dishwashers, etc.), they are unfamiliar with the notion of how these would function as a holistic networked system and consequently uncertainty surrounds the criteria by which respondents would assess such a system's performance. Within these contexts, understanding is no longer a separate trust dimension. Understandability and familiarity, together with the ability to gauge the performance of the system, are perceived as being interrelated and load together onto one factor. This trust dimension has been labelled "Experiential based performance assessment". Within both of these scenarios there is one factor with almost identical item loadings. This factor is characterized by items related to acceptance, commitment, security, truth and honesty, and reflective of a generalized confidence or faith in the relevant system performing appropriately. Within both these scenarios this dimension has been labelled "Constancy" to reflect the notion that the relevant system will be trustworthy in terms of being "unchanging or unwavering as in purpose, loyalty or faithfulness".

Experience with the content portrayed in the TM scenario is also likely to be low which has a significant impact on the ability to make performance assessments. This situation is likely to be exacerbated given the credence-based nature of the service portrayed in the scenario. Consequently, trust becomes uni-dimensional and is based on confidence or faith in the entire system performing appropriately. Hence, this dimension has been named "System-wide trust". The notion of system-wide trust has previously been explored in the technology and psychology literatures. This is a means of evaluating the reliability of a system's compliance (Keller and Rice, 2010) with user expectations of its performance. Trust in this context relates to the predictability of behaviour in the system (Geels-Blair *et al.*, 2013). However, perceptions of predictability by the user may be a function of preferences, which vary according to user savviness (competency) in relation to the IoT, as well as psychographic and behavioural factors (e.g. Briggs and Thomas, 2015; Sillence and Briggs, 2008). This may be derived not from direct experience of the system itself but through agent-based trust and trust acquired from the behaviours of other similar techno-service system customers or, indeed, other techno-service systems with which they have interacted. Consequently, they are able to draw on these experiences to "fill in the gaps" of their knowledge (Denning, 2015) and to mitigate risks and base their trust decisions. Identifying the predictors of system-wide trust would be an interesting direction in which to direct further research.

This research has also identified an emergent category of actor within IoT systems that could potentially fulfil a role attuned to that of a trust manager (Cho *et al.*, 2015). All three scenarios, to varying degrees, identified a faith-based or constancy dimension to trust within IoT contexts. A trust management system could potentially provide users (consumers) with estimates of the reliability of behavioural responses within the system for particular operations under conditions of imperfect knowledge and uncertain risk, hence informing decision making. In effect, it could provide a level of assurance (soft security) for users who may then take some informed action to influence the flow of information across the system. These findings broadly reflect Bapna *et al.'s* (forthcoming) levels of trust within a social network based on familiarity with the relationship context. For example, where social ties are stronger among actors, a consequence of more frequent interaction, trust is stable, irrespective of whether it is extrinsically or intrinsically motivated. Thus, from a managerial perspective, one way that system-wide trust may be facilitated is to increase the visibility and number of interactions with the techno-service system via the trust manager. The challenge in this approach is that from individual suppliers' perspectives within the network, an increase in interactions may not be cost effective. An important role for any trust manager solution is, therefore, to optimize the network flow between all actors.

Finally, these results suggest that taken overall, the dimensionality of trust factors within differing techno-service smart systems varies depending on some underlying but as yet, unidentified phenomenon. This has implications for the ways in which trust is conceptualized and used for different types of techno-service system: the research highlights that traditional measures of relational (dyadic) trust are not effective predictors of trust in these contexts. This suggests further research into the validation, measurement and refinement of instruments that assess trust within such contexts is required.

Conclusions

This research has identified how current dimensions of interpersonal- and technology-based trust within the extant literature may be inappropriate within some IoT techno-service contexts (e.g. Morgan and Hunt, 1994; Bapna *et al.*, forthcoming). Additionally, insights provided have been into the dimensionality of trust in circumstances where service users engage not with individual actors within a complex network but with a holistic techno-service system. The trust dimensions identified (constancy, understandability/familiarity, performance and system-wide trust) are broader in nature than previous findings within other contexts. However, in interpreting this, it is posited that IoT techno-service system users may, to varying degrees, have a limited perspective of the complexity of the system and the entities and processes it encompasses. Consequently, many of the specific interactions of and interdependencies between actors and objects described in the scenarios are beyond the cognition of potential users. This is unsurprising when one considers the IoT potentially represents thousands of simultaneous interactions between "things" (some human, some machine-based, and others being machines assuming human behaviours). In such circumstances, trust becomes confidence in or faith that a system as a whole will perform appropriately. For those that engage in these contexts, it is possible that socio-technological systems facilitate participatory access to knowledge, reflecting Mumford's (2006) point that "voluntary simplicity" leads to increased quality of life.

It is envisaged these findings will have important implications for managers and firms providing elements of the services enabled through IoT technologies in a number of trust areas. First, that trust decisions by end users may be delegated to agents that are capable of making intelligent interpretations of available information (e.g. Sillence and Briggs, 2008), i.e., trust managers. Given the complexity and multi-layered nature of potential IoT techno-service systems, it is proposed that this may apply to firms who provide, moderate and improve aspects of system information flow through their propositions and who ultimately deliver end-user services. This implies a need for a different level of "market sensing" than traditionally undertaken by firms. It is apparent from the contexts described, and the research findings related to each, that a trust manager is most likely to be a machine that is capable of analyzing large and continually evolving data sets. Such a machine will need to demonstrate learning capability in order to offer predictive solutions for users, say by "filling in the gaps" for a specific individual user at early stages of their techno-service system usage. Such data application demonstrating "understanding" of actor behaviours in IoT contexts can only be achieved by computationally modelling the service. In this way, it will optimize alignment between the multiple dynamic changes in the system as it "learns" (e.g. Ferrucci *et al.*, 2013). As the research highlights, however, trust is also a dynamic concept, reflecting different contexts of use and extent of user familiarity, and this too will need to be incorporated into modelling, in addition to the likelihood of different predictors for each scenario (a matter for future research to consider).

At this juncture, these aspects are not currently embedded within IT-based facilities at the techno-service system level. Consequently, future development of "service-on-service"

(e.g. trust manager) propositions that enable both customers and firms to make informed decisions (e.g. von Foerster, 2003; Vargo and Lusch, 2011) on appropriate trust-based interactions in timely ways is an important next step to facilitate adoption among users. Notwithstanding, the requirement for technological development, this will also necessitate the development of appropriate skillsets across firms to interpret and respond to new and emergent classes of data (information and knowledge) that such facilities will render for management decision making, including the ability to interact with systems through service agents. For example, consideration of what and how data flow should be controlled through their proposition into and across other propositions within the system context. This is not a trivial task, and will require technical, operational and management level implementation.

There is also likely to be consequential social adaptations made by techno-service system consumers that represent novel adoption behaviours, particularly where new types of service value may be derived through systems. One such example is the demand for predictive analytics that directly influence, say, dietary guidance on the use of specific ingredients where health benefits will result from long-term use, travel recommendations where the incorporation of a period of time walking per day will be beneficial, and even cultural engagement activities that stimulate well-being and inspire future thinking and creativity. Whilst the intentional and ubiquitous adoption of such services may be desirable (say, by public sector stakeholders), there are also likely to be unintended and unpredictable consequences of their use. Within current service system contexts, two identified patterns of social interactive behaviour have emerged: one is the disengagement with the technicalities of a system such that "blind" trust has resulted in its ultimate failure through disembedded use (Lobler, 2014). The other is technological interference (hacking the system, modifying content, both in increasingly sophisticated ways), which leads to sub-optimal outcomes for some users and, in worse case scenarios, system failures (e.g. Pfleeger and Pfleeger, 2011). Therefore, important considerations may not only be the real-time trust-based proposition as described above but also consumers' predisposed engagement with trust-based propositions estimated from their use of other similar techno-service systems. Needless to say, there are significant ethical and technical challenges that require examination for these developments to be implemented in practice involving a broad range of stakeholders (consumers, firms, public sector bodies, technology providers, etc.).

Furthermore, within such contexts and the various bodies literature considered in developing this work, issues of risk, risk management and security are inextricably linked together with trust because of the need to contextualize and evaluate contingent outcomes (Luhmann, 1995; Giddens, 1990). Consequently, it becomes necessary to devise mechanisms that oversee risk management, as alluded to above. This may well be analogous to the IS approaches to risk management of algorithm-based ratings (Friedman *et al.*, 2007; Aggarwal and Yu, 2008). To extend Sillence and Brigg's (2008) proposal on the proxy use by end users of agents that mitigate risks and through which trust decisions are enacted, however, the emergent role of trust manager (Cho *et al.*, 2015) becomes crucial. Automated reputation management technology is already in use by end users that provide estimates of the reliability of behavioural responses (e.g. TripAdvisor) within the system for particular operations under conditions of imperfect knowledge and certain risk. As such, they are used by end-customer human actors to inform decision making. These systems do not exist at present for firm actors in service systems, nor do they accurately reflect the specific behaviours of users themselves across a networked techno-service system. In effect, such facilities could provide a necessary level of assurance (soft security) that may then be used to support decision making in these contexts. This would be another interesting direction to focus future research.

References

Aggarwal, C.C. and Yu, P.S. (2008), "A survey of randomization methods for privacy-preserving data mining", *Privacy-Preserving Data Mining*, pp. 137-156.

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. (1994), *Advanced Methods of Marketing Research*, Blackwell Business, Cambridge, MA.

Bagozzi, R.P., Yi, Y. and Phillips, L.W. (1991), "Assessing construct validity in organizational research", *Administrative Science Quarterly*, Vol. 36 No. 3, pp. 421-458.

Bandura, A. (1997), *Self-Efficacy: The Exercise of Control*, Freeman, New York, NY.

Bandura, A. (2001), "Social cognitive theory: an agentic perspective", *Annual Review of Psychology*, Vol. 52, pp. 1-26.

Bao, F. and Chen, I.R. (2012), "Dynamic trust management for Internet of Things applications", *2012 International Workshop on Self-Aware Internet of Things*, San Jose, CA, 16-20 September.

Bapna, R., Gupta, A., Rice, S. and Sundararajan, A. (forthcoming), "Trust and the strength of ties in online social networks: an exploratory field experiment", *MIS Quarterly* available at: www.misq.org/forthcoming; www.misq.org/skin/frontend/default/misq/pdf/Abstracts/14077_RA_BapnaQiuAbstract.pdf

Bartlett, M.S. (1954), "A note on multiplying factors for various chi-squared approximations", *Journal of the Royal Statistical Society*, Vol. 16, pp. 296-298.

Beatty, P., Reay, I., Dick, S. and 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.

Berelson, B. (1952), *Content Analysis in Communication Research*, The Free Press, Glencoe, IL.

Berscheid, E. (1993), "Emotion. In close relationships", in Kelley, H.H., Christensen, A., Harvey, J.H., Huston, T.L. and Levinger, G. (Eds), W.H. Freeman, New York, NY, pp. 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.

Bolger, M. (2014), "The Internet of Things", available at: www.themarketer.co.uk/analysis/features/the-internet-of-things/ (accessed 23 March 2017).

Briggs, P. and Thomas, L. (2015), "An inclusive, value sensitive design perspective on future identity technologies", *ACM Transactions on Computer-Human Interaction*, Vol. 22 No. 5, doi: 10.1145/2778972.

Butler, J.K. (1991), "Toward understanding and measuring conditions of trust: evolution of a conditions of trust inventory", *Journal of Management*, Vol. 17 No. 3, pp. 643-663.

Cameron, D. (2014), *CeBIT 2014: David Cameron's Speech*, available at: www.gov.uk/government/speeches/cebit-2014-david-camerons-speech

Castelfranchi, C. and Falcone, R. (2010), *Trust Theory: A Socio-Cognitive and Computational Model*, Vol. 18, John Wiley and Sons, London.

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.

Chen, I., Bao, F. and Guo, J. (2015), "Trust-based service management for social Internet of Things", *IEEE Transactions on Dependable and Secure Computing*, Vol. 13 No. 6, pp. 1545-5971.

Chen, Y. (2012), "Keynote", *Proceedings of the IEEE International Conference on Green Computing and Communications*, *Besancon*, pp. xliv-xlviii.

Cheung, C. and 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.

Cho, J.-H., Chan, K. and Adali, S. (2015), "A survey on trust modelling", *ACM Computing Surveys*, Vol. 48 No. 2, pp. 28-40.

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.

Cohen, J. (1988), *Statistical Power Analysis for the Behavioural Sciences*, 2nd ed., Lawrence Earlbaum Associates, Hillsdale, NJ.

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. and 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.

Dimoka, A. (2010), "What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study", *MIS Quarterly*, Vol. 34 No. 2, pp. 373-396.

Doney, P.M. and Cannon, J.P. (1997), "An examination of the nature of trust in buyer-seller relationships", *Journal of Marketing*, Vol. 61 No. 2, pp. 35-51.

Eloff, J., Eloff, M., Dlamini, M. and Zielinski, M. (2009), "Internet of people, things and services-the convergence of security, trust and privacy", *3rd Annual CompanionAble Consortium Workshop - Internet of People, Things and Services (IoPTS), 2 December*, Novotel Brussels, Brussels, available at: www.companionable.net/index.php?option=com_phocadownload&view=category&id=7:3rd-companionable-workshop-iopts-proceedings&Itemid=6

Emery, F.E. and Trist, E.L. (1960), "Socio-technical systems", in Churchmann, C.W. and Verhurst, M. (Eds), *Management Sciences, Models and Techniques*, Vol. 2, Pergamon Press, London, pp. 83-97.

Engen, V., Pickering, J.B. and Walland, P. (2016), "Machine agency in human-machine networks; impacts and trust implications", in Kurosu, M. (Ed.), *Human-Computer Interaction. Novel User Experiences*, Lecture Notes in Computer Science, Vol. 9733, Springer, Cham, pp. 96-106.

Ferrucci, D., Levas, A., Bagchi, S., Gondek, D. and Mueller, E.T. (2013), "Watson: beyond jeopardy!", *Artificial Intelligence*, Vols 199-200, pp. 93-105.

Floyd, F.J. and Widaman, K.F. (1995), "Factor analysis in the development and refinement of clinical assessment instruments", *Psychological Assessment*, Vol. 7 No. 3, pp. 286-299.

Friedman, B., Khan, P. and Howe, D. (2000), "Trust online", *Communications of the Association for Computing Machinery*, Vol. 43 No. 12, pp. 34-40.

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

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

Frow, P., McColl-Kennedy, J.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.

Gao, L. and Bai, X. (2014), "An empirical study on continuance intention of mobile social networking services: integrating the IS success model, network externalities and flow theory", *Asia Pacific Journal of Marketing and Logistics*, Vol. 26 No. 2, pp. 168-189.

Geels-Blair, K., Rice, S. and Schwark, J. (2013), "Using system-wide trust theory to reveal the contagion effects of automation false alarms and issues on compliance and reliance in a simulated aviation task", *International Journal of Aviation Psychology*, Vol. 23 No. 3, pp. 245-266.

Gefen, D. and Pavlou, P.A. (2012), "The boundaries of trust and risk: the quadratic moderating role of institutional structures", *Information Systems Research*, Vol. 23 No. 3, pp. 940-959.

Giddens, A. (1990), *The Consequences of Modernity*, Polity Press, Cambridge.

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.

Hair, J., Anderson, R., Tatham, R. and Black, W. (1995), *Multivariate Data Analysis*, Maxwell MacMillan International, Englewood Cliffs, NJ.

Hojer, M. and Wangel, J. (2015), "Smart sustainable cities: definition and challenges", in Hilty, L.M. and Aebischer, B. (Eds), *ICT for Sustainability, Advances in Intelligent Systems and Computing*, Innovations, Springer, New York, NY, pp. 333-349.

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 No. 3, pp. 322-336.

Iansiti, M. and Lakhani, K.R. (2014), "Digital ubiquity: how connections, sensors and data are revolutionizing business (digest summary)", *Harvard Business Review*, Vol. 92 No. 11, pp. 91-99.

Jaakkola, E. and Alexander, M. (2014), "The role of customer engagement behaviour in value co-creation: a service system perspective", *Journal of Service Research*, Vol. 17 No. 3, pp. 247-261.

Janson, A., Hoffmann, A., Hoffmann, H. and Leimeister, J. (2013), "How customers trust mobile marketing applications", *International Conference of Information Systems*, *Milano*, *15-18 December*.

Jia, H., Wu, M., Jung, E., Shapiro, A. and Sundar, S. (2012), "Balancing human agency and object agency: an end-user interview study of the Internet of Things", *Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ACM*, *New York, NY*, *5-8 September*, pp. 1185-1188.

Kaiser, H.F. (1970), "A second generation little jiffy", *Psychometrika*, Vol. 35, pp. 401-415.

Kalman, R.E. (1960), "A new approach to linear filtering and prediction problems", *Journal of Basic Engineering*, Vol. 82 No. 1, pp. 35-45.

Keller, D. and Rice, S. (2010), "System-wide trust versus component-specific trust using multiple aids", *Journal of General Psychology*, Vol. 173 No. 1, pp. 114-128.

Killinger, B. (2010), *Integrity: Doing the Right Thing for the Right Reason*, McGill-Queen's University Press, Quebec, CA.

Komiak, S.Y. and Benbasat, I. (2006), "The effects of personalization and familiarity on trust and adoption of recommendation agents", *MIS Quarterly*, Vol. 30 No. 4, pp. 941-960.

Krippendorff, K. (2013), *Content Analysis: An Introduction to its Methodology*, 3rd ed., Sage Publications, London.

Lataifa, S.B. (2014), "The uneasy transition from supply chains to ecosystems", *Management Decision*, Vol. 52 No. 2, pp. 278-295.

Lemke, J.L. (2007), "Video epistemology in-and-outside the box: traversing attentional spaces", in Godman-Segall, R. and Pea, R. (Eds), *Video Research in the Learning Sciences*, Erlbaum, Mahwah, pp. 39-52.

Lobler, H. (2014), "When trust makes it worse-rating agencies as disembedded service systems in the US financial crisis", *Service Science*, Vol. 6 No. 2, pp. 94-105.

Luhmann, N. (1995), *Social Systems*, Stanford University Press, Stanford, CA.

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*, Vol. 2 No. 2, doi: 10.1145/1985347.1985353.

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.

Madsen, M. and Gregor, S. (2000), "Measuring human-computer trust", *11th Australasian Conference on Information Systems*, Brisbane, 6-8 December.

Masani, P. (1985), *Norbert Wiener: Collected Works with Commentaries*, Vol. IV, MIT Press, Cambridge, MA, pp. 793-799.

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.

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.

Mick, D.G. (2006), "Meaning and mattering through transformative consumer research", in Pechmann, C. and Price, C. (Eds), *Presidential Address Before the Association for Consumer Research*, Vol. 33, Duluth, MN, pp. 1-4.

Minsky, M. (1988), *The Society of the Mind*, Simon and Schuster, New York, NY.

Minsky, M. (2006), *The Emotion Machine*, Simon and Schuster, New York, NY.

Moore, J.F. (2006), "Business ecosystems and the view from the firm", *Antitrust Bulletin*, Vol. 51 No. 1, pp. 31-75.

Moorman, C., Zaltman, G. and Deshpande, R. (1992), "Relationships between providers and users of market research: the dynamics of trust within and between organizations", *Journal of Marketing Research*, Vol. 29 No. 3, p. 314.

Morgan, R.M. and Hunt, S.D. (1994), "The commitment-trust theory of relationship marketing", *Journal of Marketing*, Vol. 58, July, pp. 20-38.

Mumford, E. (2006), "The story of socio-technical design: reflections on its successes, failures and potential", *Information Systems Journal*, Vol. 16 No. 4, pp. 317-342.

Nass, C., Fogg, B. and Moon, Y. (1996), "Can computers be teammates?", *International Journal of Human-Computer Studies*, Vol. 45 No. 6, pp. 669-678.

Neuhofer, B., Buhalis, D. and Ladkin, A. (2015), "Smart technologies for personalized experiences: a case study in the hospitality domain", *Electronic Markets*, Vol. 25 No. 3, pp. 243-254.

Nicolescu, B. (2002), "A new vision of the world – transdisciplinarity", The design and delivery of inter- and pluri-disciplinary research, Proceedings from MUSCIPOLI Workshop Two, report from The Danish Institute for Studies in Research and Research Policy No. 2002/7, Aarhus.

Ozanne, J., Pettigrew, S., Crockett, D., Firat, A.F., Downey, H. and Pescud, M. (2011), "The practice of transformative consumer research-some issues and suggestions", *Journal of Research for Consumers*, Vol. 19 No. 1, pp. 1-7.

Park, C.W., Jaworski, B.J. and MacInnis, D.J. (1986), "Strategic brand concept-image management", *Journal of Marketing*, Vol. 50, October, pp. 135-145.

Pauwels, L. (2011), "An integrated conceptual framework for visual social research", in Margolis, E. and Pauwels, L. (Eds), *The Sage Handbook of Visual Research Methods*, Sage Publications, London, pp. 3-23.

Pearl, J. (2000), *Causality: Models, Reasoning, and Inference*, Cambridge University Press, Cambridge.

Pfleeger, C.P. and Pfleeger, C.L. (2011), *Analyzing Computing Security: A Threat/Vulnerability/ Countermeasure Approach*, Prentice Hall, Upper Saddle River, NJ.

Pink, S. (2007), *Doing Visual Ethnography*, Sage Publications, London.

Porter, M.E. and Heppelmann, J.E. (2014), "How smart, connected products are transforming competition", *Harvard Business Review*, Vol. 92 No. 11, pp. 11-64.

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.

Rose, J. and Truex, D. (2000), "Machine agency as perceived autonomy: an action perspective", in Baskerville, R., Stage, J. and DeGross, J. (Eds), *Organizational and Social Perspectives on Information Technology*, Springer, pp. 371-388.

Russell, S. and Norvig, P. (1995), *Artificial Intelligence: A Modern Approach*, Prentice Hall, Englewood Cliffs, NJ.

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*, Sage, London.

Schembri, S. and Boyle, M.V. (2013), "Visual ethnography: achieving rigorous and authentic interpretations", *Journal of Business Research*, Vol. 66 No. 1, pp. 1251-1254.

Schrammel, J., Hochleitner, J. and Tscheligi, M. (2011), "Privacy, trust and interaction in the Internet of Things", in Keyson, D.V. *et al.* (Eds), *Ambient Intelligence 2011, Lecture Notes in Computer Science*, Vol. 7040, Springer, Berlin, pp. 378-379.

Sekhon, H., Ennew, C., Kharouf, H. and Devlin, J. (2014), "Trustworthiness and trust: influences and implications", *Journal of Marketing Management*, Vol. 30 Nos 3-4, pp. 409-430.

Seppänen, R., Blomqvist, K. and Sundqvist, S. (2007), "Measuring inter-organizational trust – a critical review of the empirical research in 1990-2003", *Industrial Marketing Management*, Vol. 36 No. 2, pp. 249-265.

Sheppard, B. and Sherman, D. (1998), "The grammars of trust: a model and general implications", *Academy of Management Review*, Vol. 23 No. 3, pp. 422-437.

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.

Simmel, G. (1978), *The Philosophy of Money*, Routledge, London.

Smith, J., Leahy, J., Anderson, D. and Davenport, M. (2013), "Community/agency trust: a measurement instrument", *Society and Natural Resources*, Vol. 26 No. 4, pp. 472-477.

Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A. and Leimeister, J. (2014), "Understanding the formation of trust", in David, K. *et al.* (Eds), *Socio-technical Design of Ubiquitous Computing Systems*, Springer International Publishing, London, pp. 39-57.

Taddei, S. and Contena, B. (2013), "Privacy, trust and control: which relationships with online self-disclosure", *Computers in Human Behavior*, Vol. 29 No. 3, pp. 821-826.

Vargo, S.L. and Lusch, R.F. (2011), "It's all B2B… and beyond: toward a systems perspective of the market", *Industrial Marketing Management*, Vol. 40 No. 2, pp. 181-187.

von Foerster, H. (2003), *Understanding Understanding: Essays on Cybernetics and Cognition*, Springer Science, New York, NY.

Weinberg, B., Milne, G., Andonova, Y. and Hajjat, F. (2015), "Internet of Things: convenience vs privacy and secrecy", *Business Horizons*, Vol. 58 No. 6, pp. 615-624.

Weiss, G. (1999), *Multi-Agent Systems: A Modern Approach to Distributed Artificial Intelligence*, MIT Press, Cambridge.

Weizenbaum, J. (1966), "ELIZA – a computer program for the study of natural language communication between man and machine", *Communications of the ACM*, Vol. 9, pp. 36-45.

Wuenderlich, N.V., Heinonen, K., Ostrom, A.L., Patricio, L., Sousa, R., Voss, C. and Lemmink, J.G. (2015), "'Futurizing' smart service: implications for service researchers and managers", *Journal of Services Marketing*, Vol. 29 Nos 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, June, 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.

Further reading

The Guardian (2014), "David Cameron: the Internet of Things – funding to double", 9 March.

Corresponding author

Tracy Harwood can be contacted at: tharwood@dmu.ac.uk

Appendix 1

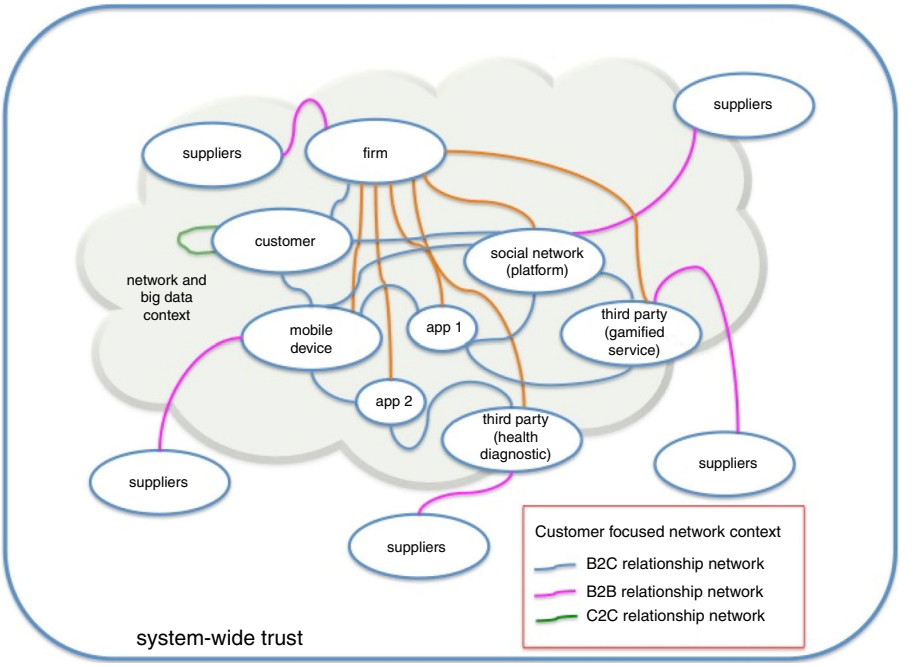

Figure A1. Example of a wearable technology value proposition

Appendix 2. Scripting the scenarios

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, well-being and whereabouts status. The data are shared and used in conjunction with a range of people, devices and environments.

Film 2: the Travel Manager (TravM) System

At least once a month Harry and Maddy visit John and Jane. Neither of them drive, living and working in a city there is no need, but getting to Harry's parent's home in the country can be challenging. They use a travel management programme to help them plan their visit. The final ten minutes of their journey has to be on foot as there is no public transport at that end, but at least the programme manager tells them about the weather forecast so they can plan what to wear. They enter the time they would like to arrive at their destination, and the programme manager coordinates their itinerary based on fastest travel time and best value for money, to optimize their scarce resources. In this instance, it selects a shared car service with a bus that connects to a train and an automated minicab, taking just less than an hour overall. The programme manager monitors their journey and updates as delays occur en route. They receive notifications via their smartphones. If necessary, it changes their itinerary to ensure their route continues to be optimized in real time. Where the delays are likely to impact on their arrival plans, it sends status updates to John and Jane, so they can make adjustments to their plans accordingly.

Film 3: the Household Manager (HHM) 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.

Film 4: the Treatment Manager (TM) System

Jane's tracker monitors her responses to her cancer treatments and feeds back data to a centralized treatment manager. The treatment manager is based on a large network of data collected from thousands of patients and best practice in the management of similar treatments from around the world. In turn, the manager remotely adjusts Jane's treatment programme to ensure that drug levels are optimized, also deployed through a discreet wearable device. She is sent status updates and messages about her condition regularly via her smartphone, and periodically receives a personal call from a specialist consultant who discusses her progress and has oversight of the treatment manager.

Jane has the option to attend a local treatment centre to top up her drugs as needed, or the device may trigger a delivery direct to her home, depending on her family and social plans. John, Harry and Maddy use their smart devices to keep in touch with the progress updates that Jane chooses to share with each of them, individually and as a family, and this also helps them to plan their family activities together, such as best days to go out, what to eat, etc.

Appendix 3. Measurement instrument (Treatment manager)

(1) Understandability (source: Madsen and Gregor, 2000):

- 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.

(2) 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.

(3) Personalization (Komiak and Benbasat, 2006):

- P1: overall, the Treatment manager system would understand my needs.
- P1: overall, the Treatment manager system would know what I want.

(4) 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.

(5) 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.

(6) Reliability (source: McKnight *et al.*, 2011):

- R1: overall, the Treatment manager system would perform reliably.
- R1: overall, the Treatment manager system would be dependable.

(7) 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.

(8) Faith (source: Madsen and Gregor, 2000):

- 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.

Table AI.
Bi-variate correlation table

Appendix 4

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	0.702**	1																		
3. Would correctly use the information provided	0.682**	0.652**	1																	
4. Would do its best for me	0.587**	0.598**	0.682**	1																
5. Feel secure with sensitive info. being collected	0.538**	0.561**	0.548**	0.522**	1															
6. Understand how work	0.398**	0.367**	0.398**	0.411**	0.391**	1														
7. Concerned about my personal privacy	0.461**	0.489**	0.479**	0.433**	0.586**	0.343**	1													
8. Easy to follow what does	0.537**	0.512**	0.533**	0.511**	0.454**	0.571**	0.448**	1												
9. Would know what I want	0.597**	0.675**	0.407**	0.522**	0.538**	0.407**	0.526**	0.585**	1											
10. Would be honest	0.565**	0.540**	0.366**	0.598**	0.544**	0.366**	0.532**	0.528**	0.602**	1										
11. Skills and expertise to make correct decisions	0.551**	0.586**	0.361**	0.509**	0.577**	0.361**	0.559**	0.502**	0.629**	0.564**	1									
12. Understand how assist me with my decisions	0.483**	0.528**	0.531**	0.523**	0.464**	0.531**	0.436**	0.578**	0.541**	0.530**	0.545**	1								

(*continued*)

Item	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
13. Would be open and receptive to my needs	0.552**	0.611**	0.387**	0.571**	0.584**	0.387**	0.540**	0.532**	0.660**	0.555**	0.647**	0.603**	1							
14. Faith in system providing the best advice	0.557**	0.596**	0.355**	0.529**	0.628**	0.355**	0.588**	0.490**	0.603**	0.567**	0.676**	0.526**	0.676**	1						
15. Would act in my best interest	0.582**	0.607**	0.359**	0.598**	0.604**	0.359**	0.579**	0.505**	0.628**	0.630**	0.626**	0.552**	0.660**	0.725**	1					
16. Truthful in its dealings with me	0.532**	0.520**	0.375**	0.560**	0.548**	0.375**	0.523**	0.502**	0.546**	0.711**	0.530**	0.507**	0.580**	0.602**	0.700**	1				
17. Would be dependable	0.652**	0.616**	0.413**	0.528**	0.588**	0.413**	0.528**	0.550**	0.604**	0.627**	0.588**	0.537**	0.606**	0.662**	0.673**	0.688**	1			
18. Accept the system's advice	0.528**	0.576**	0.298**	0.494**	0.586**	0.298**	0.542**	0.464**	0.576**	0.525**	0.604**	0.484**	0.580**	0.699**	0.639**	0.567**	0.639**	1		
19. Safe place to coll. and rec. sensitive info.	0.511**	0.561**	0.333**	0.460**	0.721**	0.333**	0.619**	0.453**	0.546**	0.565**	0.590**	0.450**	0.558**	0.641**	0.626**	0.589**	0.619**	0.657**	1	
20. Would keep its commitments	0.575**	0.575**	0.411**	0.580**	0.612**	0.411**	0.559**	0.561**	0.601**	0.629**	0.600**	0.556**	0.658**	0.637**	0.676**	0.682**	0.679**	0.615**	0.669**	1

Note: **$p < 0.01$ (2-tailed)

Table AI.

Table AII.
Bi-variate correlation table for the Transport Management (TravM) System scenario

Appendix 5

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	*0.656***	1																		
3. Would correctly use the information provided	0.620**	0.596**	1																	
4. Would do its best for me	0.497**	0.478**	*0.574***	1																
5. Feel secure with sensitive info. being collected	0.498**	*0.504***	*0.511***	0.390**	1															
6. Understand how work	0.304**	0.329**	0.386**	0.315**	0.359**	1														
7. Concerned about my personal privacy	0.372**	0.367**	0.390**	0.272**	*0.518***	0.242**	1													
8. Easy to follow what does	0.438**	0.446**	0.422**	0.382**	0.358**	*0.587***	0.327**	1												
9. Would know what I want	*0.523***	*0.558***	*0.514***	0.442**	0.415**	0.419**	0.452**	*0.561***	1											
10. Would be honest	*0.506***	0.461**	0.471**	0.485**	*0.514***	0.309**	*0.507***	0.411**	*0.548***	1										
11. Skills and expertise to make correct decisions	*0.502***	*0.518***	0.486**	0.408**	*0.519***	0.350**	*0.523***	0.427**	*0.526***	*0.579***	1									
12. Understand how assist me with my decisions	0.414**	0.418**	0.415**	0.384**	0.376**	*0.584***	0.315**	*0.584***	0.495**	0.437**	0.508**	1								
13. Would be open and receptive to my needs	0.470**	*0.502***	0.458**	0.453**	0.480**	0.374**	0.438**	0.435**	*0.572***	0.458**	0.614**	*0.535***	1							

(*continued*)

Item	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
14. Faith in system providing the best advice	0.496**	0.469**	0.494**	0.436**	*0.566***	0.337**	0.491**	0.420**	*0.521***	*0.586***	0.664**	0.465**	*0.602***	1						
15. Would act in my best interest	*0.542***	*0.555**	*0.512***	0.436**	0.493**	0.359**	*0.501***	0.463**	*0.595***	*0.623***	0.625**	0.485**	*0.600***	*0.707***	1					
16. Truthful in its dealings with me	0.491**	0.470**	0.467**	0.436**	*0.513***	0.306**	*0.500***	0.383**	*0.503***	*0.730***	0.555**	0.396**	*0.520***	*0.590***	*0.662***	1				
17. Would be dependable	*0.643***	*0.569***	0.496**	0.434**	*0.533***	0.338**	0.465**	0.440**	*0.557***	*0.618***	0.583**	0.435**	*0.524***	*0.621***	*0.593***	*0.629***	1			
18. Accept the system's advice	0.443**	0.464**	0.443**	0.408**	*0.505***	0.264**	0.401**	0.331**	0.440**	0.439**	0.542**	0.408**.	*0.533***	*0.635***	*0.589***	*0.505***	*0.592***	1		
19. Safe place to coll. and rec. sensitive info.	0.430**	0.451**	0.422**	0.305**	*0.678***	0.258**	*0.561***	0.302**	0.417**	*0.516***	0.561**	0.306**	0.467**	*0.599***	*0.529***	*0.535***	*0.571***	*0.588***	1	
20. Would keep its commitments	*0.523***	*0.525***	0.470**	0.464**	*0.561***	0.350**	0.476**	0.462**	*0.521***	*0.616***	0.588*	0.429**	*0.616***	*0.616***	*0.630***	*0.691***	*0.633***	*0.580***	*0.598***	1

Table AII.

Table AIII.
Bi-variate correlation table for the Household Management (HHM) System scenario

Appendix 6

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	*0.684***	1																		
3. Would correctly use the information provided	*0.641***	*0.599***	1																	
4. Would do its best for me	*0.558***	*0.571***	*0.652***	1																
5. Feel secure with sensitive info. being collected	0.444**	*0.556***	0.471**	0.496**	1															
6 Understand how work	0.339**	0.278**	0.288**	0.397**	0.264**	1														
7. Concerned about my personal privacy	0.430**	0.472**	0.418**	0.385**	*0.551***	0.275**	1													
8. Easy to follow what does	*0.519***	0.462**	0.478**	0.489**	0.402**	0.494**	0.410**	1												
9. Would know what I want	*0.567***	*0.680***	*0.502***	*0.555***	*0.558***	0.334**	0.492**	*0.525***	1											
10. Would be honest	*0.533***	*0.521***	*0.574***	*0.633***	0.485**	0.313**	0.469**	*0.525***	*0.564***	1										
11. Skills and expertise to make correct decisions	*0.511***	*0.551***	0.485**	0.471**	*0.585***	0.287**	*0.524***	0.453**	*0.637***	0.482**	1									

(*continued*)

Item	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
12. Understand how assist me with my decisions	0.440**	0.540**	0.491**	0.547**	0.417**	0.388**	0.401**	0.464**	0.505**	0.523**	0.463**	1								
13. Would be open and receptive to my needs	0.550**	0.627**	0.593**	0.573**	0.613**	0.354**	0.532**	0.518**	0.638**	0.562**	0.601**	0.587**	1							
14. Faith in system providing the best advice	0.523**	0.608**	0.518**	0.466**	0.604**	0.280**	0.569**	0.459**	0.572**	0.510**	0.617**	0.505**	0.632**	1						
15. Would act in my best interest	0.542**	0.579**	0.554**	0.608**	0.635**	0.250**	0.527**	0.423**	0.598**	0.574**	0.546**	0.518**	0.631**	0.671**	1					
16. Truthful in its dealings with me	0.468**	0.490**	0.525**	0.554**	0.543**	0.313**	0.479**	0.467**	0.514**	0.683**	0.420**	0.529**	0.579**	0.590**	0.689**	1				
17. Would be dependable	0.599**	0.588**	0.582**	0.514**	0.549**	0.352**	0.497**	0.496**	0.560**	0.590**	0.517**	0.514**	0.598**	0.634**	0.661**	0.689**	1			
18. Accept the system's advice	0.481**	0.594**	0.436**	0.430**	0.561**	0.236**	0.601**	0.419**	0.575**	0.497**	0.560**	0.468**	0.518**	0.671**	0.576**	0.538**	0.606**	1		
19. Safe place to coll. and rec. sensitive info.	0.433**	0.572**	0.414**	0.444**	0.714**	0.234**	0.576**	0.417**	0.559**	0.500**	0.536**	0.425**	0.557**	0.647**	0.607**	0.537**	0.571**	0.682**	1	
20. Would keep its commitments	0.516**	0.540**	0.570**	0.594**	0.588**	0.356**	0.507**	0.488**	0.578**	0.546**	0.501**	0.493**	0.638**	0.610**	0.636**	0.643**	0.623**	0.550**	0.631**	1

Table AIII.

Table AIV.
Bi-variate correlation table for the Treatment Management (TM) System scenario

Appendix 7

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	*0.736***	*1*																		
3. Would correctly use the information provided	*0.754***	*0.739***	*1*																	
4. Would do its best for me	*0.650***	*0.681***	*0.761***	*1*																
5. Feel secure with sensitive info. being collected	*0.642***	*0.601***	*0.656**	*0.632***	*1*															
6. Understand how work	*0.540***	0.486**	*0.523***	*0.503***	*0.548***	*1*														
7. Concerned about my personal privacy	*0.540***	*0.600**	*0.617***	*0.594***	*0.637***	*0.505***	*1*													
8. Easy to follow what does	*0.610***	*0.590***	*0.644**	*0.580***	*0.580***	*0.639***	*0.596***	*1*												
9. Would know what I want	*0.664**	*0.738**	*0.643***	*0.592***	*0.672***	0.471**	*0.648***	*0.639***	*1*											
10. Would be honest	*0.635***	*0.607***	*0.677***	*0.631***	*0.622***	0.463**	*0.615***	*0.608***	*0.677***	*1*										
11. Skills and expertise to make correct decisions	*0.590***	*0.640***	*0.636***	*0.577***	*0.604***	0.436**	*0.621***	*0.575***	*0.670***	*0.624***	*1*									
12. Understand how assist me with my decisions	*0.561***	*0.576***	*0.607***	*0.569***	*0.584***	*0.629***	*0.584***	*0.674***	*0.586***	*0.598***	*0.631***	*1*								

(*continued*)

Item	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
13. Would be open and receptive to my needs	0.601**	0.657**	0.644**	0.622**	0.635**	0.430**	0.659**	0.592**	0.720**	0.611*	0.699**	0.648**	1							
14. Faith in system providing the best advice	0.509**	0.646**	0.679**	0.613**	0.681**	0.439**	0.672**	0.544**	0.668*	0.600**	0.707**	0.572**	0.762**	1						
15. Would act in my best interest	0.620**	0.654**	0.704**	0.672**	0.641**	0.467**	0.671**	0.605**	0.677*	0.686**	0.681**	0.628**	0.734**	0.771**	1					
16. Truthful in its dealings with me	0.604**	0.568**	0.654**	0.610**	0.561**	0.489**	0.569**	0.609**	0.600*	0.720**	0.597**	0.554*	0.617**	0.603**	0.726**	1				
17. Would be dependable	0.697**	0.663**	0.682**	0.588*	0.652**	0.532**	0.594**	0.674**	0.677*	0.662**	0.640**	0.629**	0.670**	0.703**	0.728**	0.718**	1			
18. Accept the system's advice	0.581**	0.606**	0.638**	0.564**	0.664**	0.390**	0.595**	0.571**	0.641**	0.613**	0.648**	0.529**	0.657**	0.731**	0.714**	0.625**	0.697**	1		
19. Safe place to coll. and rec. sensitive info.	0.637**	0.634**	0.643**	0.583**	0.737**	0.501**	0.670**	0.618**	0.662*	0.673**	0.688**	0.604**	0.661**	0.664*	0.702**	0.673**	0.673**	0.703**	1	
20. Would keep its commitments	0.651**	0.645**	0.683**	0.664**	0.664**	0.507**	0.665*	0.684*	0.666*	0.709**	0.677**	0.686**	0.690**	0.658**	0.734**	0.701**	0.701**	0.687**	0.760**	1

Table AIV.