INITIAL TRUST IN EMERGING TECHNOLOGIES AND THE EFFECT OF THREATS TO PRIVACY

A thesis submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy in Information Systems

at the University of Canterbury

by Natasha. C. H. L. Mazey

University of Canterbury

2018

Abstract

Purpose*: This thesis seeks to identify what factors influence technology trust beliefs in emerging technologies, as opposed to non-emerging technologies, with which individuals have little prior knowledge or experience of. In particular, it explores the relationship between perceived threats to personal information privacy (PIP) and technology trust. This research is comprised of two studies. Study 1 explores a new framework to identify emerging technologies, unique PIP threats to emerging technologies, and whether these PIP threats effect initial technology trust beliefs. A number of covariates are also tested, including disposition to trust generally, disposition to technology trust, faith in humanity, economic environment, subjective norms and initial familiarity. Study 2 tests the predictive validity of the findings in Study 1 and further investigates the relationships between initial trust, PIP threats and the significant covariates found in Study 1. Initial technology trust models are developed and tested, and compared between emerging and non-emerging technologies.*

Methodology*: A wide range of literature, including Information Systems, Psychology, E-Commerce, Economics, Science and Legal, is considered for theory development. Study 1 performs a controlled, randomised post-test experiment on 293 subjects with four emerging technology groups and one non-emerging control group. Factor analyses, MANOVAs and MANCOVAs are performed. For Study 2, PLS-SEM procedures test the proposed initial technology trust model against both emerging and non-emerging technologies.*

Findings*: A framework to assess whether emerging technologies are truly "emergent" is identified based on their innovative and transformative nature. New dimensions for PIP threats are discovered (intrusiveness, omnipotence and invisibility) for emerging technologies. These are found to have a negative influence on initial technology trust beliefs. A new dimension for technology trust is discovered for non-emerging technologies called "data integrity." Findings suggest situational normality should be removed from existing initial technology trust models as an antecedent for institutional-based trust in emerging technologies. The covariate variables all had a significant effect on initial technology trust beliefs. Further investigation using PLS-SEM supports the inclusion of the covariates in future technology trust research and demonstrates two different initial technology trust models exist for emerging and non-emerging technologies. Evidence indicates the cognitive process to evaluate initial trust in emerging technologies is distinct from non-emerging technologies and the two cannot be considered, or assumed, to be the same.*

Keywords:

trust, personal information privacy threats, emerging technologies, non-emerging technologies, faith in humanity, economic environment, subjective norms, PLS-SEM

Acknowledgements

I would like to express my sincere gratitude to Dr. Stephen Wingreen. Thank you for your continuous support, optimism, motivation and patience. I could not have asked for a better advisor or mentor. Your insight and encouragement guided me throughout this journey and challenged me to achieve more than I could have imagined. Thank you for your unwavering faith in me. You have made me believe anything is possible.

To my parents, thank you for always believing in me and never giving up on me. Your endless love, support and encouragement to persevere and try my best has made me the person I am today. You have given me the confidence to try without fear of failing.

To JP, thank you for helping me keep perspective of what matters and keeping my feet on the ground. Thank you for constantly putting up with me, suffering through my rambles and moods, reading my drafts and indulging my questions of "Does it make sense if…" You remind me that we never journey alone.

To my sister, Summer, thank you for always being by my side, keeping me sane and picking me up when life pushed me down. You have given me strength and courage. Thank you for humouring me with talk about my research and pointing out the obvious. I don't know what I would do without you.

So, I dedicate this to you.

Table of Contents

SECTION 1. INTRODUCTION

We are in the midst of a technology revolution. Sparked by the computer revolution in the 1970s, this revolution has only just set its course and is building up speed. Unlike the big noise and smoke of the industrial revolution, this revolution is quietly buzzing and seamlessly integrating itself into society and the lives of individuals, with little regard to its societal and behavioural impacts or the reaction of individuals. Increasing radical technological developments are creating multitudes of new emerging technologies in today's social environment. While some individuals are embracing these with excitement and anticipation, it seems not everyone is willing to adopt them; not everyone is willing to *trust* them.

Researchers have been delving into the phenomenon of trust for the past fifty years, building a new body of knowledge relating to its formation, development and implications. More recently, they have begun to turn the concept of trust towards technology. Previous trust research has been limited to interpersonal, institutional and inter-organisational trust, neglecting the fact that technology can be an object of trust too (Ellingson, 2003; Lewicki, Tomlinson, & Gillespie, 2006; Mayer, Davis, & David Schoorman, 1995; McAllister, 1995; McKnight, Cummings, & Chervany, 1998; Rotter, 1971; Rousseau, Sitkin, Burt, & Camerer, 1998; Zaheer, McEvily, & Perrone, 1998). The uniqueness of technology trust makes it especially relevant for research because the trust object is a thing, not a person or people-based construct connected to human emotion, expression or incentives (H. C. Brown, Poole, & Rodgers, 2004; Gefen, Benbasat, & Pavlou, 2008; Li, Hess, & Valacich, 2008; Xin Luo, Li, Zhang, & Shim, 2010; McKnight, Carter, Thatcher, & Clay, 2011; Pavlou, 2003; Vance, Elie-Dit-Cosaque, & Straub, 2008).

Historically, trust research has been predominantly found and curated in Psychology research, but has recently emerged as topical area of interest in e-commerce research. Although trust would intuitively seem to be a relevant factor in economic trade relationships and intentions, it only exists to a small extent within the Economics literature. While existing trust literature is limited, research in this area is relevant for academics and practitioners because of its significance to technology adoption research. It will also enable a better understanding of the social implications of technology and will add to the academic field of technology trust, specifically regarding initial trust formation. Understanding which factors and characteristics of technologies promote trust, as opposed to distrust, is relevant to

successfully market and implement technologies, support user adoption and effective technology utilisation success, and perhaps encourage brand loyalty and organisation reputation and goodwill invaluable (Gefen et al., 2008; Li et al., 2008; Lippert & Davis, 2006; Xin Luo et al., 2010; McKnight et al., 2011; McKnight, Liu, & Pentland, 2014; Pavlou, 2003).

McKnight et al. (2011) offer a theoretical basis for technology trust and call for further research to better understand and realise its potential opportunities. Most other research has taken the form of field studies and correlational analysis. Although field studies establish that variables are related, they do not allow inferences to be made about causation. It is unclear whether differences between individual technologies artefacts explain the variance in technology trust levels or whether it is the characteristics unique to technology as a class that explain the variance in trust from people-related trust research. If the latter is correct, this also begs the question of whether different sub-domains of technology also impact initial trust beliefs. This could have significant repercussions on the understanding of how individuals' trust and interact with technologies over time for both academics and practitioners. Successfully understanding how individuals' trust different technologies could impact how effectively academics and practitioners are able to support individuals to trust, use and adopt various sub-domains of technology by appropriately recognising and adjusting for their differences.

Personal information privacy (PIP) research has grown rapidly with the rise of the internet and increasing developments in technology, making it an area of modern interest. However, the literature is yet to identify a link between PIP threats to PIP and technology trust, a link which is intuitively valid and can be supported by several technology and privacy paradox theories which demonstrate the complex, and often irrational, natures of man-kind (M. M. Brown, 2015; Hajli, Sims, & Ibragimov, 2015; Holland, 2010; R. W. Jones & Ruffin, 2008; S. S. Jones, Heaton, Rudin, & Schneider, 2012; Mazey & Wingreen, 2017; Motiwalla & Li, 2016; Norberg, Horne, & Horne, 2007; Ohta & Ohta, 2008; Young & Quan-Haase, 2013). Trust is the willingness to accept risk and be vulnerable (Mayer et al., 1995). If someone, or something, poses a threat to an individual's PIP, it presents a risk that individuals must choose to accept. Individuals are innately risk adverse (Shapiro, 2005). Therefore, a perceived threat to PIP is likely to influence the formation of trust beliefs to some degree. This research seeks to investigate this theory by utilising, and further developing, the

characteristics of emerging technologies that threaten PIP identified by Conger, Pratt, and Loch (2013).

Technology is a driving force of today's world, becoming increasingly more embedded in the social and private lives of individuals. Emerging technologies are new technologies that are still in development, not yet fully exploited or yet to reach maturity (Conger et al., 2013; Einsiedel, 2008). They can be revolutionary and transformative with the potential to change industries and traditional relationships. They can be socially disruptive and could trigger new institutional rules and relationships (Einsiedel, 2008). In addition to increasingly complex designs, use and understanding, emerging technologies also share characteristics of "ubiquity, invisibility, invasiveness, collectability of heretofore uncollectible information, programmability and wireless network accessibility," which also pose threats to individuals' PIP (Conger et al., 2013). Perceived threats are relevant in the formation of trust beliefs, but have not yet been fully explored in the fields of PIP and trust in emerging technology artefacts. It is the combination of invasiveness, potential loss of autonomy, complexity and lack of understanding of emerging technologies which present threats to individuals and are relevant to technology trust.

The fact that trust beliefs determine an individual's intentions to interact with, use and adopt technology gives this research area significance (Lippert & Davis, 2006). Further research is not only important but its future implications invaluable (Gefen et al., 2008; Li et al., 2008; Xin Luo et al., 2010; McKnight et al., 2011; McKnight et al., 2014; Pavlou, 2003). Moreover, because technology trust affects e-commerce, IT implementation and technology support process effectiveness, technology trust research which gives regard to perceived threats to PIP, creates an opportunity to better understanding technology trust formation in new technologies and to better support individuals using unfamiliar technologies. Researching initial trust formation in emerging technologies presents even greater opportunities of value in an era where the rate of radical technology development is ever increasing. The lack of available first-hand knowledge and experience regarding emerging technologies means that perceptions of risk and uncertainty will surely be at their highest.

Therefore, this research addresses the following overarching research question:
RQ 1. What influences individuals to decide whether they can trust emerging technologies without prior experience or knowledge of the technology?

This thesis examines the current literature of technology trust and the characteristics of emerging technologies which present a simultaneous threat to users' PIP. It investigates whether perceived PIP threats influence initial technology trust levels for emerging technologies and explores the effects of different variables by proposing a new model for initial trust in emerging technologies. Because of the lack of significant research available, this research utilises a controlled post-test experiment for a number of emerging technologies to complement existing technology trust research. The experimental design offers greater external reliability and internal validity than existing literature on general trust research, while still maintaining sufficient levels of comparability with existing correlational analyses and field studies. Based on the surprising findings of the experiment it was decided to introduce a second study, which was not originally intended. This study used partial least squares structural equation modelling (PLS-SEM) analysis to further explore the variables which were theorised to affect initial trust in emerging technologies and supplement the findings of the primary experiment by investigating their predictive validity.

This thesis is organised as follows: it considers the existing literature, develops and proposes new theory (section 2), discusses the research methodology (section 3), experiment results and findings (section 4), PLS-SEM results and findings (section 5), contributions to knowledge (section 6), summary and conclusions (section 7), references (section 8) and appendices (section 9).

SECTION 2. LITERATURE & THEORETICAL DEVELOPMENT

Researchers have been delving into the phenomenon of trust for more than fifty years, but only recently has the concept of trust been turned towards technology. Existing trust literature in technology artefacts is limited. Nevertheless, technology trust research is important because of its alignment to technology adoption and Information Systems implementation research (Gefen et al., 2008; Li et al., 2008; Lippert & Davis, 2006; Xin Luo et al., 2010; McKnight et al., 2011; McKnight et al., 2014; Pavlou, 2003). McKnight et al. (2011) offers a theoretical basis for technology trust and its antecedents, but further research is necessary to better understand technology trust and realise its potential opportunities in supporting individuals interact with new technologies. This is especially true in the 21st century, an era in which individuals are increasingly more dependent on technologies and where emerging technologies are increasingly more radical and transformative. What's more, by the very nature of being "new and emerging," individuals have severely limited knowledge about these technologies to form reliable initial trust beliefs about whether to trust and use them, especially as their increasing sophistication presents greater threats to PIP (Conger et al., 2013). Individuals must depend on their own perceptions of a technology artefact, its vendors, their managers and the severity of its possible risks and threats. In this literature review, the general concepts of trust are described before exploring the relevance of popular, people-based trust theory to technology trust and, in particular, emerging technologies. Other variables which may also affect initial trust formation in emerging technologies are then discussed.

Note, two branches of hypothesis are proposed in this section. Hypotheses H1 to H7 relate to the primary relationship under investigation between perceived threats to PIP and initial technology trust in emerging technologies. Hypotheses Ha to Hj relate to a set of secondary effects and relationships which may impact initial technology trust in emerging technologies.

2.1. Trust

Trust is a widely discussed, interdisciplinary topic (Mayer et al., 1995; McKnight & Chervany, 2001; Rotter, 1971; Rousseau et al., 1998). While definitions vary, Mayer et al. (1995) is considered to have one of the best, robust definitions of trust (Lewicki et al., 2006) and has been widely cited across trust literature (Lau & Tan, 2006; Lewicki et al., 2006; McKnight & Chervany, 2001; Pavlou, 2003; Rousseau et al., 1998). They define trust as the

willingness to take on risk and be vulnerable irrespective of the ability to control the outcome or trustee. All at once it includes intentions, beliefs, behaviours, disposition and institutions as part of a dynamic phenomenon which changes according to the nature of risk and interdependencies of a situation (McKnight & Chervany, 2001; Rousseau et al., 1998). Trust is innately personal. It illustrates the extent to which we are willing to be completely vulnerable and subject ourselves to risk at someone – or something – else's hands. Subject to external forces, it is also affected by variables such as culture, subjective norms, education and institutional assurances (Gefen et al., 2008; Li et al., 2008; Xin Luo et al., 2010; Vance et al., 2008).

Most trust literature focusses on interpersonal trust where one individual trusts another individual due to some element of interdependence (H. C. Brown et al., 2004; Lau & Tan, 2006; Lewicki et al., 2006; Mayer et al., 1995; McKnight & Chervany, 2001; McKnight et al., 1998; Rotter, 1971; Rousseau et al., 1998). Different forms of trust were identified by Rousseau et al. (1998) including calculus-based trust, in which individuals employ rational decision-making and cost-benefit assessments to determine their course of action; relational-based trust, in which trust beliefs are dependent upon perceptions of reliability, past interactions and experience, and; institution-based trust, the belief that existing environmental structures will support a trust situation and lead to positive outcomes. The use of knowledge-based trust emerged to extend relational-based trust and is also very relevant to the topic of technology trust. Knowledge-based trust encompasses trust beliefs based on past interactions in addition to other information learned about the trustee through other experiences or second-hand knowledge (Lewicki et al., 2006; McKnight et al., 2011; Wingreen & Baglione, 2005). The necessity of understanding trust is identified as an important issue across a variety of research areas, specifically as an antecedent to engage in e-commerce and in technology adoption research (H. C. Brown et al., 2004; Gefen et al., 2008; Li et al., 2008; Lippert & Davis, 2006; Xin Luo et al., 2010; Pavlou, 2003; Vance et al., 2008; Wingreen & Baglione, 2005). An accurate understanding of technology trust could be critical to effectively supporting individuals to trust technologies, and the successfulness of intended change, interactions, use and adopt technologies, as well as promote organisational brand trust.

2.2. Technology Trust

Just as trust can be placed in another individual or entity, trust can be placed in a technology artefact. This form of trust, where the object of an individual's trust is a technology artefact,

will henceforth be referred to as "technology trust" in this thesis. With the growing developments and dependencies of technologies, it is certain that the role of technology trust will become more pivotal in everyday life as it governs how individuals interact with society and live their lives. Examples may include their use of transport, social media, robotics or biomedical technologies. In these contexts, the literature is unclear about how individuals trust inanimate objects or 'things' given that trust is innately personal, ruled by reason and emotion.

Whilst it has not been explicitly defined in current literature, technology trust can be presumed to be the willingness to be vulnerable and accept risks relating to the use of an information technology artefact, as adapted from Mayer et al. (1995). McKnight et al. (2011) discussed how technology trust is distinct from all other types of trust due to its unique focus on an object or thing. Instead of a person or person-built construct (e.g. organisations), the object of technology trust is a technology artefact with limited capabilities and whose trust situation relates to a lack of user control, user risks and uncertainties. This presents different risks regarding one's trust expectations. Whereas trust beliefs usually depend on beliefs regarding someone's competence, benevolence and integrity (i.e. "people-related" expectancies according to McKnight et al. (2011)), technology trust depends on the respective functionality, effectiveness and reliability of a technology (i.e. "technology-related" expectancies). Based on people-related expectancies, McKnight et al. (2011) defined the technology-related expectancies as:

Functionality – having the capabilities to do a task

Effectiveness – the ability to provide help when needed

Reliability – the ability to operate consistently without failing

These technology-related expectancies are similar to those trust beliefs identified by Lippert and Davis (2006) who suggested that technology trust was a product of a user's beliefs, or expectations, of a technology's predictability, reliability and utility. However, McKnight et al. (2011)'s translation of technology trust beliefs from people-related trust beliefs, and their respective definitions, appears most appropriate given the recognition and wide consensus of the meanings of competence, benevolence and integrity across the trust literature (Gefen et al., 2008; Mayer et al., 1995; McKnight et al., 1998). These trust beliefs can be defined as:

Competence – having the skills and ability to do a task

Benevolence – being of a caring, considerate nature with intentions of goodwill

Integrity – acceptable principles, being consistent in words and deeds, having a good reputation and sense of justice

Given that an individual's technology trust beliefs are dependent on their beliefs and expectations regarding its functionality, effectiveness and reliability, it would stand to reason that greater perceptions of these technology trust beliefs would increase one's technology trust. This is on the basis that stronger technology trust beliefs would seem to offer to compensate and protect individuals from the perceived risks exposed in trust situations.

The nature of technology trust and its antecedents are dynamic since their importance and relationships change over time. Research suggests that as knowledge-based trust increases, less reliance is placed on technology trust beliefs (Lewicki et al., 2006; McKnight et al., 2011; Wingreen & Baglione, 2005). It presumes when personal experience exists, it is perceived to be a more stable and reliable predictor in situations of uncertainty, taking precedence over rational observations that might be made and which would influence technology trust beliefs (McKnight et al., 2011). However, when no knowledge-based trust exists, second-hand knowledge can have a significant effect on initial trust beliefs (McKnight et al., 2014). This is because no previous interactions have taken place or personal experience is limited, infrequent or otherwise unreliable. In the context of technology, expert and consumer reviews are readily available on the internet, vendors will engage in promotional activities and marketing to endorse their products and provide additional product information, and individuals will seek recommendations from trusted friends and family about new technologies. Each of these situations' present different sources of second-hand knowledge that could, positively or negatively, influence an individual's technology trust beliefs by influencing the perceived level of risk that individuals would be challenged whether to accept. In the case of new and emerging technologies, individuals have no knowledge or personal experience of the technology artefact and are only able to rely on the second-hand knowledge sourced from others whom they must trust.

While a noteworthy amount of trust literature relating to information technologies exists, this is predominantly internet-based in regard to e-commerce (H. C. Brown et al., 2004; Chen & Barnes, 2007; Gefen et al., 2008; Li et al., 2008; Xin Luo et al., 2010; McKnight et al., 2014; Pavlou, 2003; Wingreen & Baglione, 2005). Trust in IT artefacts (referred to as "technology" for the purposes of this thesis and considered separate from websites in e-commerce research)

has been identified as a gap in the trust literature, particularly in relation to trust in new technologies and initial trust formation. Existing research in both technology trust and e-commerce trust neglect the effect of culture and socio-economic factors, despite the belief that this may have a significant effect on trust, just as it does in people-related trust (Gefen et al., 2008; Li et al., 2008; McKnight et al., 2011; Vance et al., 2008). The field of Information Systems favours the use of generalisable empirical research, embracing the positivist ontology. However, empirical technology trust research involving technology artefacts are very limited, and includes technologies such as a national government information system by Li et al. (2008), Microsoft Office products by McKnight et al. (2011) and a limited mix of technologies by McKnight et al. (2014) who found a "surprising" variation in technology trust across each technology.

The basis of technology trust theory is based upon, or at least remarkably consistent with, McKnight et al. (2011) who developed a theoretical framework for technology trust in addition to an empirical study regarding technology trust beliefs. In their study, they used MS Access and MS Excel as their technology objects, randomly assigned to a sample of first year Management Information Systems students in a survey. While their theory was robust, their choice of technology, combined with their population choice, weakened the strength of their findings. The problem being that both technologies were from the same, very reputable provider (Microsoft Office) and their saturation of those software markets meant there was a lack of comparable competitive products. Thus, it is possible that vendor-based trust may have been measured instead of technology trust, putting construct validity at considerable risk. It is also highly unlikely that the undergraduate students surveyed had experienced similar software products or needed to use either product at such a level to be aware of their limitations and full range of functionality to provide reliable responses since 78% of students had high school or college education and in total had reported only a mean period of 3.21 years' experience with MS Excel. In this case, it may be likely most students only had exposure to MS Excel as part of their high school or college curriculums.

Interesting to note is the scepticism that exists in the academic arena about whether technology can be a trust object, as noticed by Gefen et al. (2008). For Gefen et al. (2008), clarity is required about whether trust is behavioural or object-based in order for technology trust research to truly progress. They suggest it is object-based, dependent on the technology itself, with the ability to lead behaviour-based beliefs, and appears consistent with other

research in the literature. However, it is possible that people also impute their trust beliefs towards a technology's vendors or those responsible for the management of their PIP information, safety or privacy onto the technology. This means individual trust beliefs towards vendors, managers, organisations, institutions and humanity in general will determine how trustworthy technology is perceived. In this thesis, it is believed that technology trust is neither behavioural or object-based. Instead, it is likely to be combination of both, with object-based trust beliefs governing the greater part of initial trust formation. In addition to this, individuals are likely to also impute the trust beliefs of its people-related agents and, to some lesser extent, may also anthropomorphise the technology artefact.

2.3. Institution-based Trust

Institutional-based trust relates to the support structures that sustain and encourage risk taking and trusting behaviour as the belief that conditions exist to increase the likelihood of positive outcomes in trusting situations (McKnight & Chervany, 2001; Rousseau et al., 1998). Institutional-based trust consists of structural assurance and situational normality which encourage trusting intentions to form (Li et al., 2008; McKnight & Chervany, 2001; McKnight et al., 1998; Vance et al., 2008; Wingreen & Baglione, 2005). They are consistently defined in people-related trust literature and a large amount of e-commerce research according to McKnight and Chervany (2001) as:

> Structural assurance – the belief positive outcomes will occur due to contextual conditions such as regulations, contracts, monitoring and enforcement
>
> Situational normality – the belief that circumstances are normal, controlled and ordered and can therefore facilitate successful trust situations

McKnight et al. (2011) subsequently redefined these in specific regard to technology trust as:

> Structural assurance – "the belief that success with the specific technology is likely because, regardless of the characteristics of the specific technology, one believes structural conditions like guarantees, contracts, support, or other safeguards exist in the general type of technology that make success likely"
>
> Situational normality – "the belief that success with the specific technology is likely because one feels comfortable when one uses the general type of technology of which a specific technology may be an instance"

Research in online trust confirms that institutional-based trust influences trust intentions and website use as greater levels of institutional-based trust compensate for the perceived risks and uncertainty that exist in online interactions and transactions (Chen & Barnes, 2007; Gefen et al., 2008; Xin Luo et al., 2010; Pavlou, 2003; Wingreen & Baglione, 2005). While the uncertainty present in the online environment is not the same for technology because of the individual's ability to exert some degree of user control, a level of uncertainty will always be prevalent when users are not familiar with a technology's functionality, effectiveness or reliability. Further uncertainty might also exist regarding user safety and the intentions behind a technology's extra capabilities that do not relate to its general purpose. These include the collection of user information, automatic software changes and wireless accessibility.

It is theorised that technology trust beliefs will be influenced by an individuals' institutional-based trust beliefs. Greater levels of perceived structural assurance mean that individuals believe that a technology will have a higher minimum level of functionality, effectiveness and reliability because of factors like consumer protection laws, manufacturing standards or vendor guarantees, minimising the associated uncertainty and risk. On the other hand, greater perceived situational normality will reduce potential uncertainty due to the familiarity an individual might have with similar technologies (McKnight et al., 2011). Greater situational normality will give individuals greater confidence about the certainty that a technology has minimum levels of functionality, effectiveness and reliability and its likely limitations. The more confident individuals are about these, the more able they are to take cautionary preventative measures to protect themselves from possible risk and the likelihood of it being realised.

2.4. Initial Technology Trust

'Initial trust' is usually applied to situations where individuals first interact and trust beliefs are not based on any experience or first-hand knowledge (Li et al., 2008; McKnight et al., 1998). It is the point from which future experiences are based upon and trust increases or decreases over time (Gefen et al., 2008; Lewicki et al., 2006; McKnight et al., 1998; Rousseau et al., 1998). Trust can motivate behaviour and adoption (Gefen et al., 2008; Li et al., 2008; Lippert & Davis, 2006; Xin Luo et al., 2010; McKnight et al., 2011; McKnight et al., 2014; Pavlou, 2003). Therefore, initial trust beliefs can be pivotal in establishing new expectations and patterns of behaviour going into the future. If initial trust beliefs are

relatively low, individuals may be less tolerant to uncertainty and unlikely to accept risk when deciding whether to try something new or unfamiliar in future situations. Their low or negative trust beliefs may also skew any positive experiences they may have and frame future experiences and expectations. It could even lead to distrust which promotes active avoidance behaviour (Gefen et al., 2008; Lewicki et al., 2006)

Literature on theorised initial trust levels vary (Lewicki et al., 2006) although research suggests it tends to be moderate to high due to personal disposition, norms, structural assurances and situational normality (McKnight et al., 1998; Rousseau et al., 1998). This is perhaps because of the lack of previous knowledge and personal experience with the other party, indicating that initial trust is a cognitive process which emphasizes calculus-based trust (Li et al., 2008; McKnight et al., 2011; Rousseau et al., 1998). The absence of knowledge-based trust means individuals are more likely to rely on second-hand information from other individuals with first-hand knowledge, personal intuition, contextual factors, generalised expectancies and other similar experiences to form initial trust beliefs (Li et al., 2008; Rotter, 1971).

People-related trust research suggests disposition and institution-based trust play a role in initial trust and that reliance on institution-based trust increases when situations are novel, ambiguous or lack certainty (Li et al., 2008; McKnight & Chervany, 2001; Rousseau et al., 1998; Vance et al., 2008). This is likely to apply to initial technology trust levels because of the limited amounts of knowledge-based trust which forces individuals to rely on other indicators of trust (Chen & Barnes, 2007; Li et al., 2008; McKnight et al., 2011; Vance et al., 2008). According to McKnight et al. (2011), institutional-based trust has been found to have a negative relationship with knowledge-based trust. This means as the frequency of interactions with technology objects grow, less reliance is placed on institutional-based trust.

Of the existing empirical research in technology trust reviewed, only Li et al. (2008) researched initial technology trust. They proposed a model to examine initial trust in technology generally and found faith in humanity, trust stance, technological situational normality and structural assurance did not affect initial technology trust. On the other hand, organisational situational normality, reputation, calculus-based trust and social norms were significant factors and were consistent with e-commerce trust research. Under McKnight et al. (2011), some of these variables are people-related trust dimensions. This includes faith in

humanity and trust stance, which McKnight et al. (2011) proposed should be translated to faith in general technology and technology trust stance. Despite this, Li et al. (2008)'s faith in humanity hypothesis may still be valid regarding initial technology trust given the role of vendor-based trust in technology trust formation, as discussed in section 2.7. Furthermore, Xueming Luo (2002) suggest perceived usefulness, perceived risk, culture, norms, self-efficacy and other socio-economic factors would be likely to influence initial technology trust. These variables are consistent with some of the variables proposed by Pavlou (2003) using the Technology Acceptance Model as the foundation of his hypothesis.

Previous research in technology trust has been based on non-emerging technology artefacts without proper consideration as to whether sub-classes of technology embody intrinsically distinct characteristics which might cause variation in the formation of technology trust. By neglecting this, they purport to assume that they are the same and their trusting situations are similar. However, it is theorised that the relationships in the context in emerging technologies are different and perhaps more critical than those in the context of non-emerging technologies.

2.5. Emerging Technologies

The growing trend of emerging technologies is a feature of today's modern world and includes information technologies, biotechnologies, nanotechnologies, robotics, internet of things, virtual reality and genomics to name a few (Bacca, Baldiris, Fabregat, Graf, & Kinshuk, 2014; Conger et al., 2013; Einsiedel, 2008; Grewal, Roggeveen, & Nordfält, 2017; Leggett, 2017; MGI, 2013; Pycroft et al., 2016a). While there has been extensive research conducted across a variety of disciplines under the label of "emerging technology" (Arora, Youtie, Shapira, Gao, & Ma, 2013; Fredrich et al., 2014; Xin Luo et al., 2010; Usal & Nouri, 2014), efforts to define what an "emerging technology" actually is remain neglected and seemingly taken for granted.

One of the few researchers to define the term, Einsiedel (2008) describes emerging technologies as being in the developmental stage of production, in the early stages of commercialisation or not yet fully exploited by firms, involving forward thinking and planning. They are revolutionary and transformative in nature with the capacity to change a wide range of sectors and shift traditional relationships. Thus, Einsiedel (2008) says they can be socially disruptive and may trigger new institutional rules and arrangements. This

recognition of emerging technologies as both social and technical is particularly relevant to the fields of trust and Information Systems. A more prominent source for emerging technology research, Conger et al. (2013) defined emerging technologies as technologies "coming into existence or maturity" featuring characteristics which threaten PIP in a way non-emerging technologies do not.

Most research uses the term "emerging" as an operational term for upgrades or new versions of an existing technology, which is not correct according to the definition proposed here. Emerging technologies are not upgrades or new versions of an existing, commercialised and matured technology e.g. iPhone 7 to iPhone 8, Microsoft Windows 7 to Microsoft Windows 10 or a manual transmission car to an automatic transmission car. In each of these cases, the fundamental technology already existed but was re-engineered or improved to create a more advanced or efficient version of the same product or service. On the other hand, blockchain is an emerging technology but, different versions of blockchain-based currencies (e.g. Bitcoin vs Ethereum) or decentralised autonomous organisations that are released over time utilising different and varied instances of blockchain are not "emerging technologies" in of themselves.

The following subsections theorise the unique characteristics of emerging technologies as opposed to non-emerging technologies, the particular relevant of initial trust in emerging technologies compared to non-emerging technologies, and the relationship between technologies and perceived threats to PIP.

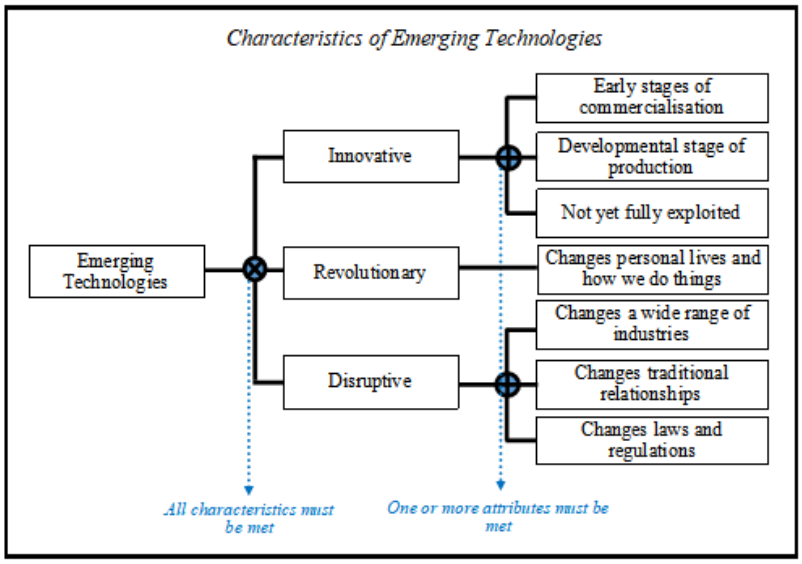
2.5.1. Characteristics of "Emerging" Technology

For the course of this research, a framework to identify whether a technology is "emergent" is proposed based on Einsiedel (2008)'s discussion about what is an emerging technology. Einsiedel (2008) did not provide any test or model from which emerging technologies could be identified, or any measurements or scales to this end. Therefore, the framework, criterion and corresponding measurements proposed here will be one of the contributions of this research and will enable researchers to be able to test whether new technologies have the necessary characteristics to be labelled an "emerging" technology consistently over time. To pass this test and be considered as an emerging technology each key characteristic must be satisfied. These characteristics are innovativeness, revolutionary and disruptiveness (as illustrated in figure 1). As emerging technologies transition into a state of non-emergence,

these characteristics will change as the social landscape from which they originally derived adapts, becoming outmoded and primeval.

1. Innovativeness

Figure 1



All emerging technologies possess an element of "innovativeness." Consistent with the Oxford definition of innovativeness, emerging technologies embody either new, advanced or original ideas, methods or designs. As characterised by Einsiedel (2008), they typically are not yet fully exploited, are in the developmental stages of production or in the early stages of commercialisation; factors which contribute to their general perception of being "new." As such, they are relatively novel, largely underutilised and with potential still to be had. "Innovativeness" knows no definitive boundaries, instead it is vague and subjective and will likely become more contentious as a technology matures and reaches the tipping point of commercialisation.

2. Revolutionary

For a technology to be considered truly emergent, it must have the potential to change our everyday lives in the way we behave, interact and do things. Several technologies exist today that have achieved this feat. Mobile phones and the internet are among the most prominent in the last few decades, in addition to automobile and aviation technology development in the last century. Emerging technologies may even change the way that we live by biologically sustaining the body and assisting the performance of bodily functions beyond what we would otherwise be capable of. Examples of such technologies include cardio pacemakers, bionic limbs or biotechnologies which release chemicals and drugs to regulate our muscles or

hormones (Allianz-Aktiengesellschaft & OECD., 2005; Royal Society & Royal Academy of Engineering, 2004; Touhami, 2014).

3. Disruptive

Emerging technologies are disruptive. Not only do they revolutionise and transform the lives of individuals, they disrupt the wider society by triggering changes in a range of industries, traditional relationships and/or laws and regulations (Einsiedel, 2008; Rayna & Striukova, 2016). Triggering a change "in a range of industries" refers to the economic adjustment of markets in more than one industry, forced by the introduction of an emerging technology (Rayna & Striukova, 2016). This may cause the birth of new markets, a shift in current markets or a significant change in the production and delivery of goods and services in a market. Only the degree of technological obsolesce of a society will limit the speed and effect of these technologies, rather than geographic borders. A change in the "traditional relationships" refers to the change in dynamics between roles such as buyer and seller, governing bodies and the public or between man, woman and child. An example of a such a relationship change is in the use of internet technology which shifted the traditional roles of seller and buyer in the e-commerce space. This gave buyers greater accessibility to markets and greater bargaining power than their counterparts (Behrang, Bornemann, Hansen, & Schrader, 2006; Porter, 2001). It also triggered the electronics industry and affected a wide range of consumer industries. Subsequently, emerging technology may trigger changes in laws or regulations because of their disruptive nature. This might relate to health and safety, legislation regulating its use, manufacturing standards, product or trade guarantees.

2.5.2. Emerging Technologies & Initial Technology Trust

Technologies are developing at an ever-increasing rate, growing more radical and transformative, and causing more emerging technologies to populate society. The lack of available first-hand knowledge and experience available for emerging technologies means that for each new major technological development individuals are being confronted with more and more initial technology trust dilemmas. By definition, emerging technologies are relatively unknown, and individuals have not yet encountered it or have little or no experience with it. Compared to any other technology trust situation, the perceptions of risk and uncertainty of emerging technologies will surely be at their highest in the initial formation of trust given no other technology offers even close resemblance.

Research by Xin Luo et al. (2010) claimed to study initial trust in emerging technologies in the use of mobile-banking. However, according to the definition adopted in this research mobile-banking cannot be considered an emerging technology as it was an already commercialised, exploited technology. Although trust in technology was researched, the validity of their initial trust measures is questionable given the variance in existing knowledge and experience of subjects who have used mobile-banking. Despite this, Xin Luo et al. (2010) suggest perceived usefulness, perceived risk, culture, norms, self-efficacy and other socio-economic factors would be likely to influence initial technology trust. These variables are consistent with some of the variables proposed by Pavlou (2003) using the Technology Acceptance Model as the foundation of his hypothesis.

In addition to increasingly complex designs, use and understanding, emerging technologies also share characteristics of "ubiquity, invisibility, invasiveness, collectability of heretofore uncollectible information, programmability and wireless network accessibility," which also pose threats to individuals' personal information privacy (PIP) (Conger et al., 2013). If trust is the willingness to accept risk and be vulnerable, perceived threats to PIP are likely to be relevant in the formation of technology trust beliefs.

2.5.3. Technology Trust & Personal Information Privacy Threats

The research field of personal information privacy (PIP) has grown rapidly with the emergence of the internet in the 1990s and the development of technologies making it a relevant area of interest for this era. Martin, Gupta, Wingreen, and Mills (2015) described PIP as being a key challenge in the modern digital age where "a vast spectrum and variety of data, not mere demographic and transactional, are routinely shared." This presents a challenge for individuals who must choose to be vulnerable to technology artefacts and the entities who can control or possess their personal information and trust they will not abuse it.

Existing research has identified the relevance between PIP and trust research in the e-commerce literature, but it does not distinguish between different PIP threats, concerns or technology characteristics that pose threats to PIP and their effect on different types of trust (Bélanger & Crossler, 2011; Dinev, McConnell, & Smith, 2015; Eastlick, Lotz, & Warrington, 2006; Xueming Luo, 2002; Malhotra, Kim, & Agarwal, 2004; Metzger, 2004; Smith, Dinev, & Xu, 2011). Research indicates that PIP concerns and trust have a negative relationship and the extent of an individual's privacy concern will vary according to the

websites they use (Smith et al., 2011). PIP concerns can be likened to perceived threats to PIP given that a risk, threat or vulnerability must first be identified for an individual to become concerned with its source.

Following this, if someone, or something, poses a threat to an individual's PIP, it presents a risk that individuals must choose to accept or reject. PIP threats are relevant in the formation of trust by the very definition of trust, which is the williness to accept risk and be vulnerable (Mayer et al., 1995). Hence, perceived threats to PIP are likely to influence the formation of trust beliefs. This is particularly relevant for emerging technologies, especially given the combination of invasiveness, potential loss of autonomy, complexity and lack of understanding of emerging technologies. Existing theory supports this, although it is yet to be tested (Conger et al., 2013). This rationale only highlights the relationship between privacy and technology trust research, which has been left neglected and unexplored. Therefore, it is hypothesised:

Ha. Greater levels of perceived threats to PIP will decrease initial technology trust in emerging technologies, and vice versa.

2.6. Personal Information Privacy

This section explores PIP literature, which this thesis builds on by defining and explaining different types of PIP threats that has been identified Conger et al. (2013). These definitions are a contribution of this research. Key concepts of vendor-based trust and institutional-based trust are established and arguments that PIP threats are relevant to these constructs are given. These constructs are further developed in relation to technology trust in section 2.7.

2.6.1. Emerging Technology Personal Information Threats

In their study, Martin et al. (2015) proposed that the main factors that affect perceived threats to PIP relate to the disclosure, awareness, storage, use and collection of information. More specifically, in regards to technology induced PIP threats, Conger et al. (2013) identified the characteristics of ubiquity, invisibility, invasiveness, collectability of information, programmability and wireless accessibility which represent a threat to individuals' PIP, but did not define, develop or test these. Conger et al. (2013) refers to ubiquity as a PIP threat and a characteristic of emerging technology simultaneously. Although its meaning is clear in the field of Information Systems, it is more commonly

regarded as the extent to which something is perceived as being everywhere. For the course of this research, two limbs of ubiquity are proposed: physical ubiquity and network ubiquity. The Information Systems literature seems to mostly concern itself with network ubiquity. However, non-experts often consider the term "ubiquity" for technologies in two regards, its physical state and its information or networking state. Therefore, the definitions for physical and network ubiquity are proposed for clarity. In addition, because Conger et al. (2013) did not develop or define any other of their characteristics, it would be prudent to explicitly define the remaining characteristics for completeness. The definitions for these characteristics, which also pose a threat to PIP, will be another contribution of this research.

2.6.1.1. Physical Ubiquity

Physical ubiquity is associated with the degree of familiarity or awareness individuals have with technology being present in everyday life. It also includes the ability to interact with it. For instance, light bulbs and mobile phones would be physically ubiquitous whereas 3D or 4D printers and bionic organs would not. The awareness of a technology in its physical state can serve as a physical reminder of its presence and operations, allowing a degree of comfort in that the users are more aware and may retain greater control over it and their PIP. Thus, greater perceptions of physical ubiquity present a perceived PIP threat in the sense that individuals feel more overwhelmed and less able to control or escape from a technology and its operations. This means they are more likely to perceive a constant threat to their PIP, requiring more exhaustive efforts to maintain a consistent level of defence and control over their PIP. Therefore, it is hypothesised:

H1. Greater perceptions of physical ubiquity will decrease initial technology trust in emerging technologies, and vice versa

2.6.1.2. Network Ubiquity

Network ubiquity is the extent to which technologies are connected to other entities, technologies, systems and programmes in order to share information and that this network is known to individuals. For instance, mobile phones have covert network ubiquity due to their connectivity to the internet, different devices, apps and their providers, manufacturers and cell-phone providers. These actors form part of a larger, unknown network due to their relationships with other systems and entities e.g. third-party agencies. The extent to which a technology is connected to multiple network actors refers to its network ubiquity. Greater

perceptions of network ubiquity mean that individuals believe a technology is connected to multiple network actors to share information. This presents a perceived PIP threat because it decreases the control individuals have over the distribution of their personal information. While they may be content with the primary entity to gain access to some of their personal information, they may not be willing for other entities to have that same information due to a lack of trust or necessity. Therefore, it is hypothesised:

H2. Greater perceptions of network ubiquity will decrease initial technology trust in emerging technologies, and vice versa

2.6.1.3. Invisibility

Invisibility is the degree to which a technology can operate autonomously and inconspicuously, without disrupting an individual's daily activities. There is a growing trend of technologies to become more invisible to increase user friendliness. However, invisibility increases the likelihood that a technology will be forgotten about, presenting a risk to PIP by increasing the risk that individuals will forget to act in a cautionary manner to safeguard their PIP. Thus, they are more likely to suffer a breach of their PIP. The cause for this is different to physical ubiquity where individuals are aware of a technology and its operation but, due to its omnipresent risk, fail to act cautiously because of exhaustion. An example of this in the use of surveillance technologies in George Orwell's novel *1984.* In the case of invisibility, individuals fail to act defensively altogether because they forget about the technology due to its seamless integration into their lives. This leads them into a false impression of PIP safety and lowering their defensive strategies. Examples of this include mobile phone apps, medical devices and many new instances of technologies incorporating internet of things, such as smart refrigerators which tell you when you are low on milk, or cleaning robots that have learned to pause and get out jjhof your way between 7 – 8am each weekday and resume cleaning activities once you have gone to work.

This link between invisibility and perceived PIP threats may not be intuitive because invisibility may be considered to not cause any immediate or direct issues which will impact PIP, perhaps creating a case for invisibility supporting positive initial trust formation. However, that is not the argument proposed here and it is believed that greater levels of perceived invisibility will make individuals more wary to perceived threats to PIP, causing a decrease in initial trust beliefs in emerging technologies. Therefore, it is hypothesised:

H3. Greater perceptions of invisibility will decrease initial technology trust in emerging technologies, and vice versa

2.6.1.4. Invasiveness

Invasiveness is the extent to which a technology can penetrate the private lives of individuals. With society's growing dependence and reliance on technologies, technologies are becoming more embedded into the private lives of individuals, allowing them greater access to our most private habits, routines and information. Such details of ourselves and our private lives are usually what we seek to protect when we defend our PIP. But, the reliance we can place on technologies is addictive. Again, mobile phones present a great example; mobile phones never leave our side, are seldom switched off and in constant use. We are constantly engaged with them. Through our mobile phones, organisations have the potential to track our locations, identify our daily routines, establish when we wake and sleep due routine activity levels and predictive analytics. They have the potential to record how we use our mobile phones, the software applications most used and devices we most often connect to and the purposes for which they connect. With the use of biotechnologies, technologies will soon gain access to our biochemistry, health and food habits, and advanced surveillance technologies equipped with sophisticated sensors can, already, essentially see through walls. Thus, the more a technology is perceived to be able to invade an individual's private life, the greater risk to PIP it presents. Therefore, it is hypothesised:

H4. Greater perceptions of invasiveness will decrease initial technology trust in emerging technologies, and vice versa

2.6.1.5. Collectability of Information

Collectability of information is the extent to which a technology artefact can gather personal information. As technologies become more advanced, they are being built with increased capabilities. This increases the functionality, effectiveness and reliability of a technology for the purposes for which it was designed, it also means technologies may possess a new host of capabilities which can be used to more effectively collect, store and analyse personal information. For instance, an autonomous car which records all the destinations it goes, the routes taken, number of passengers, images of passengers, entertainment preferences of passengers, location preferences (such as Starbuck's stores vs Coffee Culture or

MacDonald's vs Burger King), and is linked to the driver's mobile phone contacts and email account, analysing all these records to predict locations for driving and offer entertainment content would be considered a greater threat to PIP than an autonomous car which drivers only enter the end destination and keeps no record of the trip after a short period of time (Lafrance, 2016). This would suggest that the more a technology is perceived to be able to collect personal information, the more of a threat it would present to an individual's PIP. Therefore, it is hypothesised:

H5. Greater perceptions of collectability of information will decrease initial technology trust in emerging technologies, and vice versa

2.6.1.6. Programmability

Programmability is the extent to which individuals can control a technology's "functionality" and "effectiveness" (refer to McKnight et al. (2011)). With technology's growing complexity of functionality and capacity for autonomy, lower levels of perceived programmability will create a greater risk to PIP. This is because individuals believe they are less able to control the operations of a technology and, by association, its possible activities relating to the collection and communication of personal information. Programmability is concerned about user control, including the ability to manage autonomous activities and override default settings in order to determine how and when a technology performs. In the autonomous car example, if the driver can choose to disable its connection to his or her email account and/or mobile phone contacts, disable its ability to log destination or entertainment preferences, or switch off its analytic capabilities to and no longer provide suggestions for locations, this may reduce the driver's perceived threat to PIP. Therefore, it is hypothesised:

H6. Lower perceptions of programmability will decrease initial technology trust in emerging technologies, and vice versa

2.6.1.7. Wireless Accessibility

Wireless accessibility is a technology artefact's ability to access and upload information from the internet and communicate with other wireless devices. The greater a technology's wireless accessibility, the greater perceived threat to an individual's PIP it presents. This is because regardless of how much personal information it has access to and how much

personal information it can collect, it does not present a threat to one's PIP unless it is known by someone else who has the ability to use and exploit it, such as marketers, vendors, management, competitors or disgruntled acquaintances. If a technology has greater wireless accessibility, it suggests that it is in greater communication with other devices, systems and entities and is more likely to be sharing personal information. Therefore, it is hypothesised:

H7. Greater perceptions of wireless accessibility will decrease initial technology trust in emerging technologies, and vice versa

2.6.1.8. Changing states of emergence and personal information threats

By generating hypotheses H1 to H7, it has been implicitly assumed that Ha will be supported to show that greater perceived threats to PIP will decrease initial technology trust beliefs in emerging technologies. In addition to this, it is also hypothesised:

Hb. As individuals consider technology artefacts to be more "emergent," they will perceive increased threats to PIP

It is important to note that as emerging technologies transition to a state of non-emergence, the above PIP threats will remain an inherent characteristic of the technologies. But, as the development and implementation of emerging technologies increase, emerging technologies will populate society and become the new standard of technology. Consequently, these PIP threats may no longer be unique to emerging technologies, but rather both emerging and non-emerging technologies.

Generally, perceived threats to PIP are likely to remain static over time given the calculative nature of risk. Therefore, to diminish the perceived risk of PIP threats technology trust levels will need to increase. Such technology trust will increase over time as knowledge-based trust grows and a history of positive experiences develops which allows trust to supersede PIP threat risks. This can be explained by generalised expectancy theory (Bandura, 1997; Mazey & Wingreen, 2017; McKnight et al., 2011; Rotter, 1971). Generalised expectancy theory theorises that a technology may be perceived as a threat when it is novel and unfamiliar, but as it becomes more known and familiar to individuals, initial generalised expectancies may change. This is because individuals were unable to form reliable generalised expectancies when they first encountered the technology and adjust their expectations accordingly as more

reliable knowledge becomes available (Bandura, 1997; Mazey & Wingreen, 2017; McKnight et al., 2011; Rotter, 1971). This is relevant to the context of emerging technologies, where individuals have little to no experience or familiarity of emerging technologies. As a result, knowledge-based trust may positively impact technology trust beliefs by decreasing the perceived threats to PIP and causing technology trust beliefs in emerging technologies to increase by comparison. However, the context of uncertainty is less applicable for non-emerging technologies when forming initial generalised expectancies. Instead, it is theorised that perceived PIP threats remain relatively constant over time for non-emerging technologies and increasing levels of knowledge-based trust will cause an increase in technology-trust beliefs only.

2.6.2. Vendor-based Trust & Personal Information Privacy Threats

E-commerce research indicates that perceived threats to PIP decrease trust in online transactions (Thaw, Mahmood, & Dominic, 2009). Recent unpublished research conducted at the University of Canterbury also suggest a very significant relationship exists between vendor intentions, a consumer's PIP beliefs and trust in online websites. Such findings might suggest that vendor-based trust will mediate perceived threats to PIP from a technology artefact. Vendor-based trust (see section 2.7.2.) is the trust beliefs consumers have in a vendor's competence, benevolence and integrity (Li, Rong, & Thatcher, 2012; Wingreen & Baglione, 2005). In the context of emerging technologies in this thesis, "vendor" may apply to retail providers, manufacturers, the key creator or designer(s) responsible for its inception, or management requesting and implementing the emerging technology. Therefore, should an individual's belief that a vendor would not act in a risky manner regarding their PIP would result in a lower perceived threat to PIP than those who believe otherwise.

Vendor-based trust is theorised to be influenced by an individual's faith in humanity (McKnight et al., 1998). Therefore, when specific vendors are unknown, faith in humanity may be used as a proxy for vendor-based trust and will subsequently influence perceived threats to PIP, as well as technology trust (see section 2.7.2.1.).

2.6.3. Institution-based Trust & Personal Information Privacy Threats

The role of institutional-based trust has been found to mediate privacy concerns (Smith et al., 2011). This is because of the belief that contextual guarantees, regulations and contracts exist to mitigate perceived PIP threats (Xueming Luo, 2002). While this is true for existing

technologies, such as e-commerce where most privacy and trust research currently exist, this may not hold for less established technologies. In the case of emerging technologies specifically, laws and regulations are often too slow to adapt to adequately protect individuals in a timely manner. Consequently, individuals may have lower levels of institutional-based trust for more emergent technology and the greater perceived threat to PIP they pose.

2.7. Factors Influencing Initial Technology Trust

2.7.1. Disposition to Technology Trust & Disposition to Trust Generally

Disposition (also known as "propensity") to trust has been defined as the general willingness to be vulnerable and accept risks (Mayer et al., 1995; McKnight & Chervany, 2001). It is based upon an individual's generalised expectancies, personality and influenced by upbringing and culture (Rotter, 1971). According to Mayer et al. (1995), it explains the variance in trust levels held by individuals. H. C. Brown et al. (2004) illustrated these relationships through their use of the Interpersonal Circumplex model, also noting that a disposition to technology trust exists. Further to this, McKnight and Chervany (2001) proposed that disposition to trust is a function of an individual's faith in humanity and trust stance. They defined faith in humanity as the belief that others are generally reliable and well-intended. Likewise, they defined trust stance as the belief that trusting others generally leads to more positive outcomes than acting alone. McKnight et al. (2011) applied all these ideas in their technology trust research and translation of people-related trust constructs. They defined disposition to trust technology as "the willingness to depend on a technology across situations and technologies," comprised of faith in general technology and technology trust stance. Similar to Li et al. (2008) in their research about initial technology trust, McKnight et al. (2011) also hold that disposition to trust is closely related to institutional-based trust.

Individuals with a strong faith in general technology believe that technologies are usually trustworthy. They assume all technologies have a minimum level of functionality, effectiveness and reliability that they can be depended upon, and their trust beliefs will vary for different technologies only if evidence urges them to. Individuals with a strong trust stance are more optimistic about the benefits of trusting technologies than those who have a low trust stance. They are more inclined to incorporate technologies in their daily routines in the belief that they are more likely to yield positive outcomes than without them in a calculated cost-benefit analysis. It is also quite likely that individuals with a benevolent trusting nature will be less sensitive to evidence that has a negative effect on one's trusting

beliefs than those who have a low propensity to trust. Therefore, for the context of emerging technologies, it is hypothesised:

Hc. Greater dispositions to technology trust will increase initial technology trust in emerging technologies
Hd. Greater dispositions to trust generally will increase initial technology trust in emerging technologies

2.7.2. VENDOR-BASED TRUST

Vendor-based trust is defined as the trust beliefs consumers have regarding a vendor's trustworthiness, including the beliefs regarding their competence, benevolence and integrity which represent different dimensions of vendor-based trust (Li et al., 2012; Wingreen & Baglione, 2005). It is a people-related trust, based on an actual person or collective of people (Li et al., 2012; McKnight et al., 2011; McKnight et al., 1998; Pavlou, 2003; Wingreen & Baglione, 2005).

Li et al. (2008) hypothesized that vendor-based trust has a positive effect on technology trust. The argument for this is that in situations of uncertainty regarding a technology, individuals may have very low trust beliefs in a technology's functionality, effectiveness and reliability due to a lack of previous experience, perceived structural assurances and situational normality i.e. low levels of knowledge-based trust or institutional-based trust. This could be worsened by a weak disposition to trust. However, where individuals have had experience with a vendor from previous interactions, transactions or have acquired relevant second-hand knowledge that enables them to form person-related trust beliefs regarding their competence, benevolence and integrity, this is likely to have a positive effect on technology trust (Li et al., 2008). Strong beliefs in a vendor's competence, benevolence and integrity would suggest that they can produce a functional, effective and reliable piece of technology so that vendor trust beliefs are imputed towards the technology. This may be more prevalent in initial technology trust, where individuals have no previous experience of a technology, but it is likely to affect technology trust beyond this as well. For instance, some users of Apple have such high trust beliefs in Apple that they are likely to have higher levels of technology trust for their products than what they might for an identical product produced by Samsung, Microsoft or Google. Other users may then buy an Apple product which they then find unsatisfactory but will continue to use it, still buy more Apple products, and, in the case of faulty products, will

exchange it for a new version of the same product with the belief that the new one will not be faulty and will be functional, effective and reliable. Existing trust research does not exist to confirm or support these premises, but would be an area of relevance for future trust research to better understand the relationships between vendor trust and technology trust. Marketing research around brand loyalty and brand trust would appear to support this however (Delgado-Ballester & Munuera-Alemán, 2001; Dick & Basu, 1994).

Li et al. (2008) failed to find significant results to support the hypothesis that vendor-based trust affects initial technology trust. However, Li et al. (2008)'s use of technology (a state National Identity System) was not well suited to invoke feelings of vendor-based trust. This is because of its remoteness to a single entity who acted as a vendor, and it is argued that this was reflected in their non-significant results. Thus, it is theorised that vendor-based trust has a positive influence on technology trust levels and that research that is appropriately designed for this context would confirm this. In the context of emerging technologies, vendor-based trust needs to refer to at least one entity who is primarily responsible for its design, implementation and/or use in a way that they may impact the emerging technology's functionality, effectiveness or reliability.

2.7.2.1. Vendor-based Trust, Faith in Humanity & Initial Technology Trust

An individual's faith in humanity is likely to be a relevant variable in determining technology trust, particularly initial technology trust in the context of emerging technologies, when vendor-based trust cannot be ascertained. Research does not exist to support this premise, but faith in humanity has been theorised to have a positive effect on technology trust beliefs (McKnight et al., 2011) and vendor-based trust (Li et al., 2008; McKnight et al., 1998). In accordance with Li et al. (2008), it is believed that faith in humanity influences vendor-based trust, and vendor-based trust influences technology trust. However, in cases where vendors are not identifiable or unknown, as they may be for some emerging technologies, an individual's faith in humanity may be used as a proxy for vendor-based trust beliefs to evaluate the perceived intentions of those who produce or manage a technology artefact, and form technology trust beliefs. This is because faith in humanity represents the trustworthiness of a collective of individuals who represent part of a trustor's social universe. Faith in humanity is also an antecedent of disposition to people-related trust which suggests that it is more likely to affect, and represent, vendor-based trust beliefs rather than technology trust (McKnight et al., 2011). It is possible individual's may be more sensitive to vendor-based

trust and faith in humanity beliefs for emerging technologies because of low knowledge-based trust. Therefore, it is hypothesised:

He. When a specific vendor for an emerging technology artefact is not identifiable or unknown, greater faith in humanity will decrease perceived threats to PIP and vice versa
Hf. When a specific vendor for an emerging technology artefact is not identifiable or unknown, greater faith in humanity will increase initial technology trust in emerging technologies and vice versa

2.7.3. Subjective Norms

Subjective norms are normative beliefs held by individuals about people in society that they consider important, and their desire to act according to their expectations about how they should act and behave (Cobelli, Gill, Cassia, & Ugolini, 2014; Kaushik & Rahman, 2015; Li et al., 2008; Lippert & Davis, 2006; Pavlou & Fygenson, 2006). These social pressures can influence individual's decisions, behaviours, actions and responses to events (Kaushik & Rahman, 2015; Li et al., 2008). Subjective norms have been found to have a significant effect on trust in technology trust and e-commerce trust research (Gefen, 2000; Li et al., 2008), as well as behavioural intention in technology adoption research (Kaushik & Rahman, 2015).

With trust as a significant antecedent to technology adoption (Gefen et al., 2008; Li et al., 2008; Lippert & Davis, 2006), it would seem logical to propose that subjective norms influence trust, which in turn influences technology adoption. Thus, subjective norms have a direct, positive relationship with trust and demonstrates the strong relationship between trust and technology adoption. This is likely to be because when individuals feel pressured to adopt a technology artefact they feel pressured to trust it as well. The pressure to conform and accept some technology risks and uncertainty as a socially acceptable position of vulnerability would suggest greater subjective norms will lead to increased levels of technology trust, even if it is not entirely of the individual's own accord or willingness.

For instance, a risk-adverse individual who cares deeply about what others think about him might choose to accept a once in a lifetime offer to own and use a luxury jetpack, on condition he uses it at least twice a week. He is aware that jetpacks are still in a prototyping, not commercialised state, and presents many risks. However, he accepts the offer because he knows all his friends and colleagues believe jetpacks are safe, useful, of great value and a

mark of social status; and that he would be foolish to say no. Without the social pressure to accept such uncertainty and risk, this individual is unlikely to have accepted such an offer or trust the jetpack for everyday use.

Interestingly, Li et al. (2008) found subjective norms had the greatest impact on technology trust of all of their proposed variables, significantly affecting individual trusting beliefs, trusting attitude and trusting intention. Cobelli et al. (2014) found subjective norms also mediated trust and intent, but that it no longer held a significant influence on intention when trust in the vendor was high, and vice versa. The relationship between subjective norms and trust is not well understood or documented. However, existing research would suggest that subjective norms will have a positive effect on initial technology trust (Gefen, 2000; Kaushik & Rahman, 2015; Li et al., 2008). In addition, it seems logical to suggest subjective norms will have a positive effect on perceived threats to PIP if subjective norms compel individuals to trust a technology and accept its risks and uncertainty. This is likely to be applicable in the context of emerging technologies because of the role of second-hand knowledge in initial trust formation. In addition, pressures to follow social norms and hype around new technology use can pressure individuals to be "willing to be vulnerable and accept risk" regardless of whether they are comfortable with the risk. Therefore, it is hypothesised:

Hg. Greater perceived subjective norms will increase perceived threats to PIP
Hh. Greater perceived subjective norms will increase initial technology trust in emerging technologies

2.7.4. Economic Environment

McKnight et al. (1998) went to lengths to consider the contextual factors which might influence initial trust in non-emerging technologies, creating the constructs of structural assurance and situational normality as components of institutional-based trust – which influences people-related trust, interorganisational trust and technogy trust (Li et al., 2008; McKnight, Choudhury, & Kacmar, 2000; McKnight et al., 1998; Rousseau et al., 1998; Wingreen & Baglione, 2005). Yet to be considered a factor in trust research, it is proposed that an individual's economic environment, and its percieved safety, might also have a role in initial trusting situations for emerging technology. Initially, one might consider that this would fall under the domain of structural assurances. However, the economic environment of a trusting situation considers the effect of cultural and political influences on trade situations,

and the trust in the individuals involved. It also considers the general reliability and probity of a local economy or industry based on personal experience or second-hand knowledge (Sheth, 1983; J. D. Williams, Han, & Qualls, 1998).

The importance of the percieved safety of the economic environment in which a trusting situation occurs is especially applicable in trading situations because business relationships all have "elements of immediate self-interest, as well as mutuality and reciprocity" (Burchell & Wilkinson, 1997). It is also applicable to technology artefacts as an internationally valued trading commodity, of which many first-world countries can no longer live out. In their research, Burchell and Wilkinson (1997) considered the effects of a business and contractual environment on interorganisational trust. They adopted the use of "collective trust," which is the community driven capital which creates a trustworthy environment and found that the differences between collective and personal trust explained the differences in trust levels between and within different countries. In addition, their survey found that such trust in the economic environment was established through reputations of fair trading, long-term tradings relations, trade and marketing agreements, willingness to share business information and renegotiate terms, and honouring informal understandings. Culture and similarity also proved to be important, but to a lessor extent. From a more legal orientation, Pappila (2013) also found that different economic environments also had a impact on trust, considering legal liberty, democracy, political transparency, and freedom of trade and contracting. This research takes the argument that perceptions of the economic environment will indirectly influence trust through faith in humanity or vendor-based trust.

An individual's beliefs about an encomic environment will likely influence vendor-based trust in a technology trust situation. This is because different economic environments will likely influence how vendors' will behave, their intentions, priorities, willingness to cooperate and perform, and perhaps their likely success (Sheth, 1983; J. D. Williams et al., 1998). Subsequently, this will influence individuals' trust beliefs in their benevolence, integrity and competence. If we take the assumption that faith in humanity influences initial trust in emerging technology when specific vendors' are not identifiable or unknown, then it would seem reasonable to suggest the trust beliefs an individual might have in their economic environment will affect their faith in humanity, and consequently initial trust in emerging technologies.

For instance, consider a hovercraft supplied by two different vendors. One vendor is in South Africa and the other is in Canada. Both hovercrafts are identical and they both offer the same lucrative terms. Now consider where you would rather go to complete the trade. Many people would prefer Canada, even though neither country is renowned for its technology industry. This could be for a variety of reasons, which will not be explored here, but may include cultural simularity, economic robustness, effective governance, relative lack of corruption, political agendas, honesty and morality, causing greater levels of faith in humanity. Unlike structural assurance, this takes a more macro perspective of the trusting situation, is more contextual and generalisable. Structural assurance considers the specific terms, conditions and legal assurances directly related to a trusting situation which would reduce percieved risk and uncertainty of trustees (McKnight et al., 1998). This would include the terms of contract and market mechanisms which might protect an individual in the buying and selling of a good or service.

This macro-economic lense is applicable considering the impact these factors may have on trade relationships (Sheth, 1983; J. D. Williams et al., 1998), which can be likened to trust relationships. Furthermore, the evolution of emerging technologies is not a international phenomenon and varying economic and cultural values will likely be relevant in the design of emerging technologies, perhaps making the intention of some design assumptions less reliable, as well as influencing the buy and sell interactions of individuals and vendors and their beliefs in each other's benevolence, competence and integrity. As result, beliefs in the economic environment will likely affect vendor trust beliefs, or, when a specific vendor is not identifiable or unknown or well known, faith in humanity beliefs.

Unfortunantely, this thesis is unable to explore and develop a comprehensive theory for the effect of the percieved safety of an economic environment and trust. However, it hopes to test whether its general concept is relevant for trust research and potentially trigger a new area of research. Therefore, it is hyposthesised:

Hi. Greater perceived safety of the economic environment will lead to greater faith in huamnity, and vice versa

2.7.5. FAMILIARITY

Gefen (2000) defined familiarity as the understanding of current actions of people or objects while trust is the beliefs about the future actions of people or objects. It may be formed from first-hand experiences and second-hand knowledge, which is a component of generalised expectancies (Bandura, 1997; Gefen, 2000; McKnight et al., 2014; Rotter, 1971; Wingreen & Baglione, 2005). Gefen (2000) found a significant relationship between familiarity and trust, for both people and trust objects. This would suggest that greater familiarity of vendors, technologies in general or technology industries could increase initial technology trust by reducing the amount of perceived uncertainty and risk related to new technologies. This is because in initially complex, unfamiliar environments familiarity can create a set of expectations and individuals tend to rely heavily on these, to the extent that it can be a prerequisite for trust, especially when the trust object is not fully predictable (Bandura, 1997; Gefen, 2000). Accordingly, when familiarity is low, it has been found to heighten perceived uncertainty and individuals' risk-benefit judgement, decreasing calculus based trust (Satterfield, Kandlikar, Beaudrie, & Conti, 2009).

This idea of familiarity is consistent with knowledge-based trust theory. Knowledge-based trust theory states that the less knowledge individuals possess about a trust object, the greater uncertainty and risk they will perceive, therefore causing decreased levels of trust (Gefen, 2000; Lewicki et al., 2006; McKnight et al., 2011; McKnight et al., 2014; Wingreen & Baglione, 2005).

With regards to emerging technologies, Conger et al. (2013) observed individuals are generally not aware of emerging technologies and their implications. They also are not aware of their collection of personal data, its existence, movement or lifecycle once conceded from them. Therefore, it is likely individuals with low familiarity of emerging technologies will likely have lower initial technology trust beliefs than those with greater familiarity of the technology artefacts, its vendors and industries. Therefore, it is hypothesised:

Hj. Greater initial familiarity of emerging technologies will increase initial technology trust in emerging technologies, and vice versa

2.8. Hypotheses

To summarise, the following hypotheses were generated for this research and are illustrated in figure 2:

H1. Greater perceptions of physical ubiquity will decrease initial technology trust in emerging technologies, and vice versa
H2. Greater perceptions of network ubiquity will decrease initial technology trust in emerging technologies, and vice versa
H3. Greater perceptions of invisibility will decrease initial technology trust levels in emerging technologies
H4. Greater perceptions of invasiveness will decrease initial technology trust in emerging technologies, and vice versa
H5. Greater perceptions of collectability of information will decrease initial technology trust in emerging technologies, and vice versa
H6. Lower perceptions of programmability will decrease initial technology trust in emerging technologies, and vice versa
H7. Greater perceptions of wireless accessibility will decrease initial technology trust in emerging technologies, and vice versa

Ha. Greater levels of perceived threats to PIP will decrease initial technology trust in emerging technologies, and vice versa
Hb. As individuals consider technology artefacts to be more "emergent," they will perceive increased threats to PIP
Hc. Greater dispositions to technology trust will increase initial technology trust in emerging technologies, and vice versa
Hd. Greater dispositions to trust generally will increase initial technology trust in emerging technologies, and vice versa
He. When a specific vendor for an emerging technology artefact is not identifiable or unknown, greater faith in humanity will decrease perceived threats to PIP and vice versa
Hf. When a specific vendor for an emerging technology artefact is not identifiable or unknown, greater faith in humanity will increase initial technology trust in emerging technologies and vice versa
Hg. Greater perceived subjective norms will increase perceived threats to PIP, and vice versa

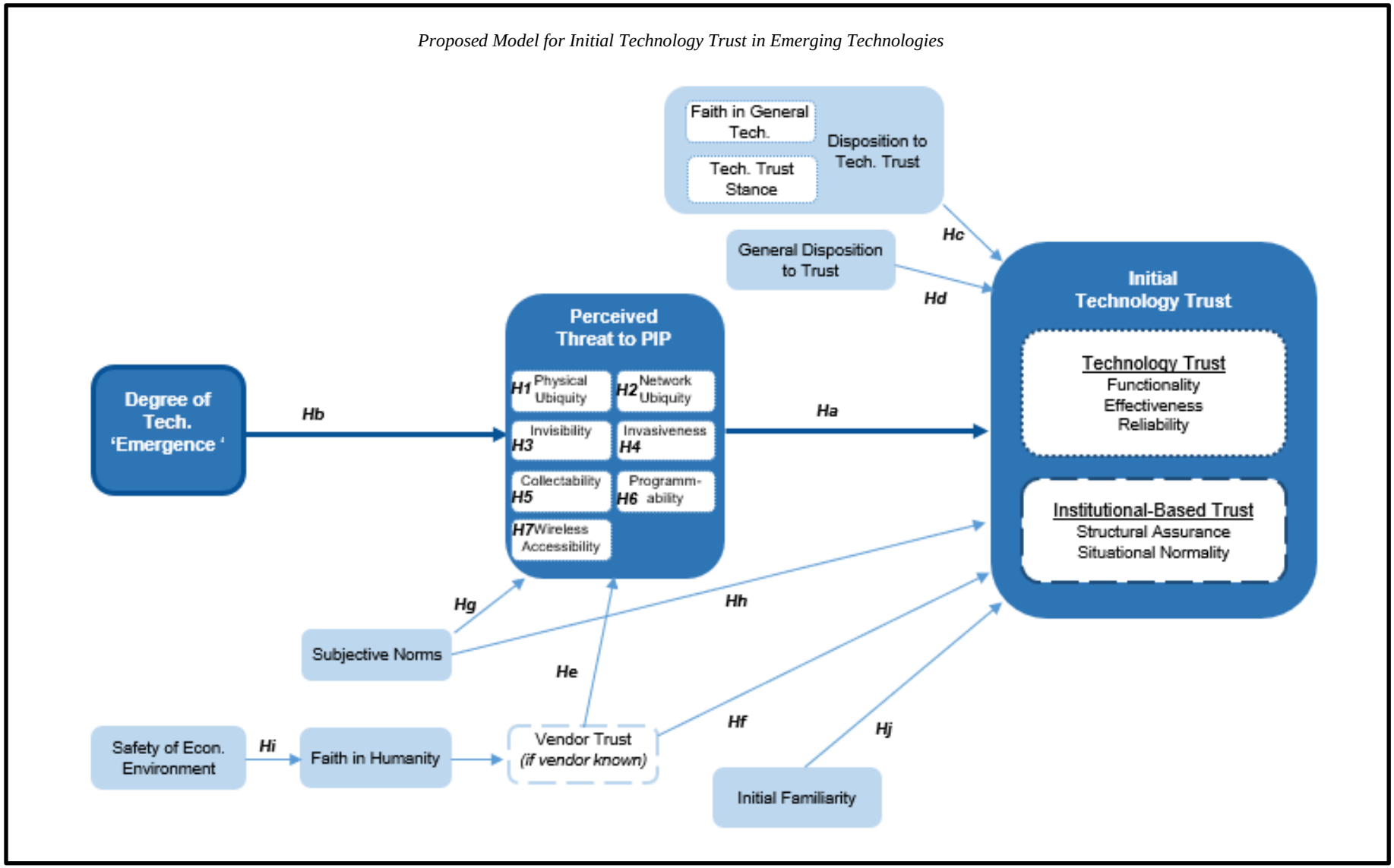
Hh. Greater perceived subjective norms will lead to greater initial technology trust in emerging technologies, and vice versa

Hi. Greater perceived safety of the economic environment will lead to greater faith in huamnity, and vice versa

Hj. Greater initial familiarity of emerging technologies will increase initial technology trust in emerging technologies, and vice versa

Figure 2

Proposed Model for Initial Technology Trust in Emerging Technologies



2.9. Summary

A literature review of technology trust has been explored and theory for initial technology trust, perceived threats to PIP and emerging technologies has been proposed, as well as general disposition to trust, institutional-based trust and vendor-based trust. In addition, hypotheses were formed based on the existing literature to develop a framework for initial technology trust for emerging technologies, as illustrated in figure 2. This framework includes threats to PIP which have, so far, been largely neglected in trust research, especially in technology trust research, despite e-commerce research pointing to its significance.

Technology trust is relatively new to the academic arena with its theoretical basis largely adapted by McKnight et al. (2011) from general trust literature. There is agreement that research in technology trust is needed and that future implications of it are invaluable. Trusting intentions of technology lead to intentions to use (H. C. Brown et al., 2004; Gefen et al., 2008; Li et al., 2008; Xin Luo et al., 2010; McKnight et al., 2011; Pavlou, 2003; Vance et al., 2008). Therefore, further research in this area may increase understanding of individual technology adoption and interaction behaviour in organisations and commerce, presenting an opportunity to develop effective ways to support potential technology users and encourage use. Given the ever increasing, radical developments in technology, research in emerging technologies can provide valuable insight in initial technology trust formation where the perceptions of risk and uncertainty are likely to be at their highest.

This review of technology trust literature suggests that the literature currently fails to connect technology trust to the PIP literature and that other forms of trust research have failed to produce a model which includes technology induced PIP threats. Threats to PIP are an increasingly common characteristic of emerging technologies and it is not clear whether mechanisms for trust operate the same for emerging technologies compared to non-emerging technologies. These PIP threats present a relevant risk which individuals must decide whether to accept when using a technology. Therefore, PIP research is relevant in considering future technology trust research.

SECTION 3. RESEARCH METHODOLOGY

3.1. Methodology Selection

The overarching purpose of this research is to determine what factors affect initial trust formation in emerging technologies. First, this research seeks to determine whether perceived threats to PIP impact initial technology trust beliefs, answering H1-H5. Psychology research appear to have utilised a various number of research methodologies, including experiments, surveys, correlational analyses, observations and interview-based investigations for people-related trust. Most Information Systems trust research has taken the form of field studies and correlational analyses, although they did not investigate emerging technologies as is defined in section 2.5. Field studies establish whether variables are related, but they do not allow inferences to be made about causation. For this reason, a controlled experiment was proposed with a control condition, randomised treatment and post-test. Secondly, this research seeks to determine what other factors influence initial technology trust beliefs, answering Ha-Hj. For this study, multi-stage modelling was used to analyse the data collected from the previous experimental setting, as recommended for exploratory theory development (Esposito Vinzi, 2010; Hair, Ringle, & Sarstedt, 2011; Ringle, Sarstedt, & Straub, 2012; Straub, Boudreau, & Gefen, 2004). The results of the experiment are significant for this research, as they determine whether threats to PIP can be included in the wider initial technology trust model for emerging technologies and provides the setting from which the initial technology trust model was later developed using multi-stage modelling with PLS-SEM.

3.1.1. PRIMARY EXPERIMENT

Experimental research is best suited for explanatory research and the examination of cause-effect relationships, making it an appropriate research design for asking what factors influence initial trust in emerging technologies (Bhattacherjee, 2012). Furthermore, experiments are especially strong in internal validity because they can discover whether changes in the dependant variables tested are in fact caused by the independent variables by controlling other external variables (Bhattacherjee, 2012; Bryman & Bell, 2011). The rigour of an experiment is relevant to this research as it will provide a strong foundation for further research by enabling this research to identify whether the characteristics embodied by emerging technologies affect perceived PIP threats and initial technology trust beliefs.

Experiments lack external validity. This means this research will be unable to confidently generalise its findings to the population. Instead, it tests whether the proposed PIP threats exist and whether they affect initial trust formation in emerging technologies which can be relied upon with a high degree of confidence. According to Mook (1983), this means that controls for external validity are not as applicable here as it would be for a field study, survey or case study. The absence of strong external validity controls does not discount any research results that are collected. Mook (1983) describes that the purpose of experiments is to discover whether something can occur under certain conditions or to contribute to understandings of a current phenomenon. This research attempts the latter by attempting to emulate processes in the real world in a controlled environment. For Mook (1983), the main concern in designing experiments is ensuring that conditions do not exist that could prevent drawing reliable conclusions as a result of artificiality or remoteness from the natural environment. After all, experiments can only offer one instance of a phenomenon while purporting to represent all possible instances. To support a more natural experimental environment in this research, treatments were designed using a series of statements from recent current news articles to describe the emerging technologies. These articles would have been readily accessible to the public should they have chosen to conduct their own investigation for second-hand knowledge to decide whether to trust the proposed emerging technology. The statements extracted represent treatments for apparent and established user benefits and risks which related to functionality, effectiveness, reliability, situational normality, structural assurances, and threats to PIP to inform subjects about the technology and impact initial trust beliefs.

A pre-test was not included in this experiment because of the limited value it would offer in terms of greater internal validity. Of concern was that a pre-test post-test design could diminish internal validity due to testing and instrumentation threats (Bhattacherjee, 2012). In this case, a pre-test could alert subjects to factors that they should be considering in evaluating emerging technologies and their trustworthiness. This could encourage a more careful and cognitive decision-making process being undertaken than that which would naturally occur.

Other research methods were considered for this research. Prior research appears to consist of theoretical frameworks, surveys and field studies. However, an advantage of this research methodology is its external reliability by combining and proposing independent variables

from prior research, many of which lack internal validity or reliability, and providing an overall element of cohesiveness regarding technology trust. The relative youth of emerging technology trust research also raises doubts as to the usefulness of a qualitative research approach, despite the personal nature of trust. Typically, qualitative research addresses research questions which are descriptive or explorative to try understand the How and Why of a phenomena (Yin, 2003). By comparison, the research question proposed in this thesis is more fundamental and basic, working with the scattered research that already exists to find an element of congruence to understand the What.

3.1.2. Multi-Stage Modelling with PLS-SEM

A larger theoretical model for initial trust in emerging technologies was hypothesized for the second part of this thesis. To test Ha to Hj, a method of multi-stage regression modelling was adopted using partial least squared structural equation modelling (PLS-SEM) techniques. PLS-SEM is a popular technique due to its ability to measure latent variables, while also testing the relationships between them, using an iterative approach to maximise explained variance of endogenous constructs (Hair, Sarstedt, Hopkins, & Kuppelwieser, 2014). There has been a push for more Information Systems and behavioural based research to utilise PLS-SEM methodologies because of its ability to capture the "bigger picture" of complex models (Lowry & Gaskin, 2014). It is also the recommended method for theory development when research is primarily exploratory and supporting theory is less developed. Thus, the research objective is not theory confirmation, but developing a model with strong predictive accuracy (Hair et al., 2011; Hair et al., 2014; Ringle et al., 2012; Wong, 2013).

PLS-SEM is particularly suitable for this research given its experimental backdrop. Experiments generally lack external validity, which means data normality cannot be guaranteed. However, PLS-SEM does not assume data is normally distributed (Hair et al., 2011; Hair et al., 2014; Ringle et al., 2012; Wong, 2013). This means, any shortcomings in the data collected through the experiment should be accounted for in the PLS-SEM procedure. This is because PLS procedures transform non-normal data in accordance with the central limit theorem (Hair et al., 2014).

Covariance based SEM (CB-SEM) is an alternative multi-stage regression SEM technique which could test Ha to Hj. However, in theory testing, it assumes samples are large, normally distributed and the model is already correctly specified (Wong, 2013). While sample size

may not be an issue here, data normality cannot be guaranteed and a correctly specified model does not already exist. CB-SEM is only suitable for confirmatory research because it largely fails in adequately meeting predictive research objectives (Hair et al., 2011). Therefore, it was not appropriate for this research. PLS-SEM also has the advantage of allowing formative measures to be incorporated into theoretical models, in addition to reflective measures, which is especially apt for research relating to intangible constructs such as trust (Hair et al., 2014).

3.2. Subjects

All the subjects for this research were students from the University of Canterbury, all of whom interact with new and varied technologies on a regular basis and would be expected to exhibit the beliefs and behaviours of interest in this thesis. The use of students as subjects are appropriate considering controlled experiments do not require a representative sample of the population (Mook, 1983). Rotter (1971) also found evidence to suggest that trust-related research involving tertiary students were similar to research using more representative, generalisable populations. This would suggest that they are a reliable source of data for trust research. The students involved in this research can also be considered as an appropriate pool of subjects on their own merits. The majority of students belong to a demographic of commonplace technology users who are familiar with a range of technologies. Students are also likely to have some understanding of emerging technologies or anticipation of potential future technologies to come. The appropriateness of students as subjects could be argued with regard to their capacities as current technology users, future consumers and the next generation of society. Finally, and very importantly, these students also represent a relatively homogeneous group of subjects which enables implicit controls for variables that might affect the outcome of dependent variables, such as age, lifestyle, income and exposure to emerging technologies.

This research received Human Ethics approval by the University of Canterbury Human Ethics Committee in July 2016. A copy of this can be found in the Appendices.

3.3. Instruments

In most cases, instruments were adopted from prior research to meet the proposed design of the experiment and subsequent testing, as organised in table 1.

Instruments from several sources were used and adapted for this research, in addition to some new instruments. Given that the theoretical framework for technology trust by McKnight et al. (2011) was adopted, it seemed preferable that the instruments for the technology trust antecedents were also adopted to increase external reliability. However, some instruments

Sources of Instruments

Dependant Variables	*Independent Variables*	*Covariates*

Initial technology trust:
• Technology-based trust:
  ○ Functionality (Vance et al., 2008)*
  ○ Reliability (Vance et al., 2008)*
  ○ Effectiveness (Vance et al., 2008)*
• Institutional trust:
  ○ Structural assurance (McKnight et al., 2011)*
  ○ Situational normality (McKnight et al., 2011)*
 	
An additional instrument for perceived PIP threats were also included.
	• PIP threats/characteristics:
	  ○ Network ubiquity*
	  ○ Physical ubiquity*
	  ○ Invasiveness*
	  ○ Invisibility*
	  ○ Collectability of information*
	  ○ Programmability*
	  ○ Wireless accessibility*
	
	• Emergence
	  ○ Innovativeness*
	  ○ Revolutionary*
	  ○ Disruptiveness*
		• General disposition to trust (Wingreen & Baglione, 2005)
		• Disposition to technology-based trust
		  ○ Faith in general technology (McKnight et al., 2011)
		  ○ Technology trust stance (McKnight et al., 2011)
		• Faith in humanity
		  ○ Benevolence (Li et al., 2008)
		  ○ Competence (Li et al., 2008)
		  ○ Integrity (Li et al., 2008)
		• Subjective norms*
		• Economic environment*
		• Familiarity (Mazey & Wingreen, 2017)

**New, original instrument(s) introduced*

were insufficient and did not address the needs of this research appropriately because of their wording and framing; adapting them for this research would require altering beyond recognition and undermine efforts to leverage instruments with known construct validity. Instead, the instruments by Vance et al. (2008) were adopted to measure the functionality and effectiveness technology trust antecedents. The measure for reliability was not adopted from Vance et al. (2008) because it only included one instrument, creating doubts about its content and construct validity. Therefore, reliability, structural assurance and situational normality were sourced from McKnight et al. (2011). Situational normality was adapted in a slightly different manner than the rest of its counterparts. Given the definition of situational normality, it did not make sense to have each item relate to the specific type of emerging technology at hand, or its relevant class of technology. By definition of an emerging technology, other similar types of technology do not exist which can be evaluated against as being normal. Hence, comparing situational normality to new technologies in general was considered most appropriate given the element of uncertainty of new technologies generally.

For the covariates, the general disposition to trust instrument was sourced from Wingreen and Baglione (2005), also used by Chen and Barnes (2007). Disposition to technology trust was sourced from McKnight et al. (2011) in the form of the technology trust stance and faith in general technology measure instruments. Measures for faith in humanity were also included on the basis that it might influence levels of technology based trust and perceived threats to PIP to some degree (see section 2.5). Instruments for faith in humanity were adapted from Li et al. (2008) and changed to refer to "vendors" rather than "others in general." The instruments from Li et al. (2008) were adopted because they separated vendor trust into three dimensions based on the three people-related trust dimensions: benevolence, integrity and competence. It was concluded that this measure was more likely to hold greater content validity than other contenders.

New instruments were introduced for the covariates of initial familiarity of technology, subjective norms, the economic environment and the PIP characteristics, which also served as a manipulation validity check since the treatment represented various PIP threats. An additional PIP related instrument was also introduced for each of the dependent variable measures to increase internal reliability as a form of manipulation validity. Appendix 2 illustrates the instruments that were used and the source from which they originated from. The covariate for initial familiarity of technology also served as a measure of manipulation validity by asking subjects to measure the extent to which they were familiar and aware of the technology that they were treated with. This is consistent with Straub et al. (2004) who require manipulation validity to be mandatory for all experiments as a means to purify data and increase internal validity. These covariates were later treated as independent latent variables in the subsequent PLS-SEM procedures, along with the perceived threat to PIP variables.

3.4. Treatments

The treatment for this research consisted of information about different emerging technologies to represent the threats to PIP they poses. Information was gathered from online news articles on the basis that the information was publicly available and readily accessible for anyone seeking to learn about the technology naturally. Therefore, it would also increase the reliability of data collected compared to self-composed technology descriptions and the artificiality this would introduce. The treatments included a general description of the technology, potential applications and risks. These statements represented treatments for

potential user benefits and risks relating to functionality, effectiveness, reliability, situational normality, structural assurances, and threats to PIP to inform subjects about the technology and impact their initial trust beliefs. Appendix 3 shows the treatments for each technology. Treatments did not include specific vendors, due to the uncontrollable variance this might cause in initial trust beliefs and risk that subjects would impute vendor trust onto technologies.

Prior to the final selection of articles, several independent individuals were asked to read and rank the excerpts in regard to its importance and give feedback regarding understandability. This eliminated some original articles and triggered adaptions to other articles for the purpose of shortening and removing jargon. A revision process of the treatments also took place after the pilot procedure based on feedback provided by subjects. The design of this treatment, utilising online articles as a source of second-hand information, seemed appropriate given that prior research suggests second-hand information is a significant factor in determining initial trust beliefs (Li et al., 2008; McKnight et al., 2011; McKnight et al., 2014; Wingreen & Baglione, 2005). It also reflects a more natural process for individuals investigating an emerging technology and would increase experiment reliability (Mook, 1983).

3.5. Pilot Experiment Procedure

Prior to the experiment, a full pilot study for five emerging technologies and a control technology was conducted. The first purpose of this was to test the emergence of the proposed technologies for the experiment and whether they were in fact perceived to be emerging technologies according to the emerging technology framework, and its three categorial tests, proposed in section 2.5.1 and the PIP threats in section 2.6.1. Thus, it sought to validate the inclusion of each technology in the experiment as well as pilot the instrumentation and identify one technology to operationalise each PIP threat. The five emerging technologies selected for the pilot procedure were 3D printing, autonomous cars, bionano sensors, bitcoin and drones. Email was the non-emerging control technology. The emerging technologies were selected because they were found to meet the requirements for an emerging technology according to the framework developed in section 2.5.1 based on a review of the current literature, media and market trends (see table 2). However, to ensure the reliability of the experiment, it was important to ensure that they were also perceived to be emerging technologies at face value. Thus, the pilot study sought to confirm manipulation validity for the coming experiment. A secondary purpose of the pilot study also existed in

Table 2

Self-Analysis of Proposed Emerging Technologies for Research and Initial Measures of Emergence and PIP Threats

	3D Printing	Advanced Robotics (Drones)	Autonomous Cars	Bio-Technologies (Bionano sensors)	Cryptocurrencies (Bitcoin)	Nano-Technologies (Bionano sensors)	Email Software (Control group)
Emerging Technology Test							
Not yet fully exploited*	✓	✓	✓	✓	✓	✓	X
Development stage of production*	✓	✓	✓	✓	X	✓	X
Early stages of commercialisation*	✓	✓	X	✓	✓	✓	X
Revolutionary	✓	✓	✓	✓	✓	✓	X
Potential to change industries**	✓	✓	✓	✓	X	✓	X
Potential to change traditional relationships**	X	✓	X	✓	✓	X	X
Potential to change institutional rules**	✓	✓	✓	✓	✓	✓	X
Emerging Technology Characteristics Which Threaten PIP							
Physical ubiquity	Low	High	High	Med	Low	Low	Low
Network ubiquity	Med	High	High	Med	High	High	High
Invisibility	Low	High	High	High	High	High	Med
Invasiveness	Low	High	High	High	Low	High	Low
Collectability of information	Med	High	High	High	High	High	Med
Programmable	Low	Med	Med	High	High	High	Low
Wireless accessibility	High	High	Med	High	NA	Med	Med

** Only one criterion need be satisfied for the "Innovative" characteristic to be met*
*** Only one criterion need be satisfied for the "Disruptive" characteristic to be met*
Emerging technology characteristics have been rated according the general characteristics of each technology group, based on an independent investigation of current reports and news items

regard to the PIP threats for each technology. By assessing the perceived PIP risks of the technologies, the pilot test was able to help refine the experiment treatments. The emerging technologies that scored the highest PIP threats were considered for inclusion in the experiment as independent variables to be manipulated.

Once subjects in the pilot study were treated, they were tested using the instruments for initial technology trust beliefs, characteristics of emerging technologies proposed in section 2.5, perceived threats to PIP based on the definitions proposed in section 2.6 followed by the proposed covariates in section 2.7. The PIP threat instruments were to also serve as a manipulation validity test for the PIP threats in the treatments and to measure the extent to which they were characteristics of interest. This sought to further internal validity, particularity construct and convergent validity. Another manipulation validity check was also included to tested whether subjects had in fact read and understood the technologies and their treatments. This asked subjects to indicate what type of information was included in the

treatment. All but one answer was correct for each of the technologies and only those who selected the incorrect answer were excluded from the data. Also included was a manipulation check where subjects were asked to declare whether they had read all the articles in the treatment. Subjects who answered "No" were removed for data analysis. After the data was cleansed it was analysed for instrument reliability and to discover which technologies were perceived to be emergent and have the greatest PIP threats. Technologies perceived to be emergent and significantly high in at least one PIP characteristic would be considered for inclusion in the experiment.

The pilot study was conducted using a 200 level Information Systems class with voluntary participation. Subjects were briefed in advance about the experiment and took approximately 10-15 minutes to complete the experiment. They were told that the research was about emerging technologies and whether they would trust them enough to use them without any mention to the role of the technology's PIP characteristics. Because of the use of multiple research groups, a Levene's test for homogeneity of variance was used to test whether variances were equal across the emerging technology groups.

3.6. Pilot Experiment Results

The pilot test had 47 participants, with 45 sets of data valid for inclusion. Inclusion was allowed if subjects passed the manipulation check by declaring whether they read the entire treatment. To test manipulation validity and whether subjects were treated appropriately, subjects were required to select what types of information were included in the treatment from a list of options to validate whether they were treated effectively. Each treatment was randomly assigned, with each technology group having 7-8 subjects for each analysis. Additionally, SPSS tests were run for unusual cases and duplicate cases. They found no results and no outliers were identified. Table 3 reports the descriptive statistics.

3.6.1. INSTRUMENT RELIABILITY

A scale reliability analysis using SPSS was conducted for each of the dependant variable and covariate scales to assess convergent validity using Cronbach's alpha, reported in table 3. Most of the results, as follows, had a Cronbach's alpha between 0.74 and 0.95 and had sufficient significant consistency among variable items. The exception to this was the covariates for technology trust stance and the benevolence limb of faith in humanity with the

Table 3

Descriptive Statistics and Cronbach's Alpha for Dependant Variables & Covariates

	Functionality	Reliability	Effectiveness	Structural Assurance	Situational Normality	Faith in General Technology	Technology Trust Stance	Faith in Humanity (Benevolence)	Faith in Humanity (Competence)	Faith in Humanity (Integrity)	Subjective Norms	Economic Environment	Disposition to Trust	Familiarity
Descriptive Statistics														
N	43	42	42	43	44	37	42	43	43	42	46	47	43	47
Mean	4.92	3.46	3.57	3.88	4.16	4.75	4.78	4.39	4.80	4.29	3.02	2.91	4.27	3.51
Std. Deviation	0.97	0.94	1.48	1.15	1.05	0.82	0.92	0.94	1.00	1.12	1.20	1.23	1.21	1.68
Cronbach's Alpha														
No. Items	5	5	4	4	5	4	3	3	3	3	1	1	4	1
Cronbach's Alpha	0.84	0.74	0.90	0.83	0.81	0.77	0.63	0.47	0.94	0.91	1.00	1.00	0.94	1.00

Cronbach's alphas of 0.63 and 0.47 respectively. These results were inconsistent with the related variables of the constructs from which they belonged and the Cronbach's alphas their authors reported. Technology trust stance was adopted from McKnight et al. (2011), along with faith in general technology as a construct of disposition to technology trust, which had reported a Cronbach's alpha of 0.86. The benevolence antecedence of faith in humanity was adopted from Li et al. (2008) who had reported a Cronbach's alpha of 0.87. This measure was adopted in addition to scales for faith in humanity's competence and integrity antecedents which had both reported a strong significant convergent reliability as below with Cronbach's alpha both greater than 0.90.

Technology trust stance and faith in humanity's benevolence were part of larger constructs and had initially reported significant Cronbach's alpha in prior research (Li et al., 2008; McKnight et al., 2011). As such, it was decided they would remain in the experiment as they were judged to be adequate for the purposes of the pilot test since the small data sample may have contributed to this result, therefore it was anticipated higher Cronbach's alphas would be reported consistent with Li et al. (2008) and McKnight et al. (2011). Furthermore, significantly adapting technology trust stance or faith in humanity's benevolence, or developing new items to replace the pilot items, could threaten the internal consistency of the disposition to technology trust and faith in humanity variables between their respective constructs.

3.6.2. Perceived Emergence of Technologies

Using a means comparison, the pilot data confirmed that each of the emerging technologies proposed for the experiment were perceived to be emerging technologies, whereas email was not. Insufficient group numbers existed for a reliable MANOVA to test the emerging technologies against the control group, email. Instead, if emergence items deviated by 1.00 or more from 4.00, which was "neutral," with a $p < 0.05$ this was considered to be sufficient to pass or fail each technology for the purposes the pilot study. To have passed the criteria to be perceived as an emerging technology each technology had to satisfy three categorical tests for innovativeness, revolutionary and disruptiveness. This follows the framework proposed in section 2.6.1. The pilot test confirmed the assumption that the proposed technologies were perceived to be "emerging," as well as in fact, thus validating their possible inclusion in the experiment. In addition, it also validated the use of email as a control treatment for the technologies in regard to their emergence. Table 4 illustrates the mean scores for each emerging technology group.

Based on these results, 3D printing, autonomous cars and bionano sensors satisfied the requirements to be perceived as "emergent." Bitcoin failed based on the perception it was not

Table 4

Emergence Test for Proposed Research Technologies

Characteristics	3D printing	Autonomous cars	Bitcoin	Bionano sensors	Drones	Email
1. Innovativeness						
a. Not yet fully exploited	**6.13**	**5.50**	**5.00**	**5.86**	**5.81**	3.14
b. Developmental stage of production	**5.00**	**6.30**	**5.88**	**6.00**	**5.00**	**3.00**
c. Early stages of commercialisation	**6.00**	**5.63**	**6.25**	**5.43**	**5.71**	4.29
	Pass	Pass	Pass	Pass	Pass	Pass
2. Revolutionary						
a. Revolutionary	**5.50**	**5.75**	4.75	**5.29**	4.57	4.57
	Pass	Pass	Fail	Pass	Fail	Fail
3. Disruptive						
a. Changes a wide range of industries	**5.88**	**5.75**	**5.38**	**5.70**	**5.00**	**5.29**
b. Changes traditional relationships	4.13	**6.00**	**5.38**	4.57	4.43	4.57
c. Changes laws and regulations	**6.13**	**6.13**	**5.88**	4.67	**6.86**	**5.29**
	Pass	Pass	Pass	Pass	Pass	Pass
Emerging Technology?	**PASS**	**PASS**	**FAIL**	**PASS**	**FAIL**	**FAIL**

Note 1. Scale: 1 = Strongly Disagree, 3 = Disagree, 4 = Neutral, 5 = Agree, 7 = Strongly Agree
Note 2. Characteristics with more than one attribute must have at least one criteria satisfied for the characteristic to be met and awarded a "pass"
Note 3. A criterion is satisfied when it deviates by 1.00 or more from 4.00 (Neutral) with $p < 0.05$

revolutionary in nature. Drones also did not pass this requirement, which was surprising, but

it was judged that this was likely to change with more data. This low score may also be attributable to the pilot study group itself: a 200 level Information Systems course studying technology design and development. However, because drones also included characteristics which were valuable for this research it was retained for inclusion in the experiment.

3.6.3. Personal Information Privacy Threats

An exploratory factor analysis of the PIP characteristics, using varimax rotation, suggested that the PIP characteristics adopted by Conger et al. (2013) demonstrated a three-dimension factor pattern, which was neither theorised or predicted by Conger et al. (2013). Using Hair, Tatham, Anderson, and Black (1998)'s rule of thumb, each PIP threat yielded a significant factor loading as illustrated to in table 5.

Table 5

Factor Loadings PIP Threats

	Factor 1 (Omnipotence)	Factor 2 (Intrusiveness)	Factor 3 (Invisibility)
Network ubiquity	**0.82**	0.25	-0.27
Physical ubiquity	**0.82**	-0.12	0.06
Invisibility	0.15	0.08	**0.90**
Invasiveness	-0.24	**0.56**	**0.60**
Collectability	-0.23	**0.87**	0.18
Programmability	**0.85**	-0.18	0.24
Wireless accessibility	0.18	**0.88**	0.02
Eigenvalue	*2.42*	*2.02*	*1.08*
% of Variance	*35%*	*29%*	*15%*

**Factor loadings 0.55 and above bolded as significant, as per Hair et al. (1998)*

Based on Conger et al. (2013), it is proposed that this set of characteristics can be simplified into three categories; omnipotence (factor 1), intrusiveness (factor 2) and invisibility (factor 3). Omnipotence is the combined threat from the physical ubiquity, network ubiquity and programmability of a technology. The ubiquitous nature of a technology suggests that users will be unable to fully control its operations, its relationships with potentially untrusted entities, and its sharing of information. This implies that an "omnipotent" technology will leave little freedom in its programmability regarding its functionality, effectiveness and its decisions about sharing information and networking. "Intrusiveness" is the threat of a technology's invasiveness, its ability to collect information and wireless accessibility. A technology's ability to penetrate deeply into the private lives of individuals presents little threat unless it can also collect that information and remove it from the control of the

individual. This threat is exacerbated as the connectivity of a technology to the internet and other systems and entities increase. Lastly, invisibility appears to remain a category largely on its own, although invasiveness cross-loaded to a lesser extent. This suggests that the threat of invisibility is worsened by the extent to which an emerging technology is invasive and can penetrate deeply into individual's private life. Given the significantly greater factor loading for invisibility compared to invasiveness for factor 3 and less variance among variables in factor 2, it is likely that invasiveness will load more strongly with factor 2, intrusiveness, once more data is collected. This is because the threat of invasiveness to PIP appears to be more complementary to an emerging technology's ability to collect information and wireless accessibility compared to invisibility.

A recent paper by Pycroft et al. (2016b) raised awareness of the security and privacy threats to emerging medical technologies, with particular regard to advancing bioneural technologies. This paper can be used to demonstrate the characteristics of omnipotence, intrusiveness and invisibility of an emerging technology. Pycroft et al. (2016b) illustrated the serious harms that could be inflicted on individuals from privacy and security breaches of medical technologies. Devices could be used to passively invade privacy by "listening" and recording many types of information or, more aggressively, be used for the dual purpose of providing medical aid and actively collecting other unrelated information. Both of these privacy breaches could be used to fuel further attacks using the individual's personal information. While security concerns are beyond the scope of this research, knowledge of such privacy risks borne by emerging technologies could be expected to reduce technology-based trust by potential users.

An analysis of means, based on the factor analysis, was conducted and compared for each technology in table 6. Interesting to note was the differences between some technologies compared to the rest of the group. 3D printing suggested results for perceived threats to PIP were inconsistent with other technologies. It scored the highest score for invisibility and omnipotence, including the non-emerging technology email, and pointedly lower intrusiveness than the other emerging technologies. The variation of perceived threats to PIP between emerging technologies was not expected. In some cases, there is greater variation between emerging technologies than the emerging technology and non-emerging technology.

Table 6

3.6.4. NEW HYPOTHESES

Mean Scores for Perceived Threats to PIP Factors

	3D printing	Autonomous cars	Bitcoin	Bionano sensors	Drones	Email
Omnipotence	5.25	4.83	4.00	4.24	2.48	4.91
Intrusiveness	4.63	5.69	5.45	5.29	5.43	6.14
Invisibility	5.25	4.75	4.38	5.14	5.14	5.14

Scale: 1 = Strongly Disagree, 3 = Disagree, 4 = Neutral, 5 = Agree, 7 = Strongly Agree

Based on the unexpected pilot study results regarding threats to PIP which were neither theorised or predicted by Conger et al. (2013), new hypotheses were generated for this research. Since the data revealed three categories of PIP threats, consisting of Conger et al. (2013)'s original seven theorised categories, the hypotheses were aggregated accordingly. The new hypotheses are as follows:

H1. A technology's degree of invasiveness, ability to collect information and wireless accessibility *relate to its level of "intrusiveness" which presents a threat to PIP*

H2. A technology's degree of physical ubiquity, network ubiquity and programmability *relate to its level of "omnipotence" which presents a threat to PIP*

H3. Greater perceived intrusiveness will decrease initial technology trust in emerging technologies, and vice versa

- *H3a. Greater perceived intrusiveness will decrease perceived functionality in emerging technologies, and vice versa*
- *H3b. Greater perceived intrusiveness will decrease perceived effectiveness in emerging technologies, and vice versa*
- *H3c. Greater perceived intrusiveness will decrease perceived reliability in emerging technologies, and vice versa*
- *H3d. Greater perceived intrusiveness will decrease perceived structural assurance in emerging technologies, and vice versa*
- *H3e. Greater perceived intrusiveness will decrease perceived situational normality in emerging technologies, and vice versa*

H4. Greater perceived omnipotence will decrease initial technology trust in emerging technologies, and vice versa

- *H4a. Greater perceived omnipotence will decrease perceived functionality in emerging technologies, and vice versa*
- *H4b. Greater perceived omnipotence will decrease perceived effectiveness in emerging technologies, and vice versa*

H4c. Greater perceived omnipotence will decrease perceived reliability in emerging technologies, and vice versa

H4d. Greater perceived omnipotence will decrease perceived structural assurance in emerging technologies, and vice versa

H4e. Greater perceived omnipotence will decrease perceived situational normality in emerging technologies, and vice versa

H5. Greater perceived invisibility will decrease initial technology trust in emerging technologies, and vice versa

H5a. Greater perceived invisibility will decrease perceived functionality in emerging technologies, and vice versa

H5b. Greater perceived invisibility will decrease perceived effectiveness in emerging technologies, and vice versa

H5c. Greater perceived invisibility will decrease perceived reliability in emerging technologies, and vice versa

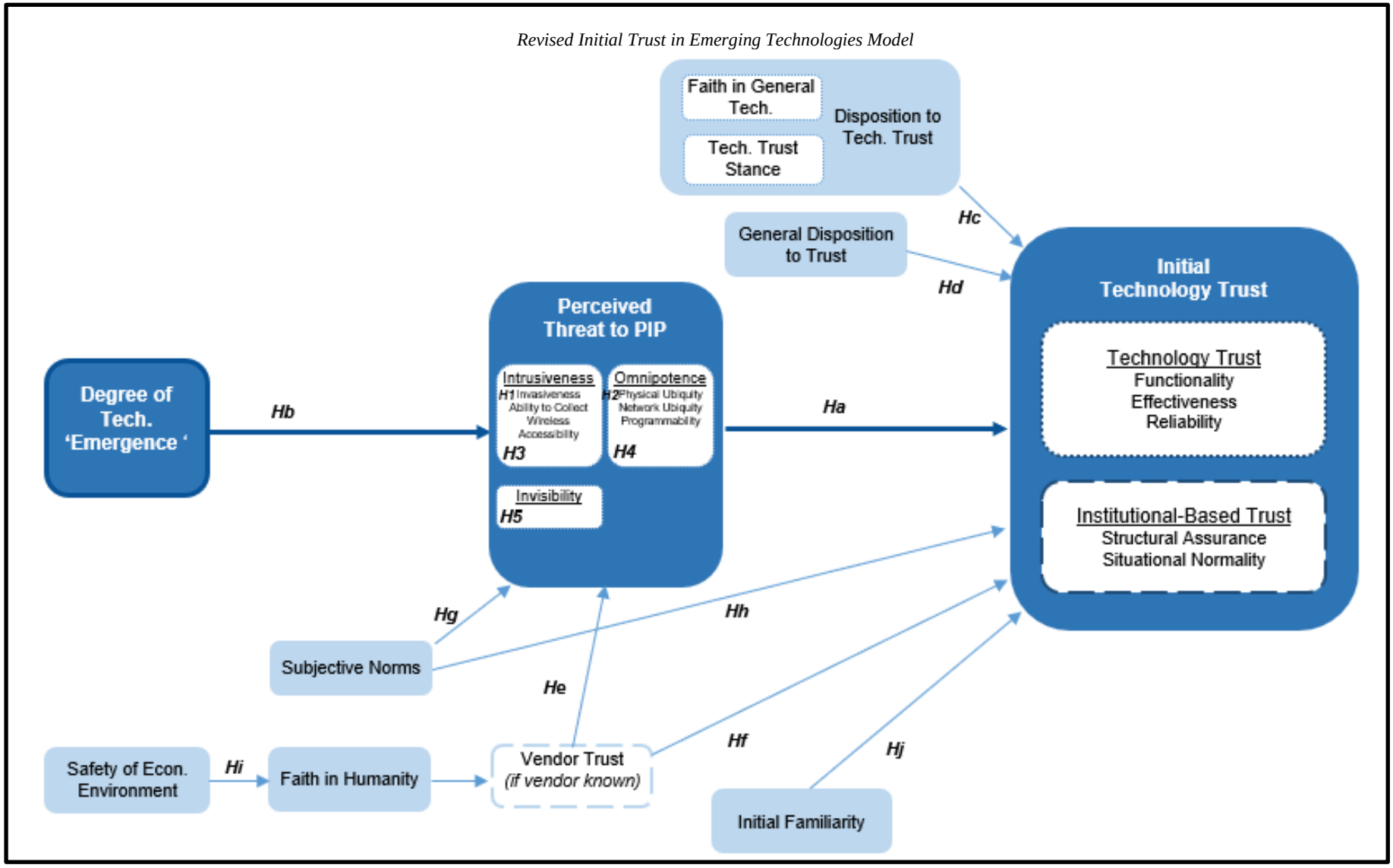
H5d. Greater perceived invisibility will decrease perceived structural assurance in emerging technologies, and vice versa

H5e. Greater perceived invisibility will decrease perceived situational normality in emerging technologies, and vice versa

Figure 4 illustrates the revised model hypothesised for initial emerging technology trust.

Figure 3

Revised Initial Trust in Emerging Technologies Model



3.6.5. POST-PILOT REVISIONS

It was decided no major changes were necessary for any dependent trust variable instruments and that all the covariates would remain, given that concerns about time and attention lapse did not appear to be as much of threat to the study as predicted based on feedback from the pilot study. However, treatments were shortened where possible to ensure this threat was mitigated.

Treatments were revised to better emphasise a PIP threat dimension according to the PIP threat profile of best fit, based on the exploratory factor analysis reported in table 5. The purpose of this was to more effectively target treatments and test dependant variables, and promote manipulation validity. The exception to revision was the use of email as the control variable for emergence and 3D printing. 3D printing produced results that suggest it was not perceived as consistently as a PIP threat compared to the other technologies. Thus, it was decided that 3D printing would not be used to operationalise a primary PIP threat dimension. Instead, it would remain largely unchanged so that it might be used as control condition that could be used against the other emerging technologies. The 3D printing treatment therefore established control conditions for both emergent vs non-emergent technologies and low PIP threats vs high PIP threats.

Based on the means analysis of the PIP factors, bionano sensors were selected to operationalise omnipotence (Factor 1: network ubiquity, physical ubiquity and programmability), autonomous cars were selected to operationalise intrusiveness (Factor 2: collectability of information and wireless accessibility) and drones were selected to operationalise invisibility (Factor 3). Consequently, their treatments were adapted to emphasise these qualities as necessary.

Some test revisions were made based on feedback from test subjects once they finished the pilot test. The main areas of concern related to the construction of the Likert scale and the structure of the questionnaire. In regard to the Likert scale, some individuals found that going from 1 (Strongly Agree) to 7 (Strongly Disagree) was not intuitive and would have preferred it if it went the other way. While other individuals found no problem in this, those who did thought it was a necessary change for the experiment and it was reversed as requested. Two individuals commented that they felt the questionnaires was a bit too long. This feedback was anticipated, however, the large majority of participants did not have this issue which suggests

the threat of unsystematic variance is weak. Test subjects suggested randomising the covariate and dependant variables sections would overcome lack of attention problems. This was also actioned as requested.

Further review of the pilot study also resulted in the reorganisation of the treatment and questionnaire order. This had the effect of moving the covariate section, as the last section, before the treatment. The reason for this was twofold. It was anticipated that this would help reduce any attention span difficulties individuals might have by further dividing and separating the questionnaire into parts. The second reason was to ensure that the treatment would not have any effect on individuals' responses to the covariates. While this was not theorised or anticipated to be of concern, it was decided that this would increase the reliability of data collected and was therefore a worthwhile cause.

3.7. Primary Experiment Procedure

As with the pilot test, the experiment design was a randomised treatment with a control condition and post-test and included the same manipulation checks. Subjects were given information about four emerging technology treatments used in the pilot study; 3D printing, autonomous cars, bionano sensors and surveillance drones. The treatments used the same information as the pilot study, but were revised to better emphasise the PIP threats identified in the pilot study factor analysis. Email was kept as the control variable for emergence and 3D printing was used a control variable for perceived PIP threats after initial results suggested that it supported all three PIP threat dimensions in opposition to the other emerging technologies.

Each treatment was intended to operationalise one PIP threat as an independent variable to increase reliability of the results and prevent data from being tainted by the interaction effect of multiple independent variables. However, the results of the experiment indicated that each technology held varying levels of PIP threats and one PIP threat could not be used to be uniquely operationalised by only one technology. Therefore, procedures to test the hypotheses H3 – H5 were based on (a) significant differences in perceived PIP between each emerging technology and the control group and (b) significant differences in perceived PIP between two emerging technologies.

The experiment study was performed on a 100 level core Commerce class with 312 subjects who participated voluntarily. Subjects were instructed in advance of the experiment and took approximately 10 minutes to complete the experiment. They were instructed that the research was about emerging technologies and whether they would trust them enough to use them, without any mention to the role of the technology's PIP characteristics. Following the initial introduction, subjects were required to complete the covariate instruments before reading the treatment. They were then tested for manipulation validity before answering the dependant variable instruments, the emergence instruments and, lastly, the threat to PIP instruments. The covariate and dependant variable instrument items were randomised, as discussed in section 3.6.5.

To maintain internal validity, a manipulation check was used for treatment validity. Like the pilot study, this took the form of a Boolean instrument testing whether subjects had read all the article extracts in the treatment. Those who had not, were not included in the research data. A manipulation validity check tested whether subjects had read and understood the article extracts by indicating what types of information was included in the treatment. Since it appeared some subjects had difficulty understanding the question and selected one answer of best fit rather than all applicable answers, therefore only two out of three options had to be correct. It was decided these rules did not need to apply to email since it could be assumed that subjects were already very familiar with email, how it works and its PIP threats, both from personal experience and second-hand knowledge. The number of subjects that declared they had not read the entire treatment for email was not large and the covariate measuring previous understanding of the technology suggested they were already very familiar with the applications, risks and benefits of email. The fact they had not read all of the treatment posed a low risk to the research given that second-hand knowledge has been shown to have a decreasing effect on trust as personal experience increases (Li et al., 2008). After removing incomplete or invalid data, and accounting for those which failed the manipulation checks, a total of 293 records remained with n = 57, 60, 57, 57 and 62 subjects in the 3D printing, autonomous cars, bionano sensors, drones and email experiment groups respectively.

To test convergent validity and whether the independent variables were related to one another in regard to initial technology trust, an exploratory factor analysis was performed on the PIP threat variables. In addition, a scale reliability analysis was taken for each dependent variable and covariate. A MANOVA with pairwise t-tests was used to examine the differences

between treatments of each technology group and a Levene's test was conducted to assess whether the test groups have significantly different population variances. The pilot procedure demonstrated that it would be very difficult to find an emerging technology that could be used to represent only one type of PIP threat. Therefore, to determine whether hypotheses H3 to H5 could be supported a significant mean difference was required to have occurred between (a) the perceived PIP threat between each emerging technology and the control group and (b) the perceived PIP threat between two emerging technologies. R^2 measures were also used to evaluate the variance in the dependant variables caused by the independent variables and covariates.

A significance level of 0.05 was used for all the experimental procedures to promote strong internal validity and reliability of the procedures to confirm whether the proposed casual and covariate relationships with initial technology trust exist with a strong level of confidence.

3.8. Multi-Stage Modelling with PLS-SEM Procedures

Following the analysis of the experimental data, the initial technology trust model for emerging technologies was analysed using 228 cases from the primary experiment. This included the data groups for emerging technologies: 3D printing, autonomous cars, bionano sensors and drones. Since the factor analysis from the pilot experiment suggested differences between emerging and non-emerging initial trust formation, the model was also tested using 62 cases from the experiment's control group for non-emerging technologies, email, to compare for any significant differences in results as evidence of any interaction effect. This subsequent analysis was not originally intended and was selected following the outcomes of the primary experiment.

The primary experiment had a very particular, focussed research aim to establish whether relationships existed with a strong degree of confidence. This secondary study, using multi-stage modelling, has more exploratory intentions to understand whether the casual relationships tested between the perceived PIP threats of emerging technologies and initial technology were indeed predictive, and whether any of the covariate variables also had a predictive relationship on perceived threats to PIP or initial technology trust. Therefore, it is necessary to highlight the change in significance levels from 0.05 in the experiment procedures to 0.10 for exploratory multi-stage modelling as recommended by Garson (2016).

PLS-SEM procedures were performed using SmartPLS 3. The complexity of the initial technology trust model for emerging technologies meant the model contained third and second order latent variables. Generally, academic PLS-SEM models are modelled as first or second order models. To account for the third order latent variables in this research, the model for initial technology trust was prepared in three stages using SmartPLS 3, consistent with methods to analyse second-order PLS-SEM models and in accordance with Lowry and Gaskin (2014). Where appropriate, bootstrapping procedures were applied using 500 subsamples alongside bias-corrected and accelerated confidence interval method procedures and two tailed tests with a significance level of 0.10 for exploratory research using PLS-SEM, as recommended by Garson (2016). Bootstrapping procedures also used a path weighting scheme of 300 maximum iterations and a stop criterion of 10^7. The change

The third order variables were analysed first. Third order variables included functionality, reliability and effectiveness, as antecedents to technology trust (a component of initial technology trust), and structural assurance and situational normality, as antecedents to institutional-based trust (the second component of initial technology trust). Both antecedents were measured independent of the initial trust model. The measures for each variable were measured as reflective indicators. The variables, as antecedents for technology trust and institutional-based trust, were also modelled as reflective items, as per Lowry and Gaskin (2014) and is illustrated in Appendix 5.1. Using the SmartPLS 3 PLS-SEM algorithm, the results were used to evaluate the respective outer item loadings of the variables to evaluate outer model reliability. The latent variable scores generated were then taken for technology trust and institutional-based trust as latent variable data for the second order model.

In the next stage of preparing the PLS-SEM data, the second and first order variables were modelled according to the initial technology trust model for emerging technologies, with all variables in the initial trust model proposed now included (illustrated in Appendix 5.2). All second order variables were measured as reflective measures, except for perceived threats to PIP which measured intrusiveness, omnipotence and invisibility as formative constructs. Measurement items were loaded onto their respective constructs and both variable and latent variable scores were generated for all variables, including second order variables. The data generated at this stage was also used to evaluate outer model reliability by using the outer item loadings or weights for each of the variables. Latent variable scores were then taken for the second order variables (emerging technology artefact, technology trust, institutional-

based trust, perceived threats to PIP and faith in humanity) as latent variable data for the first order model.

The first order was analysed last using the latent variable scores of all the variables generated from the second stage of processing, including any first order variables (illustrated in Appendix 5.3). This was necessary to measure the inner model reliably and determine the R^2 values, path coefficients, f^2 values and inner VIF factors of the initial technology trust model (Lowry & Gaskin, 2014) .

The initial technology trust model was evaluated according to outer model reliability, inner model reliability and measurement of fit (Garson, 2016; Hair et al., 2014). The primary objective of using PLS-SEM in this research was to determine the overall predictive validity of the of model proposed for initial technology trust in emerging technologies. This can be gauged by R^2 values, path coefficients, f^2 values and inner VIF factors (Garson, 2016; Hair et al., 2011; Hair et al., 2014; Ringle et al., 2012; Wong, 2013). Where insignificant f^2 values were reported, additional post hoc, two tailed fixed model linear multiple regression power analyses using G*Power software were performed to test for type II error (Chin, 1998; Cohen, 1988; Faul, Erdfelder, & Lang, 2009; Faul, Erdfelder, Lang, & Buchner, 2007).

The primary experiment already validated the use and inclusion of all the variables and measurement items. It has been noted that efforts to evaluate the outer model for PLS-SEM models which contain second and third order latent variables become less reliable and measures less effective compared to first order models (Chin, Marcolin, & Newsted, 2012; Lowry & Gaskin, 2014). Thus, measuring and reporting outer model results here only seek to reaffirm the results of the experiment regarding the validity and reliability of constructs and their items. It also provides greater transparency and completeness.

Measurement of fit was determined by taking a holistic evaluation of outer model and inner model reliability and multicollinearity. The significance of the path coefficients and R^2 results were considered the most principal factor when evaluating measurement of fit (Chin, 1998; Chin et al., 2012; Garson, 2016; Ringle et al., 2012). If these were unreliable, the model's measurement of fit was not assumed because of the impact they may have on inner model reliability. If these results were significant, then the f^2 values, inner and outer VIF factors and

outer item loadings and weights were taken into consideration and weighed up (Chin, 1998; Garson, 2016).

3.9. Missing Data

A printing error occurred during this research. The effect of this was that some experiment questionnaires included duplicate items, and thereby excluded other items. This occurred in the autonomous cars and bionano groups resulting in a loss of 5.7% of total data collected across all the groups, including missing data due to non-response. More specifically, 8.4% of total covariate data and 2.9% of total dependant variable data was missing. Fortunately, the missing items only effected one scale item of each of the affected variables.

To address the problem of missing data an available item means imputation method was used. This was applied on a case by case basis by taking the mean score of existing items of a scale for each person and imputing the mean score into the missing item (e.g. scale 1 is measured by itemA, itemB and itemC and personX is missing itemA. The mean of itemB and itemC was taken to impute into the value missing itemA) (Enders, 2003, 2010; Graham, 2009; Little, 2013; Mazza, Enders, & Ruehlman, 2015; Parent, 2013).

Because of the design of this research and the multiple experiment groups involved, an available item means imputation method was best suited to overcome the problem of missing data. This is commonly used in similar psychology research involving scales measured by multiple items (Enders, 2010; Graham, 2009; Little, 2013; Mazza et al., 2015). It is also widely accepted that this method does not bias or otherwise affect the results of multivariate statistical procedures (Enders, 2010; Little, 2013; Mazza et al., 2015; Parent, 2013).

The purpose of using multiple items to measure one variable is used to increase construct validity and ensure that a reliable measure of a variable is obtained. Theoretically, this would mean that each item for a variable would receive the same value from each person and that the removal of one item would mean the same as removing another item of the same variable. This is an important assumption for the available item mean imputation method (Graham, 2009). Examination of the affected variables supported the belief that sufficient convergent validity existed with subjects providing the same or similar scores for related items. Given this, such a means imputation should introduce little bias to the data, if any, and pose a low risk to its reliability and validity (Parent, 2013). It was also particularly appropriate given the

multiple experimental groups involved in this research. Typical mean imputation methods take the mean of all cases for an item, not its scale-related items, to impute into missing values. An evaluation of the primary data, as well as the pilot data, suggested that variables were likely to differ based on the technology treatment administered, making a mean imputation for an item based on its existing values inappropriate. Imputing a mean based on technology groups was an option to address the missing data, but given that the missing data mostly affected two groups this did not seem a viable option and threatened the reliability of data when compared to available item mean imputation.

According to research by Parent (2013), available item mean imputation is more reliable than other imputation techniques, and is ideal for the type of research design used here. He found this method overcomes the problems of the traditional methods of imputation (e.g. mean substitution, case-wise deletion) as well as the newer, more complex methods (e.g. multiple imputation). Initial examination of the data supported the belief that this method was most likely to retain data integrity. To ensure the appropriate use of this method, the existing literature identified certain rules and guidelines which should be satisfied to ensure the acceptable use of imputed missing data for research purposes, e.g. percentage of missing data allowed. This research complies with all those rules, recommendations and assumptions identified by Enders (2010), Graham (2009), Little (2013) and Parent (2013). Of particular note, a high proportion of available items was available for the effected scales, and hence it was decided each scale was only allowed to have one missing item for imputation. This was greater than the recommendations that more than half the items should be available. Moreover, initial construct validity of variables was determined to have already existed, thereby further minimising the threat to statistical conclusion validity.

3.10. Validity

In compliance with Straub et al. (2004)'s validation guidelines for Information Systems positivist research, the following procedures for manipulation validity, construct validity, reliability and statistical conclusion validity were performed to clearly identify and reiterate the measures incorporated in this research to protect its validity. In addition to those procedures required by Straub et al. (2004), procedures for internal validity and predictive validity were also included and described in the following sections.

3.10.1. Manipulation Validity

Three measures were included to specifically ensure manipulation validity and whether the treatments had their intended effect on subjects (Straub et al., 2004). These took the form of two Boolean instruments and the PIP threat instrument items, as recommended by Straub et al. (2004). The Booleans were tested directly after subjects were treated with their respective emerging technology artefact.

The first Boolean asked subjects to indicate whether they had read the entire treatment provided. The second Boolean tested subjects about what information the treatment had included. Three options were available for selection, with only one answer incorrect. Any subjects who selected the incorrect answer were removed from the analysis on the grounds of insufficient manipulation. This meant that subjects had to get a minimum pass rate of 67% for the three Booleans. Thirdly, the inclusion of the single PIP threat instruments items was intended to measure and confirm whether the operationalisation of the PIP factors (intrusiveness, omnipotence and invisibility) had effectively treated subjects and, if so, to what extent. Such confirmation would help to determine whether it was fair to conclude the independent variables were responsible for the variance in initial technology trust levels across groups.

Additionally, the pilot procedure was used to validate the assumption that the selection of technologies were in fact perceived to be emerging. This provided further manipulation validity for the experimental procedure.

3.10.2. Construct Validity (Convergent & Discriminant Validity)

To ensure construct validity, all of the dependant trust variables were adapted from previously validated research which also demonstrated high construct validity using Cronbach's alpha, as advised by Straub et al. (2004). This applied to most of the covariates as well. To overcome potential threats to construct validity by introducing new covariate and PIP threat variables, items were developed as close to the definitions and conceptualisations in the literature as possible. Factor analyses and a two-tailed Pearson's bivariate correlations with significant levels of 0.05 were also performed to confirm sufficient convergence and divergence in the experimental procedures. The use of item randomisation also reduces common method bias, which is a threat to discriminant and convergent validity, as well as reliability (Straub et al., 2004).

Furthermore, in accordance with PLS-SEM recommendations, indicators loadings and an examination of item cross loading were used to evaluate construct validity of the proposed initial technology trust model (Hair et al., 2011; Hair et al., 2014; Straub et al., 2004).

3.10.3. Reliability

Straub et al. (2004) stated that the reliability of between-subjects and between-items should be determined using Cronbach's alpha, in addition to using multiple items for construct validity. This was achieved through the post-testing of convergent validity of variables using Cronbach's alpha. To ensure reliability of internal consistency, items were randomised and separated from their other related variable items to prevent potential unsystematic variance from entering the data.

In addition to Cronbach's alpha to test instrument reliability, PLS-SEM best practise recommends composite reliability testing be carried out to complement Cronbach's alpha (Hair et al., 2014). Therefore, it was tested as well. The use of the experimental setting from which the data was sourced offers additional confidence in the internal reliability of this second study's results. The experiment procedures allowed secondary variables theorised to affect initial technology trust to be tested as covariates before testing their relationship in the initial technology trust model proposed using PLS-SEM. This provides additional support for the internal reliability of the final proposed model. It also provided an opportunity to revise the model before the second study using PLS-SEM to test its predicative validity, if needed.

3.10.5. Statistical Conclusion Validity

SPSS was used to perform all descriptive statistics, factor analyses, MANOVAs, MANCOVAs and other statistical procedures used in the data analysis for the first part of this research, the experiment. The experiment tested whether perceived threats to PIP have a significant effect on initial technology trust in emerging technologies and subsequently include it in the initial technology trust model proposed. SPSS is widely used and trusted as a reliable software to perform accurate statistics analyses compared to alternative methods of calculating and running the required statistics. A significance level of 0.05 was adopted for all statistical analyses relating to the experiment tested in SPSS to reduce the probability of type I errors. It was also necessary that an appropriate, large subject pool was used to gather

sufficient amounts of data to perform MANOVA procedures from, which could be used to produce reliable results and reduce the risk of type II errors.

For the second part of this research, PLS-SEM procedures were implemented using the SmartPLS 3 software. SmartPLS is one of the most popular choices for researchers using PLS-SEM procedures, especially in the fields of Information Systems and Marketing due to its natural ability to overcomes the challenges in social science research (Hair et al., 2014; Ringle et al., 2012; Wong, 2013). Where appropriate, bootstrapping procedures were applied using 500 subsamples, a path weighting scheme of 300 maximum iterations and a stop criterion of 10^7. Bias-corrected and accelerated confidence interval method procedures and two tailed tests with a significance level of 0.10 for exploratory research using PLS-SEM were also used, as recommended by Garson (2016). Where significant f^2 values for effect size could not be found, G*Power software was used to perform post hoc power analyses to test for potential type II errors (Chin, 1998; Cohen, 1988; Faul et al., 2009; Faul et al., 2007; Miguel & Mikko, 2015; Peng & Lai, 2012).

3.10.6. Internal Validity

To protect internal validity and mitigate the threat of students informing each other of the contents of the experiment between session times, a question was included in the experiment asking whether students had discussed the contents of the instrumentation or treatments with anyone prior to participating. They were also instructed not to discuss the research with any classmates until the end of the week. To further ensure internal validity, Levene's tests of homogeneity of variance were performed to test for the equal group variance required for multiple group experiments and treatments were randomised to prevent group selection bias. In addition, a pre-test was not included in case it alerted subjects to factors they should consider when responding to the questionnaire, introducing artificiality in the experimental environment and reducing internal validity (Mook, 1983).

3.10.7. Predictive Validity

According to Straub et al. (2004), predictive validity is concerned with the relationship between constructs and the accuracy with which particular constructs might predict a certain outcome variable. Unlike construct validity, it does not have to rely on theory for prediction. Accordingly, Straub et al. (2004) recommend SEM methodologies be adopted to evaluate

predictive validity. PLS-SEM is considered the most appropriate SEM technique for predictive, exploratory theory development and testing (Hair et al., 2011; Hair et al., 2014; Ringle et al., 2012; Wong, 2013) and was therefore employed for the second part of this research. To determine predictive validity, the PLS-SEM results generated for R^2, the path coefficients and inner and outer VIF factors were evaluated (Garson, 2016; Hair et al., 2011; Hair et al., 2014; Ringle et al., 2012; Wong, 2013).

SECTION 4. STUDY 1 – PERSONAL INFORMATION PRIVACY THREATS & TRUST EXPERIMENT

4.1. Results & Analysis

The primary experiment tested 312 subjects with a total of 293 records available after removing data that was incomplete or had failed the manipulation validity check. There were 57, 60, 57, 57 and 62 subjects in the 3D printing, autonomous cars, bionano sensors, drones and email experiment groups respectively. Tests were run to test for unusual cases and duplicate cases using SPSS prior to performing any procedures, which found no results and no outliers were identified for removal. The demographics of subjects can be found in a table to below in table 7.

Table 7

Demographics of Subjects

Age		Year of Study at University		Gender	
18-20 years	244	1st year	231	Male	61%
21-25 years	36	2nd year	46	Female	39%
25-30 years	7	3rd year	7		
31-40 years	0	4th year	8		
41-50 years	4	Unknown	1		
51 + years	2				
Total	*293*	*Total*	*293*	*Total*	*100%*

4.1.1. INSTRUMENT RELIABILITY & VALIDITY

A scale reliability analysis using SPSS was conducted for each of the dependant variable and covariate scales to assess internal consistency reliability using Cronbach's alpha as recommended by Straub et al. (2004). Most of the variable items were between 0.72 – 0.88 and have sufficient internal consistency reliability using Nunally's rule of thumb (Straub et al., 2004), even when considering the inclusion of the new PIP threat related instruments that were developed for each of the technology and institutional-based trust variables. The exceptions to this was the dependant variable for effectiveness and the covariates for technology trust stance and faith in humanity's benevolence (Cronbach's alphas of 0.68, 0.64 and 0.67 respectively). The two covariates were also low in the pilot test. Although faith in humanity's benevolence increased from 0.47 in the pilot test to 0.67, effectiveness decreased from 0.90 in the pilot test to 0.68. While close to Nunally's benchmark of 0.70 for confirmatory research, this decrease was both surprising and inconsistent with the related

Table 8

Descriptive Statistics and Cronbach's Alpha for Dependant Variables & Covariates

	Functionality	Reliability	Effectiveness	Structural Assurance	Situational Normality	Faith in General Technology	Technology Trust Stance	Faith in Humanity – Benevolence	Faith in Humanity – Competence	Faith in Humanity – Integrity	Subjective Norms	Economic Environment	Disposition to Trust	Familiarity
Descriptive Statistics														
N	293	293	291	293	293	293	293	293	289	293	190	293	293	215
Mean	4.87	4.18	4.06	4.12	4.15	5.22	4.96	4.33	5.13	4.38	4.97	5.19	4.19	3.75
Std. Deviation	0.83	0.87	0.97	0.92	0.89	0.68	0.83	0.81	0.81	0.77	1.39	1.04	1.07	1.72
Cronbach's Alpha														
No. Items	5	5	4	4	5	4	3	3	3	3	1	1	4	1
Cronbach's Alpha	0.80	0.80	0.68	0.83	0.81	0.72	0.64	0.67	0.77	0.75	1.00	1.00	0.88	1.000

variables of the constructs from which they belonged and the Cronbach's alpha originally reported. Vance et al. (2008) originally reported a Cronbach's alpha of 0.93 for effectiveness, McKnight et al. (2011) had reported a Cronbach's alpha of 0.86 for technology trust stances, and Li et al. (2008) had reported a Cronbach's alpha of 0.87 for the benevolence limb of faith in humanity. There were no missing values for faith in humanity's benevolence or effectiveness, although there was an even spread of missing values for technology trust stance across each group, affecting 4% of construct data. It is possible the variation in Cronbach's alpha is due to the use of emerging technologies compared the non-emerging technologies tested in the original research from which the instruments were sourced. Table 8 shows the descriptive statistics and Cronbach's Alpha for each initial technology trust dependent variable and for each covariate.

Further comparison of the Cronbach alphas with the pilot test shows most results decreased, although not significantly. This should be expected when the number of subjects increase and items become randomised, as they are both likely to exacerbate variance (Straub et al., 2004). Despite this, all but the aforementioned variables can be considered to have sufficient internal consistency.

A two-tailed Pearson's bivariate correlation was performed on the technology trust variables and covariates to test convergent validity (see table 9). The technology trust variables reported coefficients between 0.47 and 0.74, indicating a medium positive correlation, and reported a statistical significance of $p < 0.01$. This establishes convergent validity exists

Table 9

Pearson's Correlation Analysis of Covariate Technology Trust Variables

	N	Functionality	Reliability	Effectiveness	Structural Assurance	Situational Normality	Faith in General Technology	Technology Trust Stance	Faith in Humanity – Benevolence	Faith in Humanity – Competence	Faith in Humanity – Integrity	Subjective Norms	Economic Environment	Disposition to Trust	Familiarity
Functionality	293														
Reliability	293	**0.74**													
Effectiveness	291	**0.50**	**0.53**												
Structural Assurance	293	**0.54**	**0.61**	**0.65**											
Situational Normality	293	**0.47**	**0.61**	**0.53**	**0.55**										
Faith in General Technology	293	**0.18**	**0.25**	**0.19**	**0.30**	**0.37**									
Technology Trust Stance	293	**0.16**	**0.22**	**0.23**	**0.21**	**0.40**	**0.45**								
Faith in Humanity – Benevolence	293	0.14	**0.30**	**0.29**	**0.28**	**0.28**	**0.31**	**0.31**							
Faith in Humanity – Competence	289	**0.23**	**0.37**	**0.25**	**0.28**	**0.14**	**0.40**	**0.27**	**0.39**						
Faith in Humanity – Integrity	293	**0.16**	**0.26**	**0.25**	**0.30**	**0.25**	**0.35**	**0.38**	**0.58**	**0.39**					
Subjective Norms	190	**0.37**	**0.25**	**0.29**	**0.30**	0.17	--	--	--	--	--				
Economic Environment	293	**0.24**	0.14	**0.21**	**0.23**	**0.19**	**0.22**	**0.31**	**0.25**	**0.30**	**0.39**	--			
Disposition to Trust	293	0.13	**0.27**	**0.20**	**0.21**	**0.34**	**0.17**	**0.36**	**0.26**	**0.18**	**0.22**	--	**0.16**		
Familiarity	215	**0.30**	**0.27**	0.16	**0.22**	**0.34**	**0.10**	--	--	--	--	**0.29**	--	**-0.01**	

Bolded: $p < 0.01$
Not bolded: $p < 0.05$
Not significant: --

between all the technology trust measures. Significant coefficients with a significance of level of $p < 0.01$ was also reported for many of the covariate variables. In particular, the results support that the variable measures for disposition to technology trust (faith in general technology and technology trust) are significantly correlated, as well as the limbs of faith in humanity according to the three people-related trust beliefs. The results also indicate that all covariates are at least weakly positively correlated to the dependant technology trust variables, suggesting that a causal relationship may exist.

Interestingly, the Pearson's correlation analysis found subjective norms are positively correlated with all initial technology trust variables, but not significantly correlated with any other covariate. This may be because subjective norms measures individual's sensitivity to conform to perceived social norms whereas the other covariates are measuring beliefs about

the external environment as factors which might influence their perception of the proposed trust situation. As expected, the trust variables were also positively correlated with initial familiarity, both antecedents to disposition to technology trust, disposition to trust generally, faith in humanity and the economic environment. Initial familiarity also had a negative correlation with disposition to trust, as predicted by knowledge-based trust theory.

An exploratory factor analysis examining the instrument items for functionality, reliability and effectiveness also yielded unexpected results when only analysing the control group for non-emergent technology, as illustrated in table 10. The instruments for these technology variables were adapted from Vance et al. (2008) with a new, extra privacy adapted instrument introduced for each variable to meet the purposes of this research. The exploratory factor analysis, using varimax rotation, produced four dimensions with Eigenvalues above 1.00 and converged within 7 iterations. Three of these dimensions related to functionality, reliability and effectiveness, as they were originally sourced. The fourth dimension only included the new privacy-related instruments with factor loadings of 0.74, 0.77 and 0.83 respectively. The next highest loading for this factor was 0.15. Together, this dimension had the third highest Eigenvalue of 1.20 and explained 14.79% of the variance in results, proving to be stronger

Table 10

Exploratory Factor Analysis of Technology Trust Antecedents for Non-Emerging Technologies

	Functionality	Reliability	Effectiveness	Data integrity
t1	**0.71**	0.27	-0.11	0.09
t2	**0.75**	0.30	-0.16	0.10
t3	**0.76**	0.18	0.09	0.11
t4	0.54	0.69	0.09	0.08
t5	0.37	0.21	0.32	**0.74**
t6	0.27	**0.59**	0.41	0.06
t7	0.05	**0.72**	0.19	0.32
t8	0.39	**0.63**	0.00	0.10
t9	0.15	**0.81**	-0.11	0.16
t10	-0.11	0.29	0.10	**0.77**
t11	**0.56**	0.14	**0.55**	0.15
t12	0.48	0.04	0.30	0.17
t13	-0.14	0.03	**0.87**	0.13
t14	0.32	0.06	0.00	**0.83**
Eigenvalue	*5.36*	*1.68*	*1.08*	*1.20*
% of Variance	*21.46*	*19.56*	*10.84*	*14.79*

**Factor loadings 0.55 and above bolded as significant, as per Hair et al. (1998)*

than effectiveness. This factor is henceforth referred to as "data integrity," which is the extent to which users believe a technology will act according to the best interests of its user's privacy and that it will not exploit or abuse its ability to collect or share personal information. Further detail on the results of exploratory factor analysis can be found in Appendix 4.1.

4.1.2. Emerging Technology Characteristics

To test the validity of the emerging technology framework proposed in section 2.5.1, an exploratory factor analysis with varimax rotation was used on the instruments developed for the emerging technology characteristics, illustrated in table 11.

Table 11

Exploratory Factor Analysis of Emerging Technology Characteristics

	Innovative	Transformative	Uninhibited
E1. Not yet fully exploited	**0.74**	0.23	0.30
E2. Developmental stage of production	**0.86**	0.14	0.02
E3. Early stages of commercialisation	**0.84**	0.26	0.17
E4. Revolutionary in private lives	0.27	**0.85**	0.09
E5. Changes a wide range of industries	0.24	**0.81**	0.23
E6. Changes traditional relationships	0.13	**0.84**	0.21
E7. Changes laws and regulations	0.23	0.30	**0.91**
Eigenvalue	*1.14*	*3.79*	*0.63*
% of Variance	*16.29*	*54.11*	*8.97*

Factor loadings 0.55 and above bolded as significant, as per Hair et al. (1998)

Innovativeness loaded as expected with an Eigenvalue of 1.14 and factors between 0.74 and 0.86, explaining 16.29% of total variance. The remaining instruments for revolutionary and disruptiveness loaded expectantly. The item for revolutionary loaded with two of the items from disruptive relating to the emerging technology's ability to change industries and traditional relationships. Together, these items had a significant Eigenvalue of 3.79 and factors between 0.81 and 0.85, explaining 54.11% of variance. This factor was renamed "transformative" since each of these items represent indirect impacts of an emerging technology in society: including, individuals' personal lives in how they live and do things, the structure and practise of industries or the creating of new industries or causing the closure of others, forced by the introduction of the emerging technology; and the change of traditional relationships between buyers and sellers, the government and public or domestic roles. The remaining item for disruptiveness related to an emerging technology's ability to

change laws and regulations which had an Eigenvalue of 0.63 and a factor of 0.91, explaining only 8.97% of total variance. This was renamed “uninhibited” to represent the nature of emerging technologies that generally evolve and develop, unchecked from regulation, and the need for restraint occasionally. Unlike transformative, these changes do not usually occur gradually overtime but mark a point in time when the emerging technology is formally recognised for the transformative impact it has in society and the need to restrain its development or use and the attempt to manage its change effects.

Although uninhibited scored an Eigenvalue below 1.00, it has been left in this thesis for discussion purposes since it is possible the subject pool or New Zealand context may have contributed to this result. In countries more technology focussed, including Europe and the United States, its likely individuals are more aware of advanced technology developments and their governing bodies anticipate and respond more quickly and efficiently than New Zealand which generally is more responsive to technologies and follows international regulatory trends.

4.1.3. Perceived Emergence of Technologies

To test whether technologies were perceived as being “emergent” a MANOVA was used in SPSS using a Tukey post-hoc analysis. To pass each test for emergence, each technology’s means had to be significantly different from email using a significance interval of 0.05 and at least one test in each of the three “emerging” characteristic categories being passed (i.e. innovativeness and transformative). As illustrated in table 12, all proposed emerging technologies were perceived to be “emergent” compared to email. These results suggest that each of these technologies are perceived to be highly emergent with each technology passing all three “innovative” tests and two out three “transformative” tests at $p < 0.01$, validating their use in this research. In addition to table 12, table 13 also shows the descriptive statistics for emerging technologies according to the testing framework.

A multivariate test using Wilk’s Lambda reported a significance of $p < 0.01$, indicating that the variance in perceived emergence was significantly influenced by the individual treatments for each technology. Similarly, a test of between-subject effects reported $p < 0.01$. A Levene’s test produced significant results with $p < 0.05$ for most of the emergence tests. Because the purpose of this test was to evaluate the validity of the experimental technologies

Table 13

Mean Differences Between Email and Emerging Technologies

Characteristics	3D printing	Autonomous cars	Bionano sensors	Drones
1. Innovativeness				
a. Not yet fully exploited	**2.31**	**1.92**	**1.92**	**1.81**
b. Developmental stage of production	**2.25**	**2.52**	**2.30**	**1.60**
c. Early stages of commercialisation	**1.78**	**1.98**	**1.61**	**1.50**
	Pass	Pass	Pass	Pass
2. Transformative				
a. Revolutionary in daily life	**1.03**	0.74	**0.97**	0.80
b. Changes a wide range of industries	**1.30**	**0.86**	**1.11**	**1.36**
c. Changes traditional relationships	--	--	0.76	0.75
	Pass	Pass	Pass	Pass
3. Uninhibited*				
a. Changes laws and regulations	**1.10**	**1.09**	**0.97**	**1.50**
	Pass	Pass	Pass	Pass
Emerging Technology?	**PASS**	**PASS**	**PASS**	**PASS**

Bolded: $p < 0.01$
Not Bolded: $p < 0.05$
No significant difference: -
**The test for "uninhibited" was not validated and is reported for interest only*
Note. Characteristics with more than one attribute must satisfy at least one criterion for the characteristic to exist and awarded a "pass." An attribute is satisfied when it has mean difference which is significantly different from e

Table 12

Descriptive Statistics for Emerging Technology Characteristics

Characteristics & Criterion	3D printing		Autonomous cars		Bionano sensors		Drones		Email	
	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.
1. Innovative										
a. Not yet fully exploited	5.70	1.05	5.32	1.17	5.32	1.07	5.20	1.16	3.39	1.38
b. Developmental stage of production	5.25	1.12	5.52	1.20	5.30	1.00	4.60	1.40	3.00	1.64
c. Early stages of commercialisation	5.65	1.01	5.85	0.97	5.47	0.98	5.36	1.02	3.87	1.77
2. Transformative										
a. Revolutionary in daily life	5.39	1.10	5.10	1.35	5.33	1.22	5.16	1.34	4.34	1.62
b. Changes a wide range of industries	5.60	0.96	5.15	1.34	5.40	1.07	5.66	1.11	4.30	1.48
c. Changes traditional relationships	5.02	1.08	5.07	1.21	5.30	1.19	5.29	1.31	4.53	1.49
3. Uninhibited										
c. Changes laws and regulations	5.63	1.05	5.63	1.23	5.51	1.18	6.04	0.94	4.57	1.34

**The test for "uninhibited" was not validated and is reported for interest only*

and it was possible significant variances might exist across the perceived characteristics of emergence for each technology, these results are acceptable. Given that each technology will be used to operationalise different PIP threats uniquely characterised by emerging technologies, these results support the assumption that each technology are "emergent" and are significantly different from non-emergent technologies (as operationalised with email) from which the remainder of this research could be based upon.

4.1.4. Personal Information Privacy Threats

4.1.4.1. Exploratory Factor Analysis

An exploratory factor analysis using varimax rotation indicated that the PIP threats characterised by emerging technologies proposed by Conger et al. (2013) have a three dimensional pattern, as hypothesised in section 4.6.4 and supporting H1 and H2. Table 14 reports these results and reports the factor loadings and Eigenvalues for each variable.

Table 14

Factor Loadings for PIP Threats of Emerging Technology

	Factor 1 Intrusiveness	Factor 2 Omnipotence	Factor 3 Invisibility
Network ubiquity	0.28	**0.74**	- 0.19
Physical ubiquity	0.04	**0.77**	0.13
Invisibility	0.12	0.10	**0.96**
Invasiveness	**0.85**	- 0.17	0.12
Collectability of information	**0.88**	- 0.02	0.08
Programmability	- 0.23	**0.76**	0.16
Wireless accessibility	**0.62**	0.25	- 0.04
Eigenvalue	*2.08*	*1.80*	*0.97*
% of Variance	*30%*	*26%*	*14%*

**Factor loadings 0.55 and above bolded as significant, as per Hair et al. (1998)*

Intrusiveness explained 30% of variance with an Eigenvalue of 2.08. It supports H1 with loadings from invasiveness, collectability of information and wireless accessibility. Unlike the pilot test, the variable for invasiveness did not cross load with invisibility and it reported a loading of 0.85 for intrusiveness and 0.12 for invisibility. Additionally, wireless accessibility did not load strongly for intrusiveness, as in the pilot test, but loaded a relatively weaker significant relationship with a factor loading of 0.62 compared to invasiveness and collectability of information of 0.85 and 0.88 respectively. This suggests wireless accessibility is an important characteristic of emerging technologies which presents a PIP threat, but perceptions of invasiveness and its ability to collect information bears greater

weight. However, this must be taken with caution given that experiments should not be relied upon to make inferences about significance (Bhattacherjee, 2012; Mook, 1983).

Omnipotence explained 26% of total variance with an Eigenvalue of 1.08. It supports H2 with loadings from physical ubiquity, network ubiquity and programmability, similar to the pilot test.

Invisibility explained 14% of variance with an Eigenvalue of 0.97 and a factor loading of 0.96. It is generally accepted that factors that load with an Eigenvalue equal or greater than 1.00 are considered significant in factor analyses using the Kaiser criterion (Costello & Osbourne, 2005). However, the Kaiser criterion does not clearly distinguish between confirmatory research and exploratory research (Costello & Osbourne, 2005; Hoe, 2008; Patil, Singh, Mishra, & Donavan, 2007; B. Williams, Onsman, & Brown, 2010). Since the purpose of an exploratory factor analysis is to explore the main underlying dimensions of a construct to generate theory and demonstrate construct validity (Straub et al., 2004; B. Williams et al., 2010), it was determined the invisibility factor was significant enough for the exploratory purpose of this research and should be retained for further analysis and discussion as it offered potentially valuable contributions to research. This is on the basis that invisibility yielded an Eigenvalue of 0.97, which is very close to the recommended static threshold of 1.00, and considering that the purpose of this test was of exploratory nature to build a theory which can be further validated and tested in future research, thereby suggesting the risk for this test is not the over extraction of factors but under extraction (Stewart, 1985; B. Williams et al., 2010). It was also noted that criticism of current literature existed relating to the objectivity of the Kaiser criterion, suggesting that theoretical considerations should be accounted for and sound judgement should be exercised considering the context (Patil et al., 2007; B. Williams et al., 2010).

Overall, these results support the existence of a three-dimensional structure for the proposed PIP threats of emerging technologies, confirming H1 and H2.

4.1.4.2. Operationalising Personal Information Privacy Threats

A MANOVA for the perceived PIP threats using Tukey post hoc analyses were used to discover which technologies best represented the different threats to PIP, the results of which would be used to help answer each hypothesis. To determine if an emerging technology represented a PIP threat it had to be significantly different from the baseline PIP threat that individuals were generally willing to accept, as represented by email and reported in table 15. Several emerging technologies were perceived to represent similar levels of PIP threats across each of the dimensions, as reported in table 15, with comparably similar mean scores between autonomous cars and drones for intrusiveness, bionano sensors and drones for omnipotence and invisibility. Consequently, a single emerging technology could not be used to operationalise only one PIP threat as intended. Therefore, significant mean differences among the emerging technologies was used to support findings for H3a-e, H4a-e and H5a-e. To determine whether each hypothesis could be supported a significant mean difference was required to have occurred (a) between the perceived PIP threat of each emerging technology and the control group or (b) between the perceived PIP threat of between two emerging technologies. Table 16 reports these mean differences.

Table 15

Average PIP Threat Means for Each Technology

	3D printing	Autonomous cars	Bionano sensors	Drones	Email
Intrusiveness	4.58	5.34	5.16	5.36	4.73
Omnipotence	4.72	4.49	4.03	4.11	4.60
Invisibility	4.44	4.27	4.89	4.98	4.53

Note 1. Scale: 1 = Strongly Disagree, 3 = Disagree, 4 = Neutral, 5 = Agree, 7 = Strongly Agree

Table 16

Mean Differences Between Perceived PIP Threats

Intrusiveness		Omnipotence		Invisibility	
3d – ac	**-0.77**	3d – bn	**0.69**	ac - dr	-0.71
3d – bn	**-0.58**	3d – dr	-0.61	dr – ac	0.71
3d – dr	**-0.79**	bn – em	-0.57		
ac – 3d	**0.77**	bn – 3d	**-0.69**		
ac – em	**0.62**	dr – 3d	0.61		
bn – 3d	**0.58**	em – bn	0.57		
dr – 3d	**0.79**				
dr – em	**0.64**				
em – ac	**-0.62**				
em – dr	**-0.64**				

Bolded: $p < 0.01$
Not bolded: $p < 0.05$
3d = 3D printing; ac = Autonomous cars; bn = Bionano sensors; dr = Drones; em = Email

Using a significance level of 0.05, a MANOVA shows that different technologies significantly influence perceived PIP threats. Intrusiveness saw the greatest significant variance of technologies across its spectrum, largely due to the low PIP mean from 3D printing, which was less than email. A multivariate test using Wilk's Lambda indicated individual technology characteristics have a significant influence on their associated perceived threats to PIP with $p < 0.01$. A test of between-subject effects had a $p < 0.05$ for each PIP threat, also indicating that the type of technology had a significant effect on the results for perceived PIP threats. A Levene's test produced $p > 0.05$ for intrusiveness and invisibility, but not omnipotence. This indicates that the variance within each technology was equal for the perceived PIP threats of intrusiveness and invisibility and that only a technology's perceived omnipotence varied within groups.

Based on the results of the MANOVA, intrusiveness may be measured using five different pairings, including two pairings with the control technology, for the purposes of testing H3. Omnipotence may be measured using three different pairings, including one pairing with the control technology, for the purposes of testing H4. Only one pairing with significant mean difference could be identified for invisibility for the purposes of answering H5. The lack of pairings with invisibility compared to the other PIP threats may limit the ability to answer H5. Additionally, it is interesting to note that none of the emerging technologies were found to have significantly greater threats to PIP due their omnipotence and invisibility than email, even though email was perceived to be relatively neutral, with some tendency towards acknowledging a perceived PIP threat may exist.

4.1.5. Investigating the Relationship between Trust and Personal Information Privacy

To determine whether greater perceptions of each PIP threat had a significant effect on initial trust in emerging technologies (H3, H4 and H5), it is first necessary to investigate and answer parts a to e of each hypotheses and determine whether perceptions of each PIP threat have a negative effect on technology and institutional-based trust antecedents. If so, it can be gauged that higher levels of the respective PIP threat lead to decreased levels of initial technology based trust and vice versa.

To measure parts a to e of each hypothesis, a MANOVA was performed for each trust belief (functionality, reliability, effectiveness, structural assurance and situational normality), with a Tukey post hoc analysis. To determine whether each hypothesis could be supported a

significant mean difference must have occurred between (a) an emerging technology and the non-emerging control technology or (b) any pair of emerging technologies, as indicated in the MANOVA for PIP threats in section 4.1.4.2. These additional pairings are justifiable on the basis that they represent two points on the spectrum of which a PIP threat is perceived and of which a consequential change in trust might occur. Furthermore, results had to satisfy a 0.05 significance level. MANOVA results are reported in table 17 and demonstrate a number of significant pairings which were available for each hypotheses, supporting H3a, H3b, H3c, H3d, H4a, H4b, H4c, H4d, H5a and H5c. Five hypotheses could not be supported, including all three hypothesis relating to the effect of each PIP threat on situational normality beliefs.

A multivariate test using Wilk's Lambda indicated that the operationalised PIP threats had a significant effect on individual's trust beliefs with $p < 0.01$. Similarly, a test of between-subject effects had a $p < 0.05$ for each trust type except for situational normality, indicating that each technology, and the PIP threats they represent, had a significant effect on the results for each type of trust except situational normality. A Levene's test produced $p > 0.05$ for all trust types, indicating that each technology group held equal amounts of variance and supporting the validity of further MANOVA analyses.

Table 17

Mean Differences in MANOVA Multiple Comparisons for Trust Variables

	(a) Between Emerging Technology and Non-Emerging Technology				(b) Between Other Significant Pairs						
Intrusiveness	ac - em	dr - em	em - ac	em - dr	3d - ac	3d - dr	ac - 3d	bn - dr	dr - 3d	dr - bn	
H3a – Functionality	**-0.89**		**0.89**								✓
H3b – Effectiveness		-0.54		0.54		0.55		0.56	-0.55	-0.56	✓
H3c – Reliability	**-0.83**		**0.83**								✓
H3d – Structural Assurance	**-0.60**	-0.47	**0.60**	0.47	0.46		-0.46				✓
H3e – Situational Normality											**x**
Omnipotence	3d - em	bn - em	em - 3d	em - bn	3d - bn	3d - dr	bn - 3d	dr - 3d			
H4a – Functionality	**-0.55**	0.46	**0.55**	-0.46							✓
H4b – Effectiveness		-0.46		0.46		0.55		-0.55			✓
H4c – Reliability	-0.50		0.50								✓
H4d – Structural Assurance		-0.47		0.47							✓
H4e – Situational Normality											**x**
Invisibility					ac - dr	dr - ac					
H5a – Functionality					**-0.70**	**0.70**					✓
H5b – Effectiveness											**x**
H5c – Reliability					-0.42	0.42					✓
H5d – Structural Assurance											**x**
H5e – Situational Normality											**x**

Bolded: $p < 0.01$
Not bolded: $p < 0.05$

Overall, H3, H4 and H5 can be supported and greater PIP threats cause a decrease in initial technology beliefs in emerging technologies, and vice versa. The initial technology trust antecedent for functionality and reliability were supported across all three types of PIP threats and effectiveness and structural assurance was supported for two out of three PIP threats, intrusiveness and omnipotence.

The hypotheses regarding perceived intrusiveness (H3) had the most data available for analysis. This is due to the significant difference in perceived intrusiveness between drones and 3D printing in the experiment, where 3D printing yielded a lower mean score of perceived intrusiveness than email. This provided three additional pairs of technologies that could be used to investigate for significant mean differences, in addition to all the pairings with autonomous cars which operationalised intrusiveness. The results support H3, that greater perceived threats of intrusiveness will decrease initial technology trust beliefs and vice versa. However, significant support could not be found for the effect of intrusiveness on situational normality institutional-based trust beliefs. A summary of hypotheses results can be found in table 18.

Omnipotence was operationalised by 3D printing with the MANOVA for PIP threats only yielding one other pairing of technologies for analysis. Similar to intrusiveness, results support H4 and that greater perceived omnipotence will decrease initial technology trust in emerging technologies and vice versa. Similar to H3, evidence was found to support a causal relationship between situational normality institutional-based trust beliefs.

Findings for invisibility, H5, were limited considerably by the inability to find an emerging technology that could be used to operationalise it. However, despite the hypotheses regarding invisibility being left largely unsupported due to a lack of appropriate data, a significant mean difference was found to support the causal relationship between perceived invisibility and the trust beliefs of functionality and reliability. Although evidence to support a strong causal relationship between invisibility and institutional-based trust beliefs could not be found, support does exist for H5 in general. If further pairings were available, it is possible more data may have been available to produce similar hypothesis results as H3 and H4 for invisibility.

Table 18

Summary of Hypotheses Results

	Supported
H1. A technology's degree of invasiveness, ability to collect information and wireless accessibility relate to its level of "intrusiveness" which presents a threat to PIP	✓
H2. A technology's degree of physical ubiquity, network ubiquity and programmability relate to its level of "omnipotence" which presents a threat to PIP	✓
H3. Greater perceived intrusiveness will decrease initial technology trust in emerging technologies, and vice versa	✓
H3a. Greater perceived intrusiveness will decrease perceived functionality in emerging technologies, and vice versa	✓
H3b. Greater perceived intrusiveness will decrease perceived effectiveness in emerging technologies, and vice versa	✓
H3c. Greater perceived intrusiveness will decrease perceived reliability in emerging technologies, and vice versa	✓
H3d. Greater perceived intrusiveness will decrease perceived structural assurance in emerging technologies, and vice versa	✓
H3e. Greater perceived intrusiveness will decrease perceived situational normality in emerging technologies, and vice versa	x
H4. Greater perceived omnipotence will decrease initial technology trust in emerging technologies, and vice versa	✓
H4a. Greater perceived omnipotence will decrease perceived functionality in emerging technologies	✓
H4b. Greater perceived omnipotence will decrease perceived effectiveness in emerging technologies, and vice versa	✓
H4c. Greater perceived omnipotence will decrease perceived reliability in emerging technologies, and vice versa	✓
H4d. Greater perceived omnipotence will decrease perceived structural assurance in emerging technologies, and vice versa	✓
H4e. Greater perceived omnipotence will decrease perceived situational normality in emerging technologies, and vice versa	x
H5. Greater perceived invisibility will decrease initial technology trust in emerging technologies, and vice versa	✓
H5a. Greater perceived invisibility will decrease perceived functionality in emerging technologies, and vice versa	✓
H5b. Greater perceived invisibility will decrease perceived effectiveness in emerging technologies, and vice versa	x
H5c. Greater perceived invisibility will decrease perceived reliability in emerging technologies, and vice versa	✓
H5d. Greater perceived invisibility will decrease perceived structural assurance in emerging technologies, and vice versa	x
H5e. Greater perceived invisibility will decrease perceived situational normality in emerging technologies, and vice versa	x

Together, the PIP threats explained approximately 36% of the variance in initial technology trust beliefs with an aggregate R^2 of 0.36 ($p < 0.01$). Following Cohen (1992), the PIP threats had a moderate effect on functionality with an $R^2 = 0.14$ ($p < 0.01$), explaining 14% of variance in functionality beliefs. PIP threats had a small to moderate effect on reliability with an $R^2 = 0.10$ ($p < 0.01$) and explaining 10% of variance in reliability trust beliefs. Effectiveness and structural assurances had a small effect of $R^2 = 0.05$ ($p < 0.01$) and $R^2 = 0.06$ ($p < 0.01$), explaining 5% and 6% of variance in each trust belief respectively. Situational normality had almost no effect with an $R^2 = 0.01$ ($p < 0.01$) and PIP threats explaining only 1% of variance in the trust belief.

4.1.6. The Effect of Covariates

Several covariates were included in this research, including disposition to technology trust (in the forms of general faith in technology and technology trust stance), faith in humanity's benevolence, competence and integrity and disposition to trust generally. A MANCOVA was performed for each covariate, with all covariates found to have a significant influence on the trust variables using a significance level of 0.05. A multivariate test using Wilk's Lambda confirms that the operationalised PIP threat treatments significantly influenced initial technology trust beliefs with $p < 0.01$. The Levene's tests performed with each MANCOVA indicated that the assumption of homoscedasticity is true for the purposes of this research with $p > 0.05$. With most p values less than 0.01 for the tests of between-subject effects, and remainder with p values less than 0.05, these MANCOVAs suggest significant, strong relationships between the initial technology trust variables and each covariate. However, when controlling for each covariate no significant effect was found, presenting no change to the effect of PIP threats on the initial technology trust variables. These covariates included disposition to technology trust (as faith in general technology and technology trust stance), disposition to trust generally, faith in humanity's benevolence, competence and integrity, subjective norms, economic environment and the initial familiarity of subjects of their respective technologies as an indicator of familiarity.

4.1.6.1. Disposition to Technology Trust: Faith in General Technology & Technology Trust Stance

Disposition to technology trust was measured in the form of its two constructs: faith in general technology and technology trust stance. Tested individually, both reported the same results. Levene's test produced $p > 0.05$ for both measures, indicating that the different technology groups hold equal variance, confirming homoscedasticity. Tests of between-subject effects found that both faith in general technology and technology trust stance had a significant direct effect on all of the trust values with $p < 0.01$. This means if an individual has a greater disposition to trust technology, they will have greater initial trust levels in technologies they have not used before and have no prior experience and limited knowledge of. After controlling for the effects of faith in general technology and technology trust stance, the technologies and the PIP threats they represented still had a significant effect on all the trust variables except for situational normality. This supports the proposition that disposition to technology trust influences initial technology trust and is consistent with the technology trust model proposed by McKnight et al. (2011).

An evaluation of R^2 values for faith in general technology shows that the PIP threats had a moderate effect on functionality, reliability, structural assurance and situational normality with an $R^2 = 0.16$ ($p < 0.01$), $R^2 = 0.15$ ($p < 0.01$), $R^2 = 0.14$ ($p < 0.01$) and $R^2 = 0.14$ ($p < 0.01$), and explaining 16%, 15%, 14% and 14% of variance in initial technology trust beliefs respectively (Cohen, 1992). PIP threats had a small effect on reliability with an $R^2 = 0.08$ ($p < 0.01$) and explaining 8% of variance in reliability trust beliefs (Cohen, 1992). Each of these R^2 values are greater than those reported in the MANOVA procedures, without taking into account the effect of covariates and their degrees of variance on initial technology trust beliefs.

R^2 values for technology trust stance shows that the PIP threats had a moderate effect on functionality and situational normality with an $R^2 = 0.16$ ($p < 0.01$) and $R^2 = 0.18$ ($p < 0.01$), and explaining 16% and 18% of variance in initial technology trust beliefs respectively (Cohen, 1992). PIP threats had a small to moderate effect on reliability, effectiveness and structural assurance with an $R^2 = 0.14$ ($p < 0.01$), $R^2 = 0.10$ ($p < 0.01$) and $R^2 = 0.10$ ($p < 0.01$) and explaining 14%, 10% and 10% of variance in their initial technology trust beliefs (Cohen, 1992). Each of these R^2 values are greater than those reported in the MANOVA procedures.

4.1.6.2. Disposition to Trust Generally

Consistent with existing trust research in the fields on people-related trust and e-commerce trust research, disposition to trust in general was found to have a significant effect on initial technology trust (Chen & Barnes, 2007; Gefen, 2000; McKnight et al., 2000; Pavlou, 2003; Vance et al., 2008; Wingreen & Baglione, 2005). Levene's test indicates that the different technology groups hold equal variance, confirming homoscedasticity with $p > 0.05$. Tests of between-subject effects found disposition to trust had a significant direct effect on all the trust values with $p < 0.01$. This means if an individual has a greater disposition to trust generally, whether this be people, objects, organisations or institutions, they will have relatively greater initial technology trust beliefs in technologies they have not used before and vice versa. As expected, after controlling for the effects of disposition to trust, the technologies and the PIP threats they represent still had a significant effect on all the trust variables except for situational normality.

An evaluation of R^2 values for faith in general technology shows that the PIP threats had a moderate effect on functionality, reliability and situational normality with an $R^2 = 0.16$ ($p < 0.01$), $R^2 = 0.14$ ($p < 0.01$) and $R^2 = 0.18$ ($p < 0.01$), and explaining 16%, 14% and 18% of variance in initial technology trust beliefs respectively (Cohen, 1992). PIP threats had a small to moderate effect on effectiveness and structural assurance which both reported $R^2 = 0.10$ ($p < 0.01$) and explaining 10% of variance in their respective initial technology trust beliefs (Cohen, 1992). Each of these R^2 values are greater than those reported in the MANOVA procedures, without taking into account the effect of covariates and their degrees of variance on initial technology trust beliefs.

Disposition to trust generally is both related and distinct from disposition to technology trust. Disposition to technology trust measures an individual's propensity to trust a technology object and therefore its functionality, reliability and effectiveness (McKnight et al., 2011). This will be influenced by one's disposition to trust generally to some extent, which means disposition to trust will likely exert greater influence over the remaining covariate factors of initial technology trust proposed (institutional-based trust, vendor-based trust and faith in humanity) compared to disposition to technology trust.

4.1.6.3. Faith in Humanity

Faith in humanity was measured and tested according to the three widely accepted people-related trust dimensions of benevolence, competence and integrity for greater reliability. Likewise, they too produced similar results to one another. All three Levene's tests yielded $p > 0.05$, indicating that the different technology groups hold equal amounts of variance and are homoscedastic. Tests of between-subject effects found all three dimensions of faith in humanity had a significant effect on all the trust variables with $p < 0.01$ except for the effect of faith in humanity's benevolence on perceived functionality with a p value of 0.02, which is still highly significant. This means that if an individual has greater faith in humanity, they will have greater initial technology trust beliefs in technologies they have not used before and have no prior experience or limited knowledge of, and vice versa. Nonetheless, after controlling for the effects of faith in humanity and its three dimensions, the technologies and the PIP threats they represent still had a significant effect on all the initial technology trust variables except for situational normality.

An evaluation of R^2 values for faith in humanity's benevolence shows that the PIP threats had a moderate effect on functionality and reliability with an $R^2 = 0.16$ ($p < 0.01$) and $R^2 = 0.18$ ($p < 0.01$), explaining 16% and 18% of variance in the respective initial technology trust beliefs (Cohen, 1992). PIP threats had a small to moderate effect on effectiveness and structural assurance with an $R^2 = 0.13$ ($p < 0.01$) and $R^2 = 0.14$ ($p < 0.01$) and explaining 13% and 14% of variance their respective initial technology trust beliefs (Cohen, 1992). Each of these R^2 values are greater than those reported in the MANOVA procedures.

R^2 values for faith in humanity's competence shows that the PIP threats had a moderate effect on functionality, effective and structural assurance with an $R^2 = 0.20$ ($p < 0.01$), $R^2 = 0.16$ ($p < 0.01$) and $R^2 = 0.14$ ($p < 0.01$), explaining 20%, 16% and 14% of variance in the respective initial technology trust beliefs (Cohen, 1992). PIP threats had a small to moderate effect on reliability with an $R^2 = 0.11$ ($p < 0.01$), explaining 11% of variance in reliability trust beliefs, and had a small effect on situational normality with an $R^2 = 0.06$ ($p < 0.01$), explaining 6% of variance in situational normality trust beliefs (Cohen, 1992). Each of these R^2 values are greater than those reported in the MANOVA procedures.

R^2 values for faith in humanity's integrity shows that the PIP threats had a moderate effect on functionality, reliability and structural assurance with an $R^2 = 0.17$ ($p < 0.01$), $R^2 = 0.17$ ($p < 0.01$) and $R^2 = 0.16$ ($p < 0.01$), explaining 17%, 17% and 16% of variance in the respective initial technology trust beliefs (Cohen, 1992). PIP threats had a small to moderate effect on effectiveness with an $R^2 = 0.11$ ($p < 0.01$), explaining 11% of variance in effectiveness trust beliefs, and had a small effect on situational normality with an $R^2 = 0.08$ ($p < 0.01$), explaining 8% of variance in situational normality trust beliefs (Cohen, 1992). Each of these R^2 values are greater than those reported in the MANOVA procedures.

4.1.6.4. Subjective Norms

There was a loss of data for the subjective norms variable which was evenly spread across the technology groups. Yet, 191 valid records were available for analysis with approximately 40 subjects per group; a sufficiently large dataset for a controlled experiment. A Levene's test produced $p > 0.05$, suggesting the technology groups were homoscedastic and shared equal amounts of variance. Tests of between-subject effects found subjective norms had a significant effect on trust variables with $p < 0.01$ for all initial technology trust variables except for situational normality which had a p value of 0.025, a result which is still highly

significant. This means the more an individual believes a technology will become an accepted norm, the greater their initial technology trust beliefs towards the respective technology will be and vice versa. After controlling for the effects of this, the technologies and the PIP threats they represent were found to have a significant effect on the functionality and effectiveness technology trust variables only. Although subjective norms yielded less significant effects than some of the other covariates, this is still sufficient to conclude that greater subjective norms will decrease initial technology trust and vice versa.

R^2 values for subjective norms shows that the PIP threats had a moderate effect on functionality, with an $R^2 = 0.23$ ($p < 0.01$) (Cohen, 1992). PIP threats had a small to moderate effect on effectiveness, reliability and structural assurance with an $R^2 = 0.12$ ($p < 0.01$), $R^2 = 0.11$ ($p < 0.01$) and $R^2 = 0.11$ ($p < 0.01$) explaining 12%, 11% and 11% of variance in their respective initial technology trust beliefs. Situation normality had a $R^2 = 0.03$, but with $p = 0.32$ and is therefore not statistically significant.

4.1.6.5. Economic Environment

The covariate for the perceived safety of the economic environment was included in this research to account for cultural and political influences on a trust situation. A Levene's test indicates that the technology groups were homoscedastic and shared equal amounts of variance with $p > 0.05$. Tests of between-subject effects found the perceived safety of one's economic environment had a significant effect on the initial technology trust variables, including situational normality, at $p < 0.01$. The exception was reliability which had a p value of 0.02, a result which is still highly significant. This means if an individual believes they are acting in a safe, reliable economic environment with appropriate consumer protections, they will have greater initial technology trust levels in technologies they have no experience with and vice versa. However, after controlling for the effects of this, the technologies and the PIP threats they represent were still found to have a significant effect on the all but one of the initial technology trust variables, the exception being situational normality beliefs.

R^2 values for the perceived safety of the economic environment shows that the PIP threats had a moderate effect on functionality with an $R^2 = 0.19$ ($p < 0.01$) explaining 19% of variance in the respective initial technology trust beliefs (Cohen, 1992). PIP threats had a small to moderate effect on effectiveness and structural assurance, both with an $R^2 = 0.11$ ($p < 0.01$) and explaining 11% of variance in their respective initial technology trust beliefs, and

had a small effect on effectiveness and situational normality with an $R^2 = 0.09$ ($p < 0.01$) and $R^2 = 0.05$ ($p < 0.01$), explaining 9% and 5% of variance in their respective initial technology trust beliefs (Cohen, 1992). Each of these R^2 values are greater than those reported in the MANOVA procedures.

The purpose for this measure was to account for the varying levels of the perceived safety individuals might have in their wider economic environment and belief that the current economic environment will lead to positive outcomes. This measure referred to the local economic environment of the individual's country of residence and the technology industry in New Zealand. On the surface, this appears like it should be linked to trust in structural assurances, but it takes a more macroeconomic view. It does not examine the more immediate contextual factors such as guarantees and vendor contracts that are more likely to vary across different countries and borders, but the cultural and current economic impacts differing environments impact how vendors and potential buyers behave in a trust situation. Thus, it account for some variation in faith in humanity when used as a proxy for vendor-based trust.

4.1.6.6. Initial Familiarity of Technology

A covariate was included to measure an individual's initial familiarity of the technology they were treated with before being treated and as such represents uncontrolled familiarity or second-hand information individuals have previously received. Similar to the subjective norms covariate, it was measured with one instrument and had 214 valid records available for analysis. A Levene's test produced $p > 0.05$, indicating that the technology groups were homoscedastic and shared equal amounts of variance. Tests of between-subject effects found initial familiarity had a significant effect on the initial technology trust variables with $p < 0.01$ for all the variables except for structural assurance which had a p value of 0.015, a result which is still highly significant. This means if an individual has greater second-hand knowledge about a technology, then they will have greater initial technology trust beliefs. After controlling for the effects of initial technology familiarity, the technologies and the PIP threats they represent were still found to have a significant effect on the technology trust variables, but not the institutional trust variables for structural assurance and situational normality.

R^2 values for the initial familiarity shows that the PIP threats had a moderate effect on functionality with an $R^2 = 0.16$ ($p < 0.01$) explaining 16% of variance in the respective initial

technology trust beliefs (Cohen, 1992). PIP threats had a small to moderate effect on reliability and situational normality with an $R^2 = 0.13$ ($p < 0.01$) and $R^2 = 0.12$ ($p < 0.01$) and explaining 13% and 12% of variance in their respective initial technology trust beliefs, and had a small effect on effectiveness and situational normality with an $R^2 = 0.09$ ($p < 0.01$) and $R^2 = 0.13$ ($p < 0.01$), explaining 9% and 13% of variance in their respective initial technology trust beliefs (Cohen, 1992). Each of these R^2 values are greater than those reported in the MANOVA procedures.

The following table depicts a summary of the covariate results and comparison of R^2 values in tables 19 and 20. More detailed MANCOVA reports can be found in Appendix 4.

Table 19

Summary of Covariate Results

	Significant effect of initial technology trust levels?					Significant effect of PIP threats on initial technology trust levels after controlling for covariate effects?				
	F	E	R	SA	SN	F	E	R	SA	SN
Disposition to technology trust										
Faith in general technology	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
Technology trust stance	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
Disposition to trust	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
Faith in humanity										
Benevolence	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
Competence	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
Integrity	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
Subjective norms	✓	✓	✓	✓	✓	✓	✓	x	x	x
Economic environment	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
Familiarity	✓	✓	✓	✓	✓	✓	✓	✓	x	x

F = Functionality; E = Effectiveness; R = Reliability; SA = Structural Assurance; SN = Situational Normality
Bolded: $p < 0.01$
Not bolded: $p < 0.05$

Table 20

Comparison of R^2 values With and Without Covariates

	Main Effects (Without Covariates)	Faith in General Technology	Technology Trust Stance	Disposition to Trust Generally	Faith in Humanity (Benevolence)	Faith in Humanity (Competence)	Faith in Humanity (Integrity)	Subjective Norms	Safety of the Economic Environment	Initial Awareness
Functionality	**0.14**	**0.16**	**0.16**	**0.16**	**0.16**	**0.20**	**0.17**	**0.23**	**0.19**	**0.16**
Effectiveness	**0.05**	**0.08**	**0.10**	**0.09**	**0.13**	**0.16**	**0.11**	**0.12**	**0.09**	**0.09**
Reliability	**0.10**	**0.15**	**0.14**	**0.17**	**0.18**	**0.11**	**0.17**	**0.11**	**0.11**	**0.12**
Structural Assurance	**0.06**	**0.14**	**0.10**	**0.11**	**0.14**	**0.14**	**0.16**	**0.11**	**0.11**	**0.08**
Situational Normality	**0.01**	**0.14**	**0.18**	**0.13**	**0.09**	**0.06**	**0.08**	**--**	**0.05**	**0.13**

Bolded: $p < 0.01$
Not bolded: $p < 0.05$

4.1.7. Summary of Findings

The emerging technology test framework was partially validated with the use of "innovativeness" confirmed. The characteristics "revolutionary" and "disruptiveness" reported unexpected factors with the single item for revolutionary loading with two items designed for disruptiveness. This factor was renamed "transformative" and demonstrates how emerging technologies change the personal lives of individuals and how they live, economic markets and industries, and traditional relationships in society. The remaining item for disruptiveness related how emerging technologies may trigger a change in laws and regulations and renamed "uninhibited," although it was not sufficiently validated in this research. However, it is possible this factor may prove relevant in other research when tested in countries that are more technology advanced and better anticipate technology changes.

Overall, the proposed model for initial technology trust, with its inclusion of PIP threats and covariates, appears relatively robust with perceived threats to PIP proving to have a significant effect on technology trust and institutional-based trust. In fact, the different threats to PIP had a significant effect on all of the trust variables except for situational normality. This could be a consequence of the instrumentation, the use of emerging technologies to test the model, or simply because perceived threats to PIP do not present any direct significant effect of perceived situational normality. The null hypothesis of H4e and H5b,c-e could not be rejected like those in H3a-d, however these hypotheses were tested with fewer pairs of technology and is reflected in the number of hypotheses that could be supported for each PIP threat. Had more appropriate pairings been available, it is anticipated that the PIP threats would have yielded similar results to one another regarding their effect on initial technology trust.

The results of the factor analysis indicate emerging and non-emerging technologies should also be treated with different trust models, and that non-emerging technologies have an additional technology trust antecedent that has not been recognised before, called "data integrity," which does not exist for emerging technologies. This is in addition to McKnight et al. (2011)'s functionality, reliability and effectiveness test beliefs and is made up of the privacy-adapted instruments which were introduced for this research to capture the unique threat to privacy that emerging technologies represent compared to non-emerging technologies (Conger et al., 2013). Interestingly, this antecedent did not exist when measured

against emerging technologies, and each instrument item evenly splits with the corresponding technology trust dimension it was designed for.

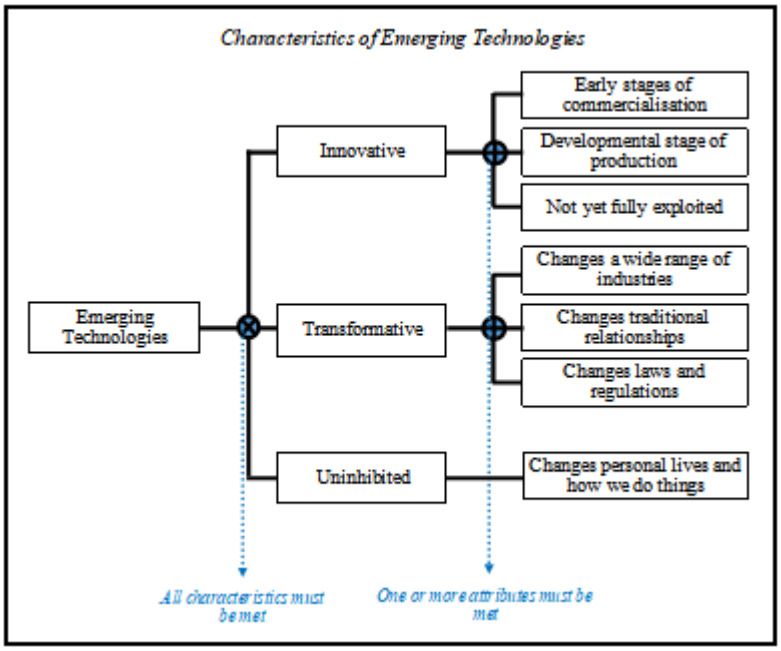
Lastly, this experiment indicates that all the covariates included in this research have a significant influence on each of the initial technology trust variables (functionality, effectiveness, reliability, structural assurance and situational normality). This appears consistent with existing research in the fields of technology trust and institutional-based trust.

4.2. Discussion & Future Directions

The purpose of this study was to address the research question: *What influences individuals to decide whether they trust emerging technologies without prior experience or knowledge of the technology?* Specifically, it sought to determine whether perceived threats to PIP influence individuals' initial trust in emerging technologies, finding causal evidence to support this. The results show that the characteristics of emerging technologies vary significantly, each offering a unique mix of PIP threats and trusting situations, and each representing different levels of emergence. This means researchers cannot rely on technologies to exclusively operationalise one PIP threat or represent emerging technologies in general. Therefore, future research is likely to find different results with potentially significant variation across technologies and their perceptions of emergence, PIP threats and technology trust beliefs because of the fluidity of technology development and innovativeness which future analyses would be based upon. McKnight et al. (2014) would seem to support this conclusion from their research, finding a "surprising" amount of variation in technology trust levels across the different technology groups they tested.

The emerging technology test framework was partially validated and the "innovative" characteristic was confirmed and new characteristics of "transformative" and "uninhibited" were introduced to replace the characteristics "revolutionary" and "disruptiveness," as shown in figure 5. These characteristics reported unexpected factors with the item for revolutionary loading with two items designed for disruptiveness. This factor was renamed "transformative" since each of these items represented indirect impacts of an emerging technology in society: including, changing individuals' personal lives in how they live and do things; the structure and practises of industries or the creating of new industries or causing the closure of others, forced by the introduction of the emerging technology; and the change of traditional relationships between buyers and sellers, the government and public or

Figure 4



domestic roles. The remaining item designed for disruptiveness related to an emerging technology's ability to change laws and regulations. This characteristic was renamed "uninhibited" to represent the evolutionary nature of emerging technologies which often develop, unchecked from regulation, and its subsequent need for regulatory restraint at times relating to the development, deployment, use and effects of a new emerging type of technology. Examples include the internet of things, autonomous vehicles, biotechnologies and the rapid development of cryptocurrencies. Unlike transformative, changes to laws and regulations do not occur gradually overtime but mark a point in time when the emerging technology is formally recognised for the transformative impact it has in society and the need to restrain its development or use or to attempt to manage its change effects. Although uninhibited scored an Eigenvalue below 1.00, and therefore excluded for use in the analysis of this thesis, it is possible the subject group used, and/or the New Zealand context, may have contributed to this result. In countries more technology focussed, including Europe and the United States, its likely individuals are more aware of advanced technology developments and their governing bodies anticipate and respond more quickly and efficiently than New Zealand which generally is more responsive to technologies and follows international regulatory trends. As result, it is possible that emerging technologies' characteristic of being uninhibited may be relevant in other contexts.

During the research process, a simple factor structure was discovered for Conger et al. (2013)'s PIP threats which are uniquely characterised by emerging technologies, which they

neither predicted nor theorised. These characteristics were further developed to account for two types of "ubiquity" not considered by Conger et al. (2013), thus including an additional feature which may threaten PIP. It was discovered that these PIP threats for emerging technologies can be classified into three groups; omnipotence, intrusiveness and invisibility. Omnipotence relates to a technology's physical and network ubiquity and programmability. Intrusiveness relates to a technology's invasiveness, its ability to collect information and wireless accessibility; and invisibility is a factor on its own. As technology continues to develop, these PIP threats will become more relevant over time as more technologies embody the characteristics of emerging technologies and become the new standard of technology. Although these technologies will eventually mature, and their "emergence" factor diminished, their threats to PIP will remain constant as they transition towards a non-emerging technology, even if their perceived threat may vary.

The experiment showed that emerging technologies present their own distinct mix of PIP threats based on their unique blend of characteristics. This was expected given the different technology features across experiment groups and the variance in technology trust found by McKnight et al. (2014) across different technology artefacts. However, the treatments were unable to communicate any primary PIP threat that was embodied by any one of the emerging technologies presented, with some emerging technologies representing similar levels of different PIP threats. Although significant mean differences could not be found with the control for each PIP threat, namely the lack of significant perceived invisibility in drones to compared to email, significant differences in PIP threats could be found between emerging technologies for each PIP threat. This illustrates that a PIP threat spectrum exists for intrusiveness, omnipotence and invisibility, and the degree of individuals' perceived threats to PIP will vary across technologies and individuals (Martin et al., 2015).

Two possible reasons exist for the lack of perceived invisibility in drones compared to email. Firstly, it is possible email already represents a high level of invisibility and was not an appropriate non-emerging technology to use as a benchmark given its intangible presence and widespread use. However, given that email is a widely used and trusted application, and has been around for over 30 years, this would argue that email would make a good benchmark indicator. Alternatively, it is possible individuals have a high threshold for perceived invisibility threats and this threat is anticipated, if not expected, by potential technology users. An observation of the current non-emerging technology landscape would suggest many

existing, non-emergent technologies are already relatively invisible, including email which continually receives, forwards and sends data without user direction. As such, many individuals might expect a certain degree of invisibility from any technology. Some might go as far as to say they purchase technologies because "they are able to be forgotten about" and can be trusted to act autonomously as part of its functionality, not recognising invisibility as a threat to their PIP (as theorised in section 2.6.1.3). An example might include a refrigerator adjusting its temperature when the door is left open, automatic transmission cars or digital TV recorders recording television shows at a specified time. Based on this argument, a high tolerance for PIP threats resulting from a technology's characteristics of invisibility suggests further research might prove invisibility has a weak significant influence on initial technology trust. However, despite this and the lack of evidence, it seems intuitive to suggest greater perceptions of invisibility would still cause a decrease in the perceived effectiveness of a technology. Highly invisible technologies should inspire suspicion in their ability to provide effective help and assistance when needed if they are perceived to be more concerned with collecting personal information. This would argue for H5b, relating to the effect of perceived PIP threats on effectiveness trust beliefs, which was unable to be supported in this study. Moreover, the ability of technologies to collect personal information arguably depends on their ability to act autonomously and be forgotten about so that individuals let down their privacy guards. The support for H5c, regarding the effect of invisibility on perceived reliability, supports this logic. It stands to reason a technology that is highly autonomous and able to be forgotten about should be considered to "operate consistently without failing."

McKnight et al. (2011) theorised initial technology trust was a product of an individual's technology trust beliefs and institutional-based trust beliefs. Overall, the experiment showed that perceived threats to PIP affect technology trust beliefs (i.e. perceived functionality, reliability and effectiveness) with perceived functionality and reliability decreasing with increased perceptions of each PIP threat. This may be because greater perceived threats to PIP suggest that a technology's functionality was built for the purpose of collecting personal information at the expense of relevant functionality for users. In addition, greater perceived threats to PIP may also suggest that a technology's reliability could be compromised due to the competing interests between users and entities collecting personal information through the technology artefact. As a result, these decreased initial technology trust in each of the emerging technologies, supporting H3, H4 and H5. Effectiveness was only found to be affected by intrusiveness and omnipotence, providing an argument that greater perceived PIP

threats may prevent technologies from acting when needed or required because they are more concerned with collecting personal information than providing effective help when needed.

An exploratory factor analysis of the instruments for functionality, reliability and effectiveness indicates the technology trust model by McKnight et al. (2011) is incomplete, at least with regard to non-emerging technology. The results suggest non-emerging technology has another antecedent from which users determine technology trust; "data integrity." Here, data integrity is the extent to which users believe a technology will act according to the best interests of its user's privacy, that it will not exploit or abuse its ability to collect or share personal information. By comparison, when these instruments are tested against emerging technologies, the data integrity antecedent no longer exists. Instead, the variable items split evenly across functionality, reliability and effectiveness as intended. This reflects the inherent threat to PIP emerging technologies have, and its lack of data integrity, due to their technical complexity which gives them characterises of invisibility, omnipotence and intrusiveness. This finding indicates data integrity beliefs do not have a positive relationship with beliefs in functionality, reliability or effectiveness for non-emerging technologies. While this result may seem unexpected, it is consistent with the belief that privacy threats are an unique characteristic common to all emerging technologies (Conger et al., 2013). This would suggest users are not expected to have significant variation in their perceived data integrity of emerging technologies, unlike non-emergent technologies, and that these concerns are more accurately captured in their beliefs of functionality, reliability and effectiveness.

The discovery that two different models for initial trust formation in technologies exist for emerging and non-emerging technologies suggests that different types of technology domains exist. Future research should further investigate this phenomenon to explore whether other variations of technology trust beliefs exist for other technology subclasses or to confirm whether the initial technology trust beliefs found for non-emerging technologies, with the use of data integrity, exist for other types of technologies.

This research produced limited evidence to suggest PIP threats affect institutional-based trust. By comparison to technology trust beliefs, only one institutional-based trust belief was found to have been affected by PIP threats, with perceived threats of intrusiveness affecting structural assurance. It was not affected by any other PIP threat. Moreover, no significant evidence was found to suggest that greater perceived threats to PIP will decrease perceived

situational normality. This result may have been a consequence of the wording of the instruments which were written differently from the other instruments and did not refer to the respective technologies in the treatment, but rather "new technologies I have not used before." This was worded on the basis that initial trust situations with emerging technologies are not likely to be easily generalisable due to their novelty and are more likely to be generalised to new technology trust situations. As result, this wording may have been too vague to collect reliable data as subjects had no specific technology artefact or class to compare their technologies to. It is also possible that the average age of subjects, 19.85 years old, was a factor. It is possible that younger individuals are generally more open minded to using various technologies, with greater anticipation for emerging technologies in the future. Thus, they may be more tolerant to situational *abnormality* and further research using a representative sample of the population will be necessary to further investigate this relationship. Despite this, the insignificant results are consistent with Li et al. (2008) who also found that no significant relationship between situational normality and new, unfamiliar technologies existed. This would suggest that perceived situational normality may not be relevant during initial technology trust formation at all and should be removed from the model originally proposed by McKnight et al. (2011). While their model is consistent with people-related trust literature, they themselves note that technology trust is unique because of its complex trust situation and the use of technology artefacts as a trust object. Consequently, this would provoke entirely different generalised expectancies which affect individuals' trust beliefs and their priorities (Bandura, 1997; Rotter, 1971; Rousseau et al., 1998) and would theoretically be most likely to have the greatest impact on situational normality, which includes generalised expectancies and strongly captured in McKnight et al. (2011)'s definition for situational normality.

People-related trust literature states individuals increase their reliance on perceived situational normality and perceived structural assurances when situations are new and ambiguous, and vice versa (Chen & Barnes, 2007; Li et al., 2008; McKnight & Chervany, 2001; Rousseau et al., 1998; Vance et al., 2008). However, only greater levels of intrusiveness and omnipotence were found to cause a decrease in perceived structural assurance and vice versa, and consequently institution-based trust, but invisibility could not be supported as having an impact. The reason for this may have been due to a lack of available data to compare group means for invisibility since a negative relationship between perceived structural assurances and perceived threats to personal information is consistent

with e-commerce literature and the results of the other two PIP threats reported here (Xin Luo et al., 2010; Smith et al., 2011).

It is possible that perceptions in structural assurance are strongly influenced by the type of technology proposed and its potential application, supporting the case that technology trust situations are highly contextual. In this experiment, the emerging technologies expected to have significant levels of structural assurance and situational normality were autonomous cars, drones and bionano sensors. While regulations and consumer protections often struggle to keep up with the constant developments in technology and the new, unique risks they present, the treatment for bionano sensors was placed in a medical context. Medical regulations and standards are often stringent and medical products usually undergo rigorous testing. Despite the inclusion of information to highlight the regulatory and safety issues of bionano sensors, it is possible trust in the structural assurances of the medical industry as a whole prevailed over the structural assurances of bionano sensors specifically. In fact, Pidgeon, Harthorn, Bryant, and Rogers-Hayden (2009) found the public was surprisingly unconcerned about nanotechnologies and the health risks they present and were more interested in the entities that would manage them. In addition, while drones may have sparked some contention in the legal courts over how to manage and regulate them, it seems the public may not have many concerns over drone technology since they tend to generalise drones to aviation technology, which are already regulated and widely used, according to Clothier, Greer, Greer, and Mehta (2015). Although Clothier et al. (2015) theorised that this neutrality was in part because of ignorance and a lack of knowledge about the capabilities of drones, this may partly explain the of lack structural assurance and situational normality effects despite scoring relatively highly across all PIP threats. Moreover, the autonomous vehicle industry currently lack uniform standards and independent regulatory bodies to ensure minimum quality and protection of consumers. The industry also is not bound by codes of confidentially. However, it is possible that individuals generalise autonomous vehicles to the human driven vehicle industry and impute their structural assurance and situational normality trust beliefs onto autonomous vehicles.

Consistent with other research, disposition to trust and disposition to technology trust, in the form of general faith in technology and technology trust stance, were found to have a significant impact on initial technology trust levels. This is consistent with people-related and e-commerce trust research which has found the propensity to trust affects the formation of

trust beliefs in the trust object and context (Chen & Barnes, 2007; McKnight et al., 2011; McKnight & Chervany, 2001; Rousseau et al., 1998; Vance et al., 2008; Wingreen & Baglione, 2005). Interestingly, this is contrary to Li et al. (2008)'s research in initial technology trust formation which found no significant results for the influence of individuals' general disposition to trust on technology trust beliefs. McKnight et al. (2011) did not consider the possible relationship with the general people-related disposition to trust in their model. However, their initial technology trust model supported the causal relationship between disposition to technology trust and technology trust beliefs which was consistent with findings found in the experiment.

Faith in humanity's benevolence, competence and integrity were all found to have a significant effect on initial technology trust and would appear to support the belief that faith in humanity may be used as a proxy for vendor-based trust when vendors are unknown. It also supports the hypotheses and initial technology trust model proposed by Li et al. (2008) that they were unable to support. This was theorised (in section 2.7.2) to be because of a poor choice of technology artefact in their research (a national identity system). These results suggest more research could be valuable in determining whether faith in humanity can be used as an effective proxy for vendor-based trust. However, these results are consistent with prior research which has identified that vendor-based trust affects both technology trust and institutional-based trust (McKnight et al., 2011; Wingreen & Baglione, 2005), and therefore initial technology trust.

The perceived safety of the wider economic environment was also found to have a significant influence on all the initial technology trust variables and was theorised to be an antecedent of faith in humanity as a proxy for vendor-based trust. This was not considered by Mayer et al. (1995), McKnight and Chervany (2001), Rotter (1971) or Rousseau et al. (1998) and could not be found to be included in any trust research in Information Systems or Psychology literature, and was only found in rare instances in the Economics literature to some degree (Burchell & Wilkinson, 1997). The significant effect of the economic environment is relatively novel and unexpected within the wider literature and should therefore be considered in future research to validate the findings in this research.

Subjective norms had a significant impact on initial technology trust levels. The relationship between subjective norms and initial technology trust is particularly interesting. For the

purposes of this research, subjective norms were tested as a measure of predicted popularity and the social pressures an individual might face to conform to the acceptance of technology risks and PIP threats. Subjective norms has received little attention in technology or people-related trust research, although studies by Lee, Lee, and Tan (2012) and Li et al. (2008) have found a significant positive relationship between subjective norms and technology trust. The consistency of these results suggest subjective norms needs to be explored in greater depth in trust research as it may be a relevant antecedent to trust. The impact of social hype is therefore also likely to be relevant. A significant positive relationship between subjective norms and initial familiarity suggests individuals with more knowledge about a technology are more likely to perceive it as being desirable by society.

The initial familiarity of a technology was also found to have a significant relationship on all the initial technology trust variables. This was expected based on Gefen (2000) who conducted an in-depth investigation exploring the relationship between familiarity and trust in the context of e-commerce. A positive relationship between initial familiarity of a technology and initial technology trust would indicate that greater initial knowledge or familiarity of a technology reduces uncertainty and risk in trust situations. This is consistent with the belief that initial trust formation is a cognitive process and individuals will depend on second-hand knowledge, similar experiences and initial preconceived beliefs in forming initial trust beliefs (Li et al., 2008; McKnight et al., 1998; McKnight et al., 2014; Rousseau et al., 1998). Further to this, McKnight et al. (2011) found a negative relationship between knowledge and institutional-based trust, suggesting individuals may have preference to rely on first or second-hand knowledge instead of individual trust beliefs and perceptions when forming initial trust beliefs. Initial familiarity was found to have a negative correlation with general disposition to trust which would also appear to support this argument.

4.3. Key Limitations

Despite the "gold standard" experiments can be heralded as for research (Bhattacherjee, 2012), limitations exist in any research. In this research, limitations relate to its methodology, subject group, measurement, instrument design, control conditions, quantitative research nature and implicit assumptions. Moreover, experiments are unable to determine to what extent any relationship is or is not truly significant (Mook, 1983). Whilst time would not be an issue in the ideal world, it was a practicality which must be taken into account; thus, limiting the scope and design of the research and preventing the acquisition of more data to

supplement existing data. It was also dependant on other external factors regarding academic and ethical requirements and approvals.

Experiments often lack external validity. This means this research may not be able generalisable to the population, however its primary purpose was to test whether or not the proposed variables affect initial trust formation in emerging technologies. According to Mook (1983), this means controls for external validity are not as applicable as it would be for a field survey, survey or case study. This can limit the generalisability of results and the extent to which relationships may or may not be significant cannot be gauged reliably. However, the absence of strong external validity controls does not discount experiment research results; the purpose of experiments is to discover whether something can occur under certain conditions or to contribute to understandings of a current phenomenon (Mook, 1983).

This research used a subject group drawn from university students. While experiments do not require a representative sample (Mook, 1983), a possibility exists that this had a significant impact on results because the education of subjects may have resulted in a more critical evaluation of emerging technologies regarding trust and perceived privacy risks. The age of tertiary students also tends to range from eighteen to their mid-twenties. It is possible that they might have a greater disposition to technology trust than other age groups due to greater familiarity and use of technologies. This means that some trust factors which might be prevalent in other demographic groups did not exist in the subject group used and will not be reflected in the data collected. Moreover, the exclusion of cultural, gender and socio-economic class may also limit research results. According to Xin Luo et al. (2010) these factors which are likely to impact technology trust. The exclusion of these factors purports to assume that that these are not relevant variables which are capable of influencing individuals, when this is unlikely to be the case.

Trust is an intangible, innately human construct making it difficult to measure. Therefore, any attempt to measure trust levels will be difficult to do reliably. The limited range of independent variables is also unlikely to capture all the relevant factors in determining trust levels, especially with perceived threats to PIP. Consequently, while this research may confirm a causal relationship with some variables it is unlikely to capture them all. The instrument design also has limitations regarding the effective capture of emerging technology characteristics and the use of only one related PIP instrument for each of McKnight et al.

(2011)'s initial technology trust variables, which then formed the "data integrity" antecedent for non-emerging technologies. Given that a range of technologies were used in the experiment, it is unlikely they will exhibit all of those characteristics at equal levels or that other technologies will hold the same mix of characters. Moreover, this study showed that emerging technologies can embody multiple PIP threats to varying degrees and it is difficult to identify one emerging technology which strongly embodies one PIP significantly more than a range of others. This limits the external validity of this research and comparability of results with other technologies, especially when considering a technology's emergence is very time and context sensitive. Moreover, the inclusion requirements for technologies to be "emergent" according to the criteria developed in section 2.5.1 with an appropriate assortment of online news articles also limited the use of relevant technologies for experimentation.

The quantitative nature of this research brings its own limitations. It assumes a positivist ontology and epistemology which may contradict the fundamental concept of trust which is neither tangible, directly observable nor measurable. It seeks to simplify what may be a complex, irrational and unpredictable phenomenon, ignoring the pressures of social convention, culture and other relationships with socio-economic factors which further limit this study. Furthermore, positivists also tend to assume that all people are the same, although they each have their own dispositions, perceptions, priorities and goals.

Lastly, this research assumes all individuals are users of technology and using any technology is optional i.e. they are not demanded by situations such as survival or are forced or controlled. Only in this context, can the results of the experiment be considered valid or reliable.

4.4. Next Steps

Based on the many significant findings of this experiment, it was decided to further develop and test the initial technology trust model that was theorised in section 2 and hypotheses H1 to H5. The purpose of this was to try and make better sense of the experiment results and its significant covariate results, providing context from which they might exist. Therefore, an investigation of the supplementary set of effects on perceived threats to PIP and initial technology trust was initiated and the second phase of this research was proposed using PLS-SEM. PLS-SEM is recommended for exploratory theory development and strong predictive

validity to understand casual relationships between variables (Hair et al., 2011; Hair et al., 2014; Mook, 1983; Ringle et al., 2012). This secondary study not originally intended, but the likelihood of discovering new, significant findings which could be valuable to both technology, trust and privacy research was promising. PLS-SEM analyses also had the added benefit that it would transform non-normal data using central limit theorem to enable generalisability and external validity (Hair et al., 2011; Hair et al., 2014; Mook, 1983; Ringle et al., 2012; Wong, 2013).

An alternative method to expand this research was to modify and reperform the experiment on a wider scale with a more representative sample of the population to confirm current findings with greater external validity. However, exploring the supplementary effects of the covariates and better developing the initial trust model proposed was predicted to be a more worthwhile contribution to knowledge. It was also truer to the original intentions and motivations of this research which was to explore *what influences individuals to decide whether they trust emerging technologies without prior experience or knowledge of the technology?*

SECTION 5. STUDY 2 – MULTI-STAGE MODELLING WITH PLS-SEM

5.1. Results & Analysis

This section describes the results of the PLS-SEM modelling procedures. It first examines the proposed initial technology trust model for emerging technology, and whether the hypotheses can be accepted or rejected, using the data collected from the primary experimental procedure and the emerging technology cases. It then examines the results for the same proposed model for initial technology trust using the data from the non-emerging technology group. This would enable a comparison of initial trust formation for emerging and non-emerging technologies. This follows from the finding from the primary experiment, and the discovery of the data integrity antecedent for non-emerging technologies, that emerging and non-emerging technologies are treated differently by individuals in the formation of initial technology trust beliefs.

5.1.1. INITIAL TECHNOLOGY TRUST IN EMERGING TECHNOLOGIES MODEL

The initial technology trust model in emerging technologies was analysed using 228 cases from the primary experiment. This only included the data groups for emerging technologies: 3D printing, autonomous cars, bionano sensors and drones. Bootstrapping procedures were applied where appropriate using 500 subsamples, bias-corrected and accelerated confidence interval method and two tailed tests with a significance level of 0.10, which is recommended for exploratory PLS-SEM theory development (Garson, 2016; Lowry & Gaskin, 2014). Procedures also used a path weighting scheme of 300 maximum iterations and a stop criterion of 10^{7}.

5.1.1.1. Outer Model

It is important to determine the outer model reliability of models analysed using PLS-SEM as this directly impacts the reliability of the inner model (Chin, 1998; Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014; Ringle et al., 2012). The primary experimental procedure demonstrated the reliability and internal validity of instrument items for each variable. It also illustrated sufficient discriminate and convergent validity between constructs. As such, this section aims to confirm outer model reliability of the initial technology trust model in accordance with results found for the primary experimental procedure. This is because the complexity of the model (using second and third order latent variables and a mixture of formative and reflective items) means measures for evaluating outer model reliability become

less effective and therefore cannot be relied upon as much as simpler PLS-SEM models (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014; Henseler, Ringle, & Sarstedt, 2015).

1.Third Order Latent Variables

Initial technology trust is a third order latent variable, measured by technology trust and institutional-based trust. In turn, technology trust was measured by functionality, reliability and effectiveness, and institutional-based trust was measured by structural assurance and situational normality. These were measured as reflective constructs and assessed by their outer indicator loadings (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014). The results were consistent with the primary experimental procedure and sufficient outer model reliability was determined for all variable items with $p < 0.01$. All significant outer indicator loadings were above the 0.40 minimum, except for SN3 regarding situational normality, and many indicators also above the 0.70 threshold for confirmatory research (Chin, 1998; Garson, 2016; Hair et al., 2014). This is significant given the exploratory nature of this study. Outer indicator loadings are reported in table 21

.

Table 21

Third Order Outer Indicator Loadings for Emerging Technologies

	Technology Trust			Institutional Trust	
item	F	R	E	SA	SN
F1	**0.80**				
F2	**0.80**				
F3	**0.80**				
F4	**0.80**				
F5	**0.43**				
R1		**0.65**			
R2		**0.73**			
R3		**0.81**			
R4		**0.87**			
R5		**0.64**			
E1			**0.87**		
E2			**0.86**		
E3			**0.56**		
E4			**0.73**		
SA1				**0.78**	
SA2				**0.83**	
SA3				**0.81**	
SA4				**0.87**	
SN1					**0.82**
SN2					**0.80**
SN3					**--**
SN4					**0.82**
SN5					**0.53**

F = Functionality, R = Reliability, E = Effectiveness, SA = Structural Assurance, SN = Situational Normality
Not bolded: p <0.10
Bolded: p <0.01

Outer VIF factors for functionality, reliability and effectiveness ranged from 1.09 to 2.04, 1.38 to 2.36, and 1.36 to 2.65 respectively. Outer VIF factors for structural assurance and situational normality ranged from 1.83 to 2.47 and 1.04 to 2.26. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011). This means multicollinearity is unlikely to exist and outer items are strongly correlated to their respective variables, indicating predictive validity.

The third order model for technology trust converged in 16 iterations and the model for institutional-based trust converged in 17 iterations. These are both well below the 300 maximum iterations allowed for exploratory research, indicating a high degree of outer model internal reliability (Garson, 2016). Overall, sufficient outer model reliability for technology trust and institutional-based trust can be ascertained.

2. Second Order Latent Variables

Perceived threats to PIP were measured using formative instrument items. Because indicator loadings cannot be used to reliability evaluate formative constructs (Garson, 2016), an examination of item cross loadings was used to confirm discriminant validity and outer model reliability instead (Hair et al., 2014). The results were consistent with those found for the primary experimental procedure. All variable items loading higher on their intended construct than their cross loadings with other constructs, thus sufficient outer model reliability was determined (Hair et al., 2014).

Emerging technologies, faith in humanity and disposition to technology trust were second order latent variables measured with reflective indicators. Consequently, they were measured by their outer indicator loadings (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014). The results were consistent with the primary experimental procedure and sufficient outer model reliability was determined for all second order variable items with $p < 0.01$ (Garson, 2016; Hair et al., 2014). All outer indicator loadings were above the 0.40 minimum threshold. Most indicators were also above the 0.70 threshold for confirmatory research, as shown in table 22, which is significant given the exploratory nature of this study. The exceptions to this related to one indicator in the variables for faith in general technology and technology trust stance, which are both antecedents for disposition to technology trust.

Table 22

Second Order Outer Indicator Loadings for Emerging Technologies

	Emerging Technology		Faith in Humanity			Disposition to Tech. Trust	
item	Inn	Tra	Ben	Comp	Int	FGT	TTS
ET1	**0.81**						
ET2	**0.82**						
ET3	**0.91**						
ET4		**0.91**					
ET5		**0.89**					
ET6		**0.90**					
FH1			**0.78**				
FH2			**0.84**				
FH3			**0.67**				
FH4				**0.82**			
FH5				**0.86**			
FH6				**0.82**			
FH7					**0.76**		
FH8					**0.77**		
FH9					**0.85**		
DT1						**0.65**	
DT2						**0.94**	
DT3						**0.80**	
DT4						**0.71**	
DT5							**0.59**
DT6							**0.89**
DT7							**0.85**

Inn = Innovative, Tra = Transformative, Ben = Benevolence, Comp = Competence, Int = Integrity, FGT = Faith in General Technology, TTS = Technology Trust Stance
Not bolded: p <0.10
Bolded: p <0.01

Outer VIF factors for innovativeness and transformative ranged from 1.31 to 1.51 and 1.81 to 2.08 respectively. Outer VIF factors for benevolence, competence and integrity were from 1.12 to 1.89, 1.53 to 1.97, and 1.48 to 1.69. Lastly outer VIF factors for faith in general technology and technology trust stance were from 1.29 to 2.74 and 1.12 to 1.61. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011). This means multicollinearity does not exist and these outer items are strongly correlated to their respective variables, indicating predictive validity.

The second order path model converged within 133 iterations. This is well below the 300 maximum iterations allowed for exploratory research, indicating a high degree of outer model internal reliability (Garson, 2016). Overall, sufficient outer model reliability for perceived threats to PIP, emerging technologies, faith in humanity and disposition to technology trust can be ascertained.

3. First Order Latent Variables

Disposition to trust generally, subjective norms, the economic environment and initial familiarity were first order latent variables measured with reflective indicators. Consequently, they were measured by their outer indicator loadings (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014), as reported in table 23. The results were consistent with those found for the primary experimental procedure and sufficient outer model reliability was determined for all variable items with $p < 0.01$ (Garson, 2016; Hair et al., 2014). All outer indicator loadings were above the 0.40 minimum threshold for exploratory research, as well as the 0.70 threshold for confirmatory research. Subjective norms, the economic environment and initial familiarity yielded outer loadings of 1.00. This might indicate multicollinearity problems. However, these variables were measured with one scale item each which, in this case, is expected.

Table 23

1st Order Outer Indicator Variables for Emerging Technologies

Item	Disp. to Trust	Subj. Norms	Econ. Environ.	Initial Fam.
D1	**0.83**			
D2	**0.83**			
D3	**0.90**			
D4	**0.76**			
S1		**1.00**		
E1			**1.00**	
IN1				**1.00**

Not bolded: p < 0.10
Bolded: p < 0.01

Outer VIF factors ranged from 1.86 to 2.74 for disposition to trust generally and 1.00 for subjective norms, the economic environment and initial familiarity. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011). This means multicollinearity is unlikely to exist and these outer items are strongly correlated to their respective variables, indicating predictive validity.

The first order path model converged within 2 iterations, well below the 300 maximum iterations allowed for exploratory research, indicating a high degree of reliability (Garson, 2016). Overall, sufficient outer model reliability for initial technology trust can be ascertained.

5.1.1.2. Inner Model

1. Perceived Threat to PIP

Emerging technology artefacts, faith in humanity and subjective norms were found to have significant predictive effect on perceived PIP threats, explaining 19% of the variance in perceived PIP threats, with $R^2 = 0.19$ and $p < 0.01$ (Hair et al., 2011; Ringle & Sarstedt, 2016; Ringle et al., 2012). This is considered a weak predictive effect of the combined variables on perceived threats to PIP (Cohen, 1992; Garson, 2016; Hair et al., 2011).

Path coefficients measure the strength of relationship between variables, between -1 and +1 (Garson, 2016; Hair et al., 2014; Wong, 2013). Emerging technology artefacts and subjective norms had significant path coefficients to perceived threats to PIP of 0.27 and 0.24 respectively, and $p < 0.01$. This means a significant weak to moderate positive causal relationship exists from emerging technology characteristics and subjective norms to perceived PIP threats. Faith in humanity had a path coefficient of 0.11 with $p = 0.11$, suggesting it may not affect perceived threats to PIP.

f^2 tests the effect size of an independent variable as the incremental change in a dependant variable (Ringle et al., 2012). It effectively measures the change in R^2 caused by including an independent variable in a model as opposed to excluding it (Esposito Vinzi, 2010). Emerging technologies, faith in humanity and subjective norms generated f^2 values of 0.08, 0.01 and 0.07 respectively, which suggests they each have a small effect size on perceived PIP threats (Chin, 1998; Cohen, 1992; Esposito Vinzi, 2010). This indicates emerging technology characteristics have an incremental change effect on perceived PIP threats equal to 8%, faith in humanity of 1% and subjective norms of 7% (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014; Ringle et al., 2012).

The f^2 value for emerging technologies was significant with $p = 0.09$, although faith in humanity and subjective norms were not significant when using a significance level of $p = 0.10$ for exploratory PLS-SEM research (Garson, 2016). Consequently, the effect size of these variables on perceived threats to PIP cannot be estimated confidently. However, that is not to suggest faith in humanity and subjective norms do not have a predictive effect on perceived threats to PIP. This was evidenced in the path-coefficients, which was significant for emerging technologies and subjective norms. Instead, it suggests if faith in humanity and subjective norms were removed from the model one at a time, while holding all other

variables, then we are unlikely to see a significant change in the R^2 of perceived threats to PIP. Therefore, these variables may be less relevant in a broader context when all other variables are included. Consequently, a post hoc power analysis for faith in humanity and subjective norms was performed, reporting a power of 0.32 and 0.97 respectively with a 95% confidence level. Statistical power exists when power is equal or greater than 0.80 (Chin, 1998; Cohen, 1988; Faul et al., 2009; Faul et al., 2007; Miguel & Mikko, 2015; Peng & Lai, 2012). This indicates that there is insufficient statistical power to reliably determine whether the faith in humanity effect size exists. On the other hand, sufficient power existed within the data to measure the effect size of subjective norms within which the PLS-SEM parameters were set for this research.

The inner VIF factors for emerging technology artefacts, faith in humanity and subjective norms ranged from 1.03 to 1.08. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011). This indicates the model does not have multicollinearity and that these variables are strongly correlated to perceived threats to PIP. This means they can be used to confidently predict perceived threats to PIP with a strong level of predictive accuracy, indicating predictive validity (Garson, 2016; Hair et al., 2011).

Consequently, these results support Hb and Hg. However, there is insufficient evidence to support He at this time. The PLS-SEM results for perceived threats to PIP are summarised in table 23.

Table 24

Perceived Threats to PIP Statistics for Emerging Technologies

		Mean	S.D.	t-value	5%	95%	p-value
R^2							
Perceived Threat to PIP	**0.19**	**0.20**	**0.05**	**3.66**	**0.12**	**0.29**	**0.00**
f^2							
Emerging Technology Artefact > Perceived Threat to PIP	**0.08**	**0.09**	**0.05**	**1.70**	**0.02**	**0.17**	**0.09**
Faith in Humanity > Perceived Threat to PIP	0.01	0.02	0.02	0.71	0.00	0.06	0.47
Subjective Norms > Perceived Threat to PIP	0.07	0.08	0.05	1.41	0.01	0.16	0.16
Path Coefficients							
Emerging Technology Artefact > Perceived Threat to PIP	**0.27**	**0.27**	**0.07**	**3.67**	**0.13**	**0.37**	**0.00**
Faith in Humanity > Perceived Threat to PIP	0.11	0.11	0.07	1.71	-0.01	0.21	0.11
Subjective Norms > Perceived Threat to PIP	**0.24**	**0.24**	**0.08**	**3.10**	**0.10**	**0.36**	**0.00**
Inner VIF Factors							
Emerging Tech. Characteristics > Perceived Threat to PIP	1.08	--	--	--	--	--	--
Faith in Humanity > Perceived Threat to PIP	1.03	--	--	--	--	--	--
Subjective Norms > Perceived Threat to PIP	1.09	--	--	--	--	--	--

Bolded: $p < 0.10$

2. Faith in Humanity

The perceived safety of the economic environment was found to have significant predictive effect on faith in humanity, explaining 17% of the variance in faith in humanity, with R^2 = 0.17 and p = 0.01 (Hair et al., 2011; Ringle & Sarstedt, 2016; Ringle et al., 2012). This is considered a weak predictive effect (Cohen, 1992; Garson, 2016; Hair et al., 2011).

Path coefficients measure the strength of relationship between variables, between -1 and +1 (Garson, 2016; Hair et al., 2014; Wong, 2013). Perceived safety of the economic environment had a significant path coefficient to faith in humanity of 0.41, with $p < 0.01$. This shows a significant moderate positive causal relationship exists between the perceptions of the economic environment and faith in humanity.

The economic environment generated a f^2 of 0.21, which suggests it has a moderate effect size on perceived PIP threats (Chin, 1998; Cohen, 1992; Esposito Vinzi, 2010). This would indicate an individual's perceptions of the economic environment from which they might encounter an emerging technology will have an incremental change effect on faith in humanity of 21% (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014; Ringle et al., 2012). This f^2 statistic was significant at p = 0.05, less than the significance level of p = 0.10 for exploratory PLS-SEM research (Garson, 2016). Consequently, the effect size of this variables on faith in humanity can be estimated confidently and suggests the exclusion of the economic environment from the model would cause a significant change in R^2. This strengthens the claim that the economic environment and faith in humanity have a strong relationship.

The inner VIF factor for the economic environment was 1.00, indicating perfect collinearity. This means an individual's perceptions about the economic environment can be used to confidently predict faith in humanity with a strong level of predictive accuracy (Garson, 2016; Hair et al., 2011).

Consequently, these results support Hi. The PLS-SEM results for faith in humanity are summarised in table 24.

Table 25

Faith in Humanity Statistics for Emerging Technologies

		Mean	S.D.	t-value	5%	95%	p-value
R^2							
Faith in Humanity	**0.17**	**0.17**	**0.07**	**2.60**	**0.07**	**0.30**	**0.01**
f^2							
Economic. Environ. > Faith in Humanity	**0.21**	**0.22**	**0.10**	**2.01**	**0.08**	**0.40**	**0.05**
Path Coefficients							
Economic Environ. > Faith in Humanity	**0.41**	**0.41**	**0.08**	**5.2**	**0.28**	**0.053**	**0.00**
Inner VIF Factors							
Economic Environ. > Faith in Humanity	1.00	--	--	--	--	--	--

Bolded: $p < 0.10$

3. Initial Technology Trust in Emerging Technologies

Perceived threats to PIP, faith in humanity, initial familiarity, disposition to technology trust and disposition to trust generally were found to have a significant predictive effect on initial technology trust in emerging technologies, explaining 38% of its variance, with $R^2 = 0.38$ and $p < 0.01$ (Hair et al., 2011; Ringle & Sarstedt, 2016; Ringle et al., 2012). This is considered a weak to moderate predictive effect of the combined variables (Cohen, 1992; Garson, 2016; Hair et al., 2011).

Perceived threats to PIP, faith in humanity, subjective norms, initial familiarity, disposition to technology trust and disposition to trust generally had significant path coefficients to initial technology trust in emerging technologies of 0.42, 0.12, 0.12, 0.11, 0.12 and 0.16 respectively. Therefore, small to moderate positive causal relationships exists from faith in humanity, subjective norms, initial familiarity, disposition to technology trust and disposition to trust generally to initial technology trust in emerging technologies (Cohen, 1992; Esposito Vinzi, 2010). Perceived threats to PIP had a path coefficient of 0.42 ($p < 0.01$), suggesting it has a moderate to strong relationship with initial technology trust in emerging technologies, consistent with the results of the primary experiment (Cohen, 1992; Esposito Vinzi, 2010).

f^2 tests the effect size of an independent variable as the incremental change in a dependant variable (Ringle et al., 2012). Faith in humanity, subjective norms, initial familiarity and disposition to technology trust each generated f^2 values of 0.02. Disposition to trust generally generated an f^2 value of 0.04. These results indicate each of these variables have a small effect size on initial technology trust in emerging technologies (Chin, 1998; Cohen, 1992; Esposito Vinzi, 2010). This suggests initial technology trust in emerging technologies will have an incremental change effect of 2% for each change in faith in humanity, subjective norms, initial familiarity and disposition to technology trust, and a change effect size of 4%

for changes in disposition to trust generally (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014; Ringle et al., 2012). Interestingly, these variables all yielded non-significant f^2 statistics when using a significance level of $p = 0.10$ for exploratory PLS-SEM research, with $p = 0.19$ to 0.44 (Garson, 2016). This means the effect size of each of these variables on initial technology trust in emerging technologies cannot be estimated confidently. Despite this, and consistent with the primary experimental procedure, perceived threats to PIP were found to have a small to moderate to high effect size on initial technology trust with $f^2 = 0.23$ (Cohen, 1988; Esposito Vinzi, 2010). This was significant with $p = 0.01$, well below the significance level of $p = 0.10$ for exploratory PLS-SEM research (Garson, 2016), and suggests initial technology trust in emerging technology trust has an incremental change effect of 23% for changes in initial technology trust.

Considering the non-significant f^2 results, post hoc power analyses were performed with 95% confidence levels. Faith in humanity, initial familiarity, subjective norms and disposition to trust had a power of 0.56 each, less than the recommended power of 0.80, which indicates insufficient power exists to reliably determine if an effect size on initial technology trust in emerging technology exists (Chin, 1998; Cohen, 1988; Faul et al., 2009; Faul et al., 2007; Miguel & Mikko, 2015; Peng & Lai, 2012). On the other hand, sufficient power existed within the data to measure the effect size of disposition to technology trust within which the PLS-SEM parameters were set for this research, reporting a power of 0.85 (Chin, 1998; Cohen, 1988; Faul et al., 2009; Faul et al., 2007; Miguel & Mikko, 2015; Peng & Lai, 2012).

These results suggest only the exclusion of perceived threats to PIP from the model, will cause a significant change in R^2. In other words, only perceived threats to PIP have a pronounced effect size on initial technology trust in emerging technologies. If faith in humanity, familiarity, subjective norms, disposition to technology trust or disposition to trust in general were removed from the model one at time while holding all other variables, then we are unlikely to see a significant change in R^2. This does not suggest these variables are not important without a significant predictive effect on initial technology trust, this was already evidenced by the significant path-coefficient. However, they may be less relevant in the broader context when all other variables are considered. Suffice to say, the significant f^2 for perceived threats to PIP of 0.23 reconfirms the salient relationship between perceived threats to PIP and initial technology trust identified in the primary experiment.

The inner VIF factors of the initial technology trust model for perceived threats to PIP, faith in humanity, initial familiarity, subjective norms, disposition to technology trust and disposition to trust generally ranged from 1.05 to 1.46. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011). This indicates the model does not have multicollinearity and that these variables are strongly correlated to initial technology trust in emerging technologies. Therefore, they can be used to confidently predict initial technology trust in emerging technologies with a strong level of predictive accuracy, indicating predictive validity (Garson, 2016; Hair et al., 2011).

Table 26

Initial Technology Trust Statistics for Emerging Technologies

		Mean	S.D.	t-value	5%	95%	p-value
R^2							
Initial Tech. Trust in Emerging Tech.	**0.38**	**0.40**	**0.05**	**7.81**	**0.12**	**0.29**	**0.00**
f^2							
Perceived Threats to PIP > Initial Tech. Trust in Emerging Tech.	**0.23**	**0.24**	**0.10**	**2.56**	**0.12**	**0.40**	**0.01**
Faith in Humanity > Initial Tech. Trust in Emerging Tech.	0.02	0.02	0.02	0.77	0.02	0.18	0.19
Initial Familiarity > Initial Tech. Trust in Emerging Tech.	0.02	0.02	0.02	0.96	0.00	0.06	0.34
Subjective Norms > Initial Tech. Trust in Emerging Tech.	0.02	0.03	0.03	0.97	0.00	0.08	0.33
Dispo. to Tech Trust > Initial Tech. Trust in Emerging Tech.	0.02	0.02	0.02	0.84	0.00	0.09	0.40
Dispo. to Trust Generally > Initial Tech. Trust in Emerging Tech.	0.04	0.04	0.03	1.30	0.00	0.09	0.20
Path Coefficients							
Perceived Threats to PIP > Initial Tech. Trust in Emerging Tech.	**-0.42**	**-0.43**	**0.07**	**6.28**	**0.31**	**0.54**	**0.00**
Faith in Humanity > Initial Tech. Trust in Emerging Tech.	**0.12**	**0.13**	**0.07**	**1.75**	**0.01**	**0.25**	**0.08**
Initial Familiarity > Initial Tech. Trust in Emerging Tech.	**0.11**	**0.11**	**0.05**	**2.01**	**0.02**	**0.20**	**0.05**
Subjective Norms > Initial Tech. Trust in Emerging Tech.	**0.12**	**0.12**	**0.07**	**1.72**	**0.01**	**0.23**	**0.09**
Dispo. to Tech Trust > Initial Tech. Trust in Emerging Tech.	**0.12**	**0.15**	**0.07**	**0.18**	**0.01**	**0.24**	**0.01**
Dispo. to Trust Generally > Initial Tech. Trust in Emerging Tech.	**0.16**	**0.15**	**0.06**	**2.65**	**0.06**	**0.25**	**0.08**
Inner VIF Factors							
Perceived Threat to PIP > Initial Tech. Trust in Emerging Tech.	1.15	--	--	--	--	--	--
Faith in Humanity > Initial Tech. Trust in Emerging Tech.	1.46	--	--	--	--	--	--
Initial Familiarity > Initial Tech. Trust in Emerging Tech.	1.05	--	--	--	--	--	--
Subj. Norms > Initial Tech. Trust in Emerging Tech.	1.17	--	--	--	--	--	--
Dispo. to Tech. Trust > Initial Tech. Trust in Emerging Tech.	1.42	--	--	--	--	--	--
Dispo. to Trust Generally > Initial Tech. Trust in Emerging Tech.	1.11	--	--	--	--	--	--

Bolded: $p < 0.10$

These results provide sufficient evidence to support Ha, Hc, Hd, Hf, Hh and Hj. The PLS-SEM results for initial technology trust are summarised in table 25.

5.1.1.3. Measurement of Fit

Overall, the path model for initial technology trust in emerging technologies can be considered to have measurement of fit, despite several of the f^2 statistics being moderate to high, but not significant. The path coefficient of all relationships, except faith in humanity to perceived threats to PIP, were positive and significant, indicator items loaded correctly on their intended constructs and the first order model achieved convergence in 2 iterations.

Further, multicollinearity was not present in the outer model or inner model, giving confidence to conclude the initial technology trust model is reasonably accurate and holds predictive validity.

5.1.1.4. Interaction Effects

Interaction effects were tested for each path using the product indicator calculation method, significance level of 0.10 and biased corrected confidence levels. Almost all moderating variables tested generated low and insignificant results. However, initial familiarity was found to have a significant negative interaction effect of -0.13 ($p = 0.03$) on the path from perceived threats to PIP to initial technology trust. Table 27 reports the interaction effects produced by each variable. These interaction effects were measured from within the emerging technology model. Multigroup moderation effects will be measured in section 5.1.2 with the non-emerging technology analysis.

Table 27

Interaction Effects of Variables in Initial Trust in Emerging Technologies Model

		S.D.	t-value	5%	95%	p-value
Emerging Tech. > Perceived Threat to PIP						
Faith in Humanity	-0.01	0.09	0.08	-0.14	0.15	0.93
Subjective Norms	0.09	1.16	0.25	-0.09	0.21	0.25
Faith in Humanity > Perceived Threat to PIP						
Subjective Norms	-0.01	0.09	0.11	-0.16	0.14	0.92
Subjective Norms > Perceived Threat to PIP						
Faith in Humanity	-0.01	0.09	0.11	-0.16	0.14	0.92
Perceived Threat to PIP > Initial Tech. Trust						
Dispo. to Trust Generally	-0.08	0.07	1.17	-0.19	0.03	0.24
Dispo. to Tech. Trust	0.03	0.09	0.27	-0.11	0.19	0.79
Faith in Humanity	-0.04	0.08	0.47	-0.18	0.10	0.64
Initial Familiarity	**-0.13**	**0.06**	**2.16**	**-0.22**	**-0.03**	**0.03**
Subjective Norms	-0.02	0.06	0.24	-0.12	0.10	0.81
Dispo. to Trust Generally > Initial Tech. Trust						
Dispo. to Tech. Trust	-0.02	0.08	0.21	-0.17	0.09	0.84
Faith in Humanity	0.02	0.08	0.31	-0.08	0.17	0.76
Initial Familiarity	0.00	0.07	0.05	-0.09	0.13	0.96
Perceived Threat to PIP	-0.08	0.08	0.94	-0.22	0.05	0.35
Subjective Norms	-0.06	0.07	0.89	-0.19	0.03	0.37
Dispo. to Tech. Trust > Initial Tech. Trust						
Dispo. to Trust Generally	-0.02	0.07	0.28	-0.16	0.08	0.78
Faith in Humanity	-0.01	0.05	0.18	-0.10	0.08	0.86
Initial Familiarity	-0.02	0.07	0.36	-0.14	0.08	0.72
Perceived Threat to PIP	-0.03	0.07	0.37	-0.13	0.11	0.71
Subjective Norms	0.03	0.06	0.45	-0.10	0.11	0.66
Faith in Humanity > Initial Tech. Trust						
Dispo. to Trust Generally	0.04	0.08	0.57	-0.09	0.16	0.57
Dispo. to Tech. Trust	-0.03	0.06	0.58	-0.12	0.07	0.57
Initial Familiarity	-0.05	0.08	0.62	-0.19	0.07	0.54
Perceived Threat to PIP	-0.06	0.07	0.94	-0.16	0.06	0.35
Subjective Norms	-0.05	0.08	0.65	-0.19	0.10	0.52
Subjective Norms > Initial Tech. Trust						
Dispo. to Trust Generally	-0.08	0.07	1.26	-0.19	0.03	0.21
Dispo. to Tech. Trust	0.05	0.06	0.83	-0.06	0.12	0.41
Faith in Humanity	-0.08	0.08	1.01	-0.20	0.06	0.32
Initial Familiarity	-0.05	0.05	0.97	-0.12	0.04	0.33
Perceived Threat to PIP	-0.05	0.06	0.82	-0.14	0.05	0.42
Familiarity > Initial Tech. Trust						
Dispo. to Trust Generally	0.01	0.07	0.10	-0.10	0.15	0.92
Dispo. to Tech. Trust	-0.02	0.07	0.24	-0.12	0.09	0.81
Faith in Humanity	-0.03	0.08	0.34	-0.15	0.09	0.73
Perceived Threat to PIP	-0.11	0.07	1.61	-0.22	0.01	0.11
Subjective Norms	-0.02	0.05	0.45	-0.11	0.07	0.65

Bolded: $p < 0.10$

5.1.1.5. Summary of Findings

The results of the PLS-SEM analysis of the primary experimental data show strong support for the initial technology trust model proposed for emerging technologies, strongly supporting Ha to Hd and Hf to Hj. The majority of results were highly significant with $p < 0.01$, which is especially noteworthy given exploratory PLS-SEM research uses a significance level of $p = 0.10$ (Garson, 2016). Many of the R^2 factors and path coefficients were weak to moderate, but significant. Outer VIF factors ranged from 1.12 and 2.74 and inner VIF factors ranged from 1.00 and 1.46. All VIF factors were less than the recommended limit of VIF = 5.00, indicating multicollinearity does not exist and providing assurance for the predictive validity of the model (Garson, 2016; Hair et al., 2011).

A summary of the concluding hypotheses results for emerging technologies can be found in table 28.

Table 28

Summary of Hypotheses Results using PLS-SEM for Emerging Technologies

Hypotheses	Supported?
Ha. Greater levels of perceived threats to PIP will increase initial technology trust in emerging technologies, and vice versa	✓
Hb. As individuals consider technology artefacts to be more "emergent," they will perceive increased threats to PIP, and vice versa	✓
Hc. Greater dispositions to technology trust will have greater initial technology trust in emerging technologies, and vice versa	✓
Hd. Greater dispositions to trust generally will have greater initial technology trust in emerging technologies, and vice versa	✓
He. When a specific vendor for an emerging technology artefact are not identifiable or unknown, greater faith in humanity will decrease perceived threats to PIP, and vice versa	x
Hf. When a specific vendor for an emerging technology artefact are not identifiable or unknown, greater faith in humanity will increase initial technology trust in emerging technologies, and vice versa	✓
Hg. Greater perceived subjective norms will lead to greater perceived threats to PIP, and vice versa	✓
Hh. Greater perceived subjective norms will lead to greater initial technology trust in emerging technologies, and vice versa	✓
Hi. Greater perceived safety of the economic environment will lead to greater faith in humanity, and vice versa	✓
Hj. Greater initial familiarity of emerging technologies will increase initial technology trust in emerging technologies, and vice versa	✓

5.1.2. Testing the Initial Technology Trust Model with Non-Emerging Technology

The initial technology trust model was tested using the non-emerging technology data to determine whether any significant differences existed between the initial trust formation of emerging technologies and non-emerging technologies. The model was analysed using 62 cases from the experiment control group, email. Where appropriate, bootstrapping procedures were applied using 500 subsamples, bias-corrected and accelerated confidence interval method and two tailed tests with a significance level of 0.10, as recommended for exploratory theory development using PLS-SEM (Garson, 2016; Lowry & Gaskin, 2014). It used a path weighting scheme of 300 maximum iterations and a stop criterion of 10^7.

5.1.2.1. Outer Model

1.Third Order Latent Variables

Technology trust was measured by functionality, reliability, effectiveness and data integrity, and institutional-based trust was measured by structural assurance and situational normality as reflective constructs. Consequently, they were measured by their outer indicator loadings (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014), as reported in table 29. The results were consistent with the primary experimental procedure and sufficient outer model reliability was determined for all variable items with $p < 0.01$ (Garson, 2016; Hair et al., 2014). All of the outer indicator loadings were above the 0.40 minimum threshold for exploratory research, with most indicators also above the 0.70 threshold for confirmatory research (Chin, 1998; Garson, 2016; Hair et al., 2014) which is noteworthy given the exploratory. The exception was E3 which was not significant. The outer indicator loadings for the data integrity provided similar results to the primary experiment, reaffirming it should be included as a trust antecedent for non-emerging technologies.

Outer VIF factors for functionality, reliability, effectiveness and data integrity ranged from 1.11 to 1.79, 1.20 to 1.73, 1.10 to 1.28 and 1.79 to 3.52 respectively. Outer VIF factors for structural assurance and situational normality ranged from 1.63 to 2.02 and 1.26 to 2.78. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011). This means multicollinearity does not exist and these outer items are strongly correlated to their respective variables, indicating predictive validity.

Table 29

Third Order Outer Indicator Loadings for Non-Emerging Technologies

	Technology Trust				Institutional Trust	
item	F	R	E	DI	SA	SN
F1	**0.81**					
F2	**0.83**					
F3	**0.77**					
F4	**0.85**					
R1		**0.73**				
R2		**0.80**				
R3		**0.78**				
R4		**0.76**				
E1			**0.87**			
E2			**0.72**			
E3			--			
D1				**0.74**		
D2				**0.86**		
D3				**0.92**		
SA1					**0.86**	
SA2					**0.77**	
SA3					**0.63**	
SA4					**0.80**	
SN1						**0.75**
SN2						**0.62**
SN3						**0.87**
SN4						**0.89**
SN5						--

F = Functionality, R = Reliability, E = Effectiveness, DI = Data Integrity, SA = Structural Assurance, SN = Situational Normality
Not bolded: p <0.10
Bolded: p <0.01
Not significant: --

The third order model for technology trust converged in 15 iterations and the model for institutional-based trust converged in 16 iterations. These are well below the 300 maximum iterations allowed for exploratory research, indicating a high degree of outer model internal reliability (Garson, 2016). This was similar to the initial technology trust model for emerging technologies.

Overall, sufficient outer model reliability for technology trust and institutional-based trust can be ascertained.

2. Second Order Latent Variables

Perceived threats to PIP were measured using formative instrument items and an examination of item cross loadings was used to confirm discriminant validity and outer model reliability (Hair et al., 2014). Although items did not cross load with each other, they did not load strongly and most outer weights were not significant. Thus, while weak discriminant validity can be ascertained, the reliability of the outer model for perceived threats to PIP cannot be

determined confidently (Hair et al., 2014). The results for cross loadings and outer weights are reported in table 30.

Table 30

Outer Weights and Cross Loadings for Perceived Threats to PIP

	Outer Weights*			Cross Loadings		
item	Intr	Invi	Omni	Intr	Omn	Inv
Network ubiquity			**0.85**	0.43	0.87	0.00
Physical ubiquity			--	0.17	0.42	0.16
Invisibility		1.00		0.14	0.13	1.00
Invasiveness	0.33			0.66	0.24	0.03
Collectability of information	**0.85**			0.85	0.38	0.15
Programmability			--	0.12	0.32	0.21
Wireless accessibility	**0.48**			0.68	0.39	0.10

Intr = Instrusiveness, Omni = Omnipotence, Invi = Invisibility
**Bold: p < 0.01*
**Not Bold: p < 0.10*
**Not significant: --*

Non-emerging technologies, faith in humanity and disposition to technology trust were measured with reflective indicators and therefore examined by their outer indicator loadings (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014), as reported in table 31. The results were consistent with the primary experimental procedure and sufficient outer model reliability was determined with all variable items significant at $p < 0.10$, with almost all loadings significant at $p < 0.01$. All outer indicator loadings were above the 0.40 minimum threshold for exploratory research, with most indicators also above the 0.70 threshold for confirmatory research.

Outer VIF factors for innovativeness and transformative ranged from 1.58 to 2.25 and 1.25 to 2.56 respectively. Outer VIF factors for benevolence, competence and integrity were from 1.11 to 1.79, 1.50 to 1.79 and 1.31 to 1.42. Lastly, outer VIF factors for faith in general technology and technology trust stance were from 1.51 to 3.41 and 1.11 to 1.88. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011), indicating multicollinearity exists and these outer items are strongly correlated to their respective variables, indicating predictive validity.

The second order path model converged in 41 iterations, well below the 300 maximum iterations allowed for exploratory research, indicating a high degree of outer model internal reliability (Garson, 2016).

Table 31

Second Order Outer Indicator Loadings for Non-Emerging Technologies

	Emerging Technology		Faith in Humanity			Disposition to Tech. Trust	
item	Inn	Tra	Ben	Comp	Int	FGT	TTS
ET1	**0.81**						
ET2	**0.82**						
ET3	**0.91**						
ET4		**0.91**					
ET5		**0.89**					
ET6		**0.90**					
FH1			**0.84**				
FH2			**0.78**				
FH3			**0.67**				
FH4				**0.82**			
FH5				**0.86**			
FH6				**0.82**			
FH7					**0.76**		
FH8					**0.77**		
FH9					**0.84**		
DT1						**0.65**	
DT2						**0.94**	
DT3						**0.80**	
DT4						**0.71**	
DT5							0.59
DT6							**0.89**
DT7							**0.85**

Inn = Innovative, Tra= Transformative
Ben = Benevolence, Comp = Competence, Int = Integrity, FGT = Faith in General Technology, TTS = Technology Trust Stance
Not bolded: p <0.10
Bolded: p <0.01

Overall, sufficient outer model reliability for perceived threats to PIP, emerging technologies, faith in humanity and disposition to technology trust can be ascertained. Although, outer model reliability is weaker than the model for emerging technologies.

3. First Order Latent Variables

Disposition to trust generally, subjective norms, the economic environment and initial familiarity were first order latent variables measured with reflective indicators. Consequently, they were measured by their outer indicator loadings (Esposito Vinzi, 2010; Garson, 2016; Hair et al., 2014). The results were consistent with those found for the primary experimental procedure and sufficient outer model reliability was determined for all variable items with $p < 0.01$ (Garson, 2016; Hair et al., 2014). All outer indicator loadings were above the 0.40 minimum threshold for exploratory research, with all other indicators also above the 0.70 threshold for confirmatory research, as reported in table 32. Subjective norms, the economic environment and initial familiarity yielded outer loadings of 1.00. This might normally indicate multicollinearity problems. However, these variables were measured with one item which, in this case, is expected.

Table 32

1st Order Latent Variables for Non-Emerging Technologies

Item	Disp. to Trust	Subj. Norms	Econ. Environ.	Initial Fam.
D1	**0.83**			
D2	**0.83**			
D3	**0.90**			
D4	**0.76**			
S1		**1.00**		
E1			**1.00**	
IN1				**1.00**

Not bolded: p < 0.10
Bolded: p < 0.01

Outer VIF factors ranged from 2.08 to 2.29 for disposition to trust generally and 1.00 for subjective norms, the economic environment and initial familiarity, which were each measured with one item. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011), indicating these outer items are strongly correlated to their respective variables, indicating predictive validity.

The first order path model converged in 2 iterations, well below the 300 maximum iterations allowed for exploratory research and indicating a high degree of reliability (Garson, 2016). Overall, sufficient outer model for initial technology trust can be ascertained.

5.1.2.2. Inner Model

1. Perceived Threat to PIP

Non-emerging technology artefacts, faith in humanity and subjective norms were found to have a significant predictive effect on perceived PIP threats, explaining 21% of the variance in perceived PIP threats, with $R^2 = 0.21$ and $p = 0.03$ (Hair et al., 2011; Ringle & Sarstedt, 2016; Ringle et al., 2012). This is considered a weak predictive effect of the combined variables (Cohen, 1992; Garson, 2016; Hair et al., 2011) and is similar to that found in the emerging technologies model.

Subjective norms had a significant path coefficient to perceived threats to PIP of 0.36, and $p < 0.01$. This shows a significant weak to moderate positive causal relationship exists between subjective norms and perceived PIP threats. Non-emerging technology artefacts and faith in humanity had path coefficients of 0.21 ($p = 0.11$) and 0.04 ($p = 0.67$) respectively, indicating that they may not affect perceived threats to PIP. This is contrary to the analysis with the emerging technology data which showed emerging technology artefacts had a significant path

coefficient to perceived threats to PIP with $p < 0.01$. Despite this, mean differences in the path coefficients in the emerging and non-emerging technology models were not found to be significant, as reported in table 31. This suggests that the emergence factor of technology artefacts do not cause an interaction effect between subjective norms, faith in humanity and technology artefact characteristics on perceived threats to PIP (Lowry & Gaskin, 2014).

Table 33

Multigroup Moderation Effects on Perceived Threats to PIP between Emerging and Non-Emerging Technology Path Coefficients

	Mean Diff.	t-value	p-value
Emerging vs Non-Emerging Technology Artefact*	0.06	0.04	0.97
Faith in Humanity*	0.64	0.46	0.64
Subjective Norms	0.12	0.78	0.44

Bolded: $p < 0.10$

**One or more path coefficients tested were not significant*

Non-emerging technologies, faith in humanity and subjective norms generated f^2 values of 0.05, 0.002 and 0.14. This would suggest the degree of emergence of technologies have a small effect size on perceived PIP threats, faith in humanity has almost no effect and subjective norms has a small to moderate effect size (Chin, 1998; Cohen, 1992; Esposito Vinzi, 2010). This indicates emerging technology characteristics have an incremental change effect on perceived PIP threats equal to 5%, faith in humanity of 0.2% and subjective norms of 16%. However, non-emerging technologies, faith in humanity and subjective norms all yielded non-significant f^2 statistics when using a significance level of $p = 0.10$ for exploratory PLS-SEM research (Garson, 2016). This suggests that the exclusion of either variable from the model, while holding all other variables, would not cause a significant change in R^2 and they may be less relevant in a broader context of initial trust formation when considering the effect of other factors.

Considering the non-significant f^2 results, post hoc power analyses were performed with 95% confidence levels. Non-emerging technologies had a power of 0.41 and faith in humanity had a power of 0.05. These measures are both less than the recommended power of 0.80, which indicates insufficient power exists to reliably determine if an effect size on perceived threats to PIP exists (Chin, 1998; Cohen, 1988; Faul et al., 2009; Faul et al., 2007; Miguel & Mikko, 2015; Peng & Lai, 2012). Subjective norms had a power of 0.87 which indicates sufficient power existed within the data to reliably measure an effect size within which the PLS-SEM

parameters were set for this research (Chin, 1998; Cohen, 1988; Faul et al., 2009; Faul et al., 2007; Miguel & Mikko, 2015; Peng & Lai, 2012).

The inner VIF factors for non-emerging technology artefacts, faith in humanity and subjective norms ranged from 1.01 to 1.11. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011). This indicates the model does not have multicollinearity and that these variables are strongly correlated to initial technology trust in emerging technologies. This means they can be used to confidently predict initial technology trust in emerging technologies with a strong level of predictive accuracy, indicating predictive validity (Garson, 2016; Hair et al., 2011).

The PLS-SEM results for perceived PIP threats in non-emerging technology are summarised in table 34.

Table 34

Perceived Threats to PIP Statistics for Non-Emerging Technologies

		Mean	S.D.	t-value	5%	95%	p-value
R^2							
Perceived Threat to PIP	**0.22**	**0.25**	**0.10**	**2.13**	**0.10**	**0.44**	**0.03**
f^2							
Non-Emerging Technology Artefact > Perceived Threat to PIP	0.05	0.08	0.09	0.61	0.00	0.25	0.54
Faith in Humanity > Perceived Threat to PIP	0.00	0.02	0.03	0.09	0.00	0.07	0.93
Subjective Norms > Perceived Threat to PIP	0.16	0.19	0.12	0.29	0.05	0.46	0.20
Path Coefficients							
Non-Emerging Technology Artefact > Perceived Threat to PIP	0.21	0.21	0.13	1.59	-0.03	0.43	0.11
Faith in Humanity > Perceived Threat to PIP	0.04	0.05	0.10	0.44	-0.11	0.22	0.67
Subjective Norms > Perceived Threat to PIP	**0.36**	**0.37**	**0.10**	**3.74**	**0.21**	**0.53**	**0.00**
Inner VIF Factors							
Non-Emerging Tech. Characteristics > Perceived Threat to PIP	1.07	--	--	--	--	--	--
Faith in Humanity > Perceived Threat to PIP	1.03	--	--	--	--	--	--
Subjective Norms > Perceived Threat to PIP	1.08	--	--	--	--	--	--

Not bolded: $p > 0.10$
Bolded: $p < 0.01$

2. Faith in Humanity

The perceived safety of the economic environment was found to have a significant predictive effect on faith in humanity, explaining 15% of the variance in faith in humanity, with R^2 = 0.15 and p = 0.05 (Hair et al., 2011; Ringle & Sarstedt, 2016; Ringle et al., 2012). This is considered a weak predictive effect (Cohen, 1992; Garson, 2016; Hair et al., 2011).

The economic environment had a significant path coefficient to faith in humanity of 0.39, and $p < 0.01$. This means a moderate positive causal relationship exists between perceptions of an economic environment and faith in humanity, similar to the results for emerging technologies. A test for multigroup moderating effects supports this, with no significant mean difference found between the path coefficients for emerging technologies model compared to the non-emerging technology model, as reported in table 35. This indicates that the emergence factor of a technology does not have an interaction effect on the relationship between the perceived safety of the economic environment and faith in humanity (Lowry & Gaskin, 2014).

Table 35

Multigroup Moderation Effects on Faith in Humanity between Emerging and Non-Emerging Technology Path Coefficients

	Mean Diff.	t-value	p-value
Economic Environment	0.02	0.02	0.99

Bolded: $p < 0.10$
**One or more path coefficients tested were not significant*

The economic environment generated a f^2 of 0.18, suggesting it has a moderate effect size on faith in humanity (Chin, 1998; Cohen, 1992; Esposito Vinzi, 2010). This indicates an individual's perceptions of the economic environment from which they might encounter a technology will have an incremental change effect on faith in humanity equal to 18%. The f^2 statistic was not significant with $p = 0.16$, suggests the exclusion of the economic environment may not cause a significant change in R^2. While the perceived safety of the economic environment may have a predictive effect on faith in humanity, it may be less relevant in a broader context when considering the effect of other factors. Subsequently, post hoc power analyses were performed with 95% confidence levels, reporting a power of 0.91. This is greater than the recommended power of 0.80, which indicates sufficient power existed within the data to reliably measure an effect size within which the PLS-SEM parameters were set for this research (Chin, 1998; Cohen, 1988; Faul et al., 2009; Faul et al., 2007; Miguel & Mikko, 2015; Peng & Lai, 2012).

The inner VIF factor for the economic environment of 1.00, indicating perfect collinearity. This means an individual's perceptions about the economic environment can be used to confidently predict faith in humanity with a strong level of predictive accuracy (Garson, 2016; Hair et al., 2011).

The PLS-SEM results for faith in humanity for non-emerging technologies are reported in table 36.

Table 36

Faith in Humanity Statistics for Non-Emerging Technologies

		Mean	S.D.	t-value	5%	95%	p-value
R^2							
Faith in Humanity	**0.15**	**0.16**	**0.08**	**1.83**	**0.04**	**0.31**	**0.07**
f^2							
Economic. Environ. > Faith in Humanity	0.18	0.21	0.13	1.40	0.04	0.09	0.16
Path Coefficients							
Economic Environ. > Faith in Humanity	**0.39**	**0.39**	**0.11**	**3.50**	**0.19**	**0.56**	**0.00**
Inner VIF Factors							
Economic Environ. > Faith in Humanity	1.00	--	--	--	--	--	--

Bolded: p < 0.10

3. Initial Technology Trust in Emerging Technologies

Perceived threats to PIP, faith in humanity, familiarity, disposition to technology trust and disposition to trust generally were found to have a significant predictive effect on initial technology trust in emerging technologies, explaining 42% of the variance in perceived PIP threats, with $R^2 = 0.42$ and $p < 0.01$ (Hair et al., 2011; Ringle & Sarstedt, 2016; Ringle et al., 2012). This is considered a weak to moderate predictive effect of the combined variables and is similar to the model for emerging technologies (Cohen, 1992; Garson, 2016; Hair et al., 2011).

The path coefficients to initial technology trust in non-emerging technologies from perceived threats to PIP was -0.03; faith in humanity was 0.55; subjective norms and initial familiarity were both 0.15; disposition to technology trust was 0.06; and, disposition to trust was 0.16. This shows initial trust in non-emerging technologies have a weak negative relationship with perceived threats to PIP; a strong positive relationship with faith in humanity; a weak positive causal relationship with disposition to technology trust; and, a weak to moderate positive causal relationship with subjective norms, familiarity, disposition to technology trust and disposition to trust generally (Cohen, 1992). Faith in humanity was the only path coefficient found to be significant with $p < 0.01$. These results vary from those generated from the emerging technologies model. The path coefficient from faith in humanity to initial technology trust was 0.12 with $p = 0.08$ and significant for emerging technologies, increasing to 0.55 with $p > 0.10$ in the context of non-emerging technologies. Perceived threats to PIP was previously found to have significant path coefficient of -0.42 and $p < 0.01$, consistent with the primary experiment, increasing to -0.03 with $p = 0.84$. A multigroup moderation test

found that these changes were statistically significant, with $p < 0.01$, as reported in table 37. This indicates the emergence of a technology has an interaction effect on the path coefficients between faith in humanity to initial technology trust and perceived threats to PIP to initial technology trust (Lowry & Gaskin, 2014). This supports the argument that perceived threats to PIP are not a significant inherent attribute to non-emerging technologies.

Table 37

Multigroup Moderation Effects on Initial Technology Trust between Emerging and Non-Emerging Technology Path Coefficients

	Mean Diff.	t-value	p-value
Perceived Threat to PIP	**0.43**	**3.06**	**0.00**
Faith in Humanity	**0.43**	**2.78**	**0.00**
Initial Familiarity	0.04	0.31	0.76
Subjective Norms	0.01	0.08	0.94
Disposition to Technology Trust	0.06	0.42	0.67
Disposition to Trust Generally	0.00	0.02	0.99

Bolded: $p < 0.10$
Not bolded: $p > 0.10$
**One or more path coefficients tested were not significant*

Perceived threats to PIP, faith in humanity, subjective norms, initial familiarity, disposition to technology trust and disposition to trust generally generated f^2 values of 0.00, 0.34, 0.03, 0.03, 0.00 and 0.04 respectively. This suggests faith in humanity has a high effect size of initial technology trust, perceived threats to PIP and disposition to technology trust have a trivial effect and the remaining variables each have a small effect size on initial technology trust in non-emerging technologies (Chin, 1998; Cohen, 1992; Esposito Vinzi, 2010). Therefore, perceived threats to PIP and disposition to technology trust both have an incremental change effect of approximately 0%, dropping from 26% in the emerging technology model results and from 2% for disposition to technology trust. On the other hand, disposition to trust generally remained the same at 4%, subjective norms and initial familiarity both rose from 2% to 3%, and faith in humanity rose from 2% to 34%. All f^2 statistics were not significant at $p = 0.10$ and generated p values between 0.12 and 0.98, which suggests each variable is unlikely to cause of a significant change in R^2 if excluded from the model while holding all other factors constant. This is coupled with the fact that none of these other variables had a significant predictive effect on initial technology trust in non-emerging technologies. Interestingly, this includes the effect of perceived threats to PIP and faith in humanity which were significant for initial trust in emerging technologies, but not non-emerging technologies.

Considering the non-significant f^2 results, post hoc power analyses were performed with 95% confidence levels. Perceived threats to PIP, initial familiarity, subjective norms, disposition to technology trust, and disposition to trust generally had a power of 0.05, 0.27, 0.27, 0.05 and 0.34 respectively. These measures are both less than the recommended power of 0.80, which indicates insufficient power exists to reliably determine if an effect size on initial technology trust in emerging technology exists (Chin, 1998; Cohen, 1988; Faul et al., 2009; Faul et al., 2007; Miguel & Mikko, 2015; Peng & Lai, 2012). Faith in humanity had a power of 0.99 which indicates sufficient power existed within the data to reliably measure an effect size within which the PLS-SEM parameters were set for this research (Chin, 1998; Cohen, 1988; Faul et al., 2009; Faul et al., 2007; Miguel & Mikko, 2015; Peng & Lai, 2012).

The inner VIF factors for perceived threats to PIP, faith in humanity, initial familiarity, subjective norms, disposition to technology trust and disposition to trust generally ranged from 1.18 to 1.60. These are less than the recommended limit of VIF = 5.00 (Hair et al., 2011). This indicates the model does not have multicollinearity and these variables are strongly correlated to initial technology trust. Therefore, these variables could be relied upon to confidently predict initial technology trust in emerging technologies with a strong level of predictive accuracy, indicating predictive validity (Garson, 2016; Hair et al., 2011).

The PLS-SEM results for faith in humanity for non-emerging technologies are summarised in table 38.

5.1.2.3. Measurement of Fit

Overall, the path model for initial technology trust in emerging technologies, using data for non-emerging technologies, cannot be considered to have measurement of fit. All the path coefficients to initial technology trust were not significant, except for faith in humanity, which just made the significance threshold with $p = 0.10$. The outer item weights for perceived PIP threats also did not load correctly, despite all other items loading correctly on their intended constructs, including the technology trust attributes which was adapted to include data integrity, which gives rise to doubt outer model reliability. Furthermore, only one f^2 statistic was significant for variables affecting initial technology trust, which in addition to the non-significant path coefficients, suggests the model does not provide sufficient inner model reliability.

Table 38

Initial Technology Trust in Non-Emerging Technologies Statistics

		Mean	S.D.	t-value	5%	95%	p-value
R^2							
Initial Tech. Trust in Emerging Tech.	**0.42**	**0.47**	**0.12**	**3.49**	**0.10**	**0.44**	**0.00**
f^2							
Perceived Threats to PIP > Initial Tech. Trust in Emerging Tech.	0.00	0.03	0.05	0.03	0.00	0.12	0.98
Faith in Humanity > Initial Tech. Trust in Emerging Tech.	0.34	0.36	0.21	1.58	0.09	0.76	0.12
Initial Familiarity > Initial Tech. Trust in Emerging Tech.	0.03	0.07	0.08	0.42	0.00	0.12	0.67
Subjective Norms > Initial Tech. Trust in Emerging Tech.	0.03	0.05	0.06	0.51	0.00	0.16	0.64
Dispo. to Tech Trust > Initial Tech. Trust in Emerging Tech.	0.00	0.02	0.03	0.11	0.00	0.08	0.90
Dispo. to Trust Generally > Initial Tech. Trust in Emerging Tech.	0.04	0.06	0.06	0.62	0.00	0.17	0.53
Path Coefficients							
Perceived Threats to PIP > Initial Tech. Trust in Emerging Tech.	-0.03	0.13	0.14	1.07	-0.27	0.21	0.84
Faith in Humanity > Initial Tech. Trust in Emerging Tech.	**0.55**	**0.53**	**0.14**	**4.05**	**0.30**	**0.74**	**0.00**
Initial Familiarity > Initial Tech. Trust in Emerging Tech.	0.15	0.16	0.14	1.08	-0.07	0.38	0.28
Subjective Norms > Initial Tech. Trust in Emerging Tech.	0.36	0.13	0.13	1.08	-0.12	0.32	0.28
Dispo. to Tech Trust > Initial Tech. Trust in Emerging Tech.	0.06	0.06	0.12	1.52	-0.01	0.26	0.61
Dispo. to Trust Generally > Initial Tech. Trust in Emerging Tech.	0.16	0.16	0.10	0.52	-0.01	0.34	0.13
Inner VIF Factors							
Perceived Threat to PIP > Initial Tech. Trust in Emerging Tech.	1.15	--	--	--	--	--	--
Faith in Humanity > Initial Tech. Trust in Emerging Tech.	1.46	--	--	--	--	--	--
Initial Familiarity > Initial Tech. Trust in Emerging Tech.	1.05	--	--	--	--	--	--
Subj. Norms > Initial Tech. Trust in Emerging Tech.	1.17	--	--	--	--	--	--
Dispo. to Tech. Trust > Initial Tech. Trust in Emerging Tech.	1.42	--	--	--	--	--	--
Dispo. to Trust Generally > Initial Tech. Trust in Emerging Tech.	1.11	--	--	--	--	--	--

Bolded: $p < 0.10$

5.1.2.4. Interaction Effects

Interactions effects were tested for each path using the product indicator calculation method, a significance level of 0.10 and biased corrected confidence levels, reported in table 39. Almost all moderating variables tested generated low and insignificant results. The exceptions were subjective norms which were found to have a significant positive interaction effect of 0.26 (p = 0.09) on the path from non-emerging technology artefact to perceived threats to PIP and non-emerging technology characteristics had a significant positive

interaction effect of 0.27 (p = 0.08) on the path from subjective norms to perceived threats to PIP.

Table 39

Interaction Effects of Variables in Initial Trust in Non-Emerging Technologies Model

		S.D.	t-value	5%	95%	p-value
Emerging Tech. > Perceived Threat to PIP						
Faith in Humanity	0.18	0.16	1.12	-0.01	0.52	0.27
Subjective Norms	**0.26**	**0.15**	**1.71**	**0.03**	**0.52**	**0.09**
Faith in Humanity > Perceived Threat to PIP						
Subjective Norms	0.09	0.19	0.46	-0.23	0.40	0.65
Subjective Norms > Perceived Threat to PIP						
Faith in Humanity	0.05	0.15	0.15	-0.17	0.31	0.88
Perceived Threat to PIP > Initial Tech. Trust						
Dispo. to Trust Generally	0.12	0.19	0.62	-0.18	0.43	0.54
Dispo. to Tech. Trust	-0.23	0.22	1.03	-0.60	0.14	0.30
Faith in Humanity	0.07	0.25	0.27	-0.39	0.43	0.78
Initial Familiarity	0.13	0.18	0.72	-0.24	0.35	0.47
Subjective Norms	-0.17	0.17	0.96	-0.44	0.10	0.34
Dispo. to Trust Generally > Initial Tech. Trust						
Dispo. to Tech. Trust	-0.23	0.22	1.03	-0.60	0.14	0.30
Faith in Humanity	0.07	0.25	0.27	-0.39	0.43	0.78
Initial Familiarity	0.13	0.18	0.72	-0.24	0.35	0.47
Perceived Threat to PIP	0.04	0.19	0.21	-0.33	0.31	0.84
Subjective Norms	-0.17	0.17	0.96	-0.44	0.10	0.34
Dispo. to Tech. Trust > Initial Tech. Trust						
Dispo. to Trust Generally	-0.03	0.17	0.16	-0.30	0.25	0.87
Faith in Humanity	-0.12	0.13	0.90	-0.29	0.11	0.37
Initial Familiarity	-0.04	0.14	0.29	-0.28	0.17	0.77
Perceived Threat to PIP	0.03	0.22	0.15	-0.30	0.38	0.88
Subjective Norms	-0.13	0.24	0.57	-0.54	0.21	0.57
Faith in Humanity > Initial Tech. Trust						
Dispo. to Trust Generally	-0.01	0.14	0.05	-0.24	0.20	0.96
Dispo. to Tech. Trust	-0.12	0.14	0.83	-0.32	0.18	0.41
Initial Familiarity	-0.24	0.18	1.37	-0.54	0.03	0.17
Perceived Threat to PIP	-0.13	0.25	0.51	-0.53	0.30	0.61
Subjective Norms	0.18	0.21	0.86	-0.19	0.50	0.39
Subjective Norms > Initial Tech. Trust						
Dispo. to Trust Generally	0.13	0.13	1.00	-0.06	0.36	0.32
Dispo. to Tech. Trust	-0.22	0.18	1.25	-0.52	0.09	0.21
Faith in Humanity	0.19	0.17	1.08	-0.13	0.45	0.28
Initial Familiarity	-0.22	0.15	1.42	-0.48	0.03	0.16
Perceived Threat to PIP	-0.18	0.16	1.15	-0.46	0.05	0.25
Familiarity > Initial Tech. Trust						
Dispo. to Trust Generally	-0.09	0.15	0.60	-0.37	0.09	0.55
Dispo. to Tech. Trust	0.05	0.16	0.29	-0.19	0.38	0.77
Faith in Humanity	-0.02	0.20	0.10	-0.43	0.21	0.92
Perceived Threat to PIP	0.11	0.14	0.80	-0.16	0.28	0.42
Subjective Norms	-0.22	0.15	1.45	-0.40	0.09	0.15

Bolded: p < 0.10

5.1.2.5. Summary of Findings

The results of the PLS-SEM analysis of the initial technology trust model proposed for emerging technologies but tested with data from non-emerging technologies, supports the proposition that emerging and non-emerging technologies cannot be considered to be the same, with respect to perceived threats to PIP and initial technology trust formation. These results show that almost all of the proposed variables have no significant path coefficients to initial technology trust, except for faith in humanity and, by extension, its relationship with perceptions of the economic environment. Most f^2 results were not significant and so no reliable conclusion can be made about their effect sizes, except that it appears unlikely that any relationships exist that can offer predictive validity for estimating initial technology trust. Overall, R^2 was significant at 0.42, which was surprising given the weak and non-significant results yielded for all the variables. However, this is likely to be a consequence of the strong, significant path coefficient and f^2 results for faith in humanity which compensated for this, which both increased greatly when using non-emerging technology data.

An illustration of the initial trust models for emerging and non-emerging technologies respectively can be found on the following page, with their respective path coefficients and R^2 statistics in figures 5 and 6. A comparison of these figures highlights the key differences between the initial technology trust models for emerging technologies as opposed to non-emerging technologies, in particular the differences in Ha and Hb whereby emerging technology characteristics do not have a predictive effect on perceived threats to PIP in non-emerging technologies, or that perceived PIP threats have a predictive effect on initial technology trust in non-emerging technologies. Disposition to trust generally, disposition to technology trust, initial familiarity and subjective norms no longer had an effect on initial technology trust when tested on non-emerging technologies, but faith in humanity did.

Figure 5

Initial Trust in Emerging Technologies: Path Coefficients and R^2 Statistics

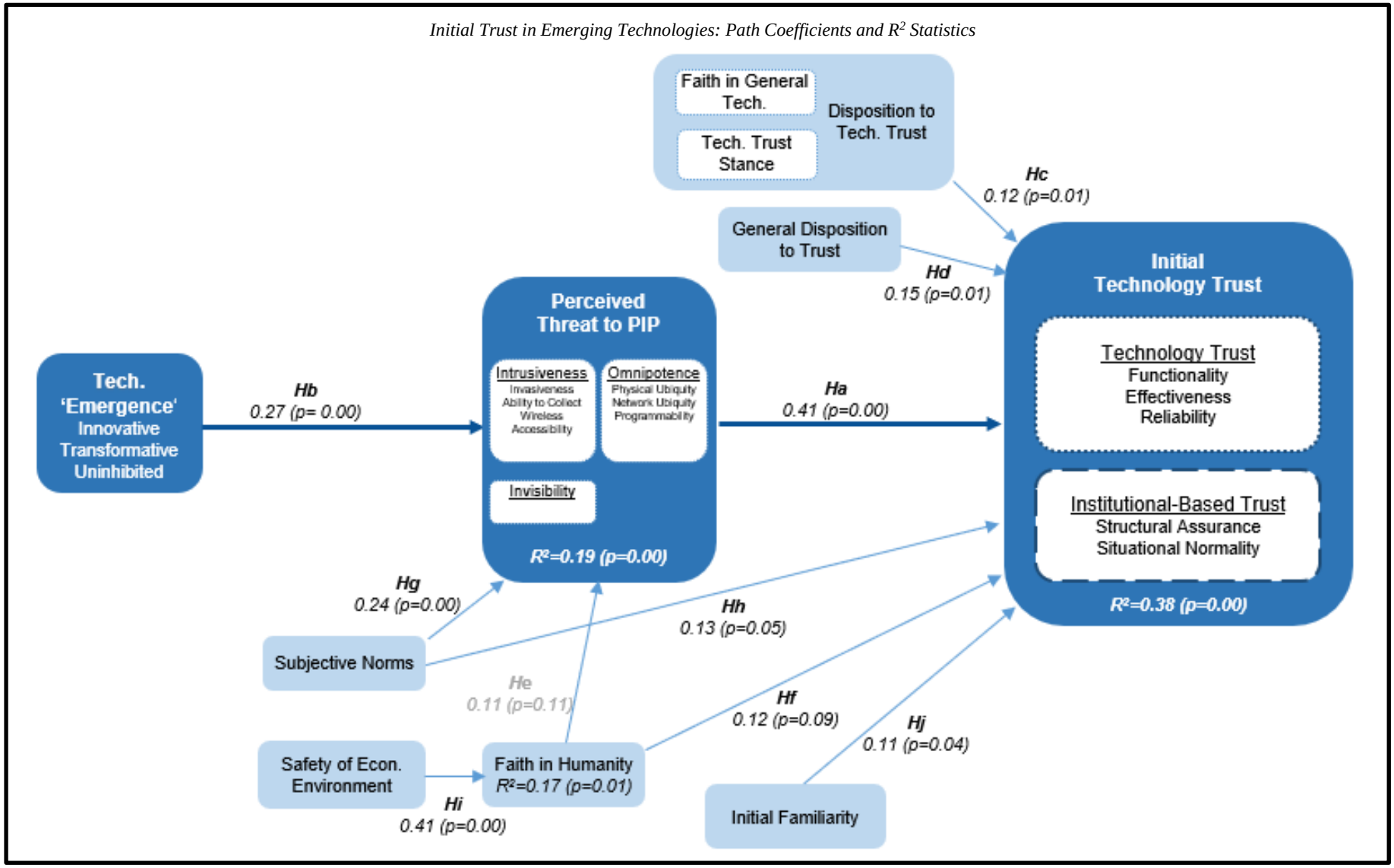
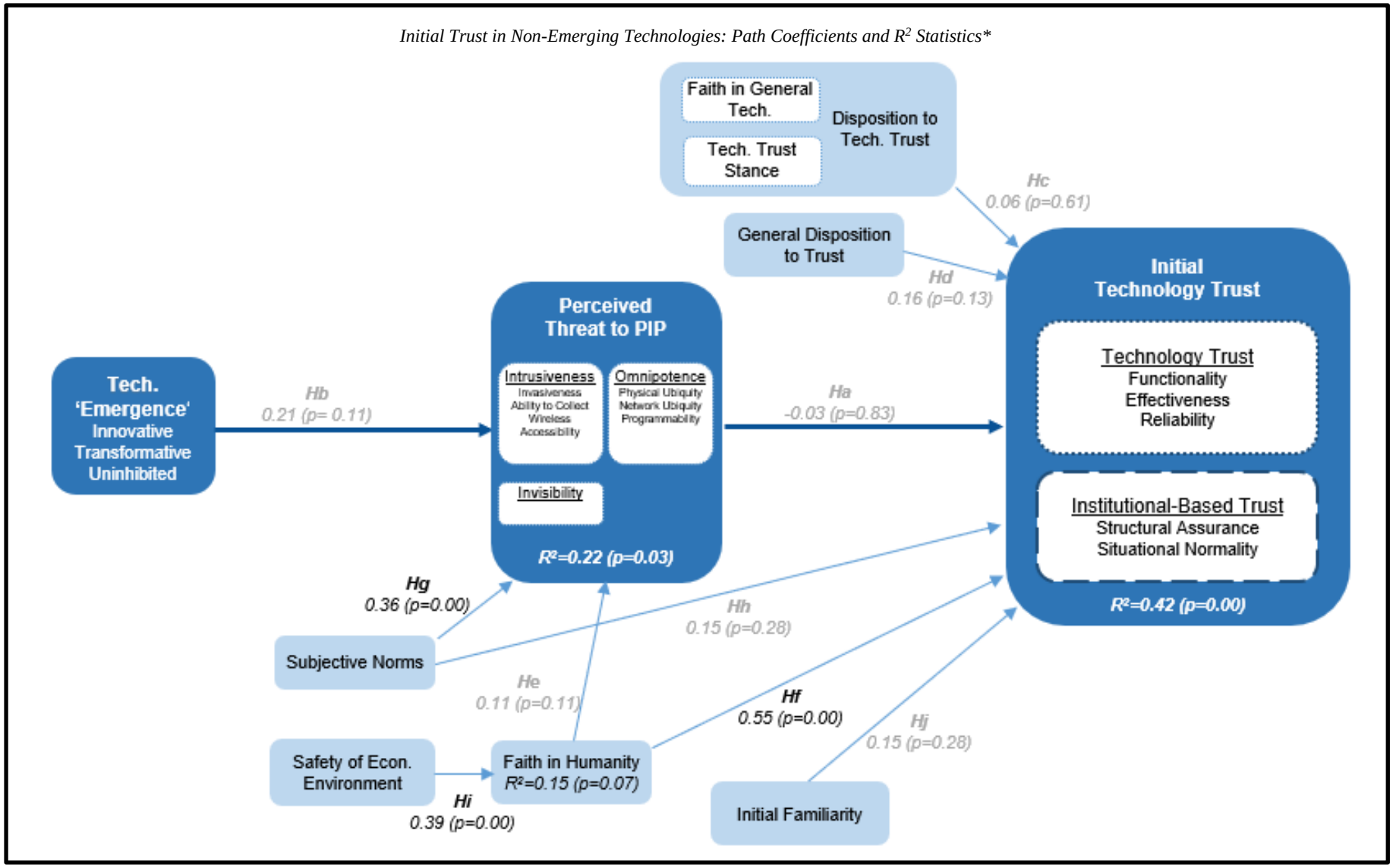


Figure 6

*Initial Trust in Non-Emerging Technologies: Path Coefficients and R^2 Statistics**



** Hypotheses labels are denoted for ease of understanding and comparability with the emerging technology model only*

5.2. Discussion & Future Directions

The primary objectives of this research were met by the experimental results and testing hypotheses H1 to H5. Only once these were met, it was decided to extend the analysis of the secondary variables proposed to influence initial technology trust in emerging technologies using PLS-SEM techniques. Thus, this study sought to explore a supplementary set of effects which were found to be related to emerging technologies, perceived threats to PIP and initial technology trust in emerging technologies. This was tested using the remaining data collected from the primary experiment to answer Ha to Hj to measure the predictive validity of the proposed model.

All but one of the hypotheses proposed were supported in the PLS-SEM analysis. This indicates that the initial technology trust model proposed was relatively accurate and that the proposed arguments for faith in humanity, the economic environment, subjective norms and initial familiarity have a strong basis from which they can be included in future technology, trust and privacy research. This is significant because these variables are not offered in other key areas of trust or privacy research and offers the opportunity for further development into these complex, and often irrational, behavioural theories.

Many of the path-coefficients are weak, but significant. These weaker path-coefficients are likely because of the exclusion of other key antecedents to technology trust and adoption which have been proven to exist, such as perceived usefulness and perceived ease of use, self-efficacy, facilitating conditions and systems quality (Davis, 1989; Fathema, Ross, & Witte, 2014; Fathema, Shannon, & Ross, 2015; Venkatesh, 2000; Venkatesh & Bala, 2008; Venkatesh & Davis, 2000). The fact the PLS-SEM analysis uses data sourced from a controlled experiment also means the extent to which relationships might exist may not be completely reliable given their lack of external validity (Mook, 1983). However, PLS-SEM does not need normally distributed data which mitigates the risk of the experiment data (Hair et al., 2014; Ringle et al., 2012; Wong, 2013). Regardless, the use of the experiment means we can confidently say whether significant relationships and predictive validity exist due to the strong internal validity of experimental procedures.

5.2.1. Emerging Technology Artefact Characteristics

The PLS-SEM results confirmed the emergence factor of an emerging technology artefact and subjective norms both have a predictive effect on perceived threats to PIP. The effect of

emerging technology characteristics on perceived PIP threats was theorised by Conger et al. (2013) and investigated, and quantitatively supported, in the experiment. This PLS-SEM analysis reaffirms the relationship between these two variables, but also confirms the predictive validity of emerging technology characteristics on perceived threats to PIP. When the relationship was tested using non-emerging technologies, it was no longer found to be significant. This provides a strong argument that emerging technologies have a unique relationship with perceived threats to PIP. As suggested by Conger et al. (2013), these PIP threats are not inherently attributable to non-emerging technologies. The PLS-SEM analysis indicates emerging technologies are perceived and evaluated using a different cognitive process than non-emerging technologies, and that they are perceived to have inherently unique characteristics. This discovery suggests that other, different technology classes may exist which may be perceived in a uniquely different way from other technology classes which will impact technology trust beliefs. In order to effectively understand and support individuals interact with technologies, future research should investigate whether other significant characteristics and trust beliefs exist, and confirm whether each of the two initial trust models discovered in this thesis are relevant.

5.2.2. Perceived Privacy Threats

Whether privacy threats have a significant impact on technology trust has not been tested before in the prior literature. The results of the PLS-SEM procedures confirmed the significant predictive effect perceived PIP threats have on initial technology trust in emerging technologies, which was initially theorised by Conger et al. (2013) but investigated and quantitively supported in the experiment. It also confirmed that this predictive effect is not significant for non-emerging technologies. This reiterates the difference between emerging and non-emerging technologies and the perceived threats and trust beliefs people hold about them, as demonstrated with the discovery of the data integrity antecedent for non-emerging technologies in the experiment. The difference in the path co-efficient from perceived threats to PIP to initial technology trust was found to be highly significant, dropping from 0.41 for emerging technologies to -0.03 for non-emerging technologies, and further supporting the proposition that the two classes of technology are evaluated using different cognitive processes.

This study provides significant evidence to support the inclusion of privacy threats in technology trust models for emerging technologies. Although, it suggests existing trust models for current non-emerging technologies do not need to include perceived PIP threats as a significant predictive variable for trust, despite the unique trust antecedent individuals have for data integrity beliefs. This may change once existing emerging technologies transition to being non-emerging and the general characteristics for non-emerging technologies evolve. This is a topic for future research.

5.2.2. SUBJECTIVE NORMS

Subjective norms have previously been found to have an effect on technology trust and technology adoption (Gefen et al., 2008; Kaushik & Rahman, 2015; Li et al., 2008; Lippert & Davis, 2006). This relationship was confirmed in the experiment with subjective norms having a significant effect as a covariate between perceived threats to PIP and initial technology trust in emerging technologies. However, the PLS-SEM analysis reaffirmed this. In addition, the PLS-SEM found subjective norms have a direct significant effect on perceived threats to privacy as well. Interestingly, this was also found in the initial technology trust model using non-emerging technologies. Therefore, it can be concluded that subjective norms are relevant to technology in general. This provides additional support for its inclusion in more widely accepted and more popular technology trust and adoption models, such as McKnight et al. (2011)'s technology trust model and TAM and its many extensions (Davis, 1989; Fathema et al., 2014; Fathema et al., 2015; Venkatesh, 2000; Venkatesh & Bala, 2008; Venkatesh & Davis, 2000). Given subjective norms are not particular to technology use, it should also be considered for people-related trust research as well. Prior people-related trust research has theorised or tested it before to limited extent (Bandura, 1997; Rotter, 1971; Rousseau et al., 1998). However, subjective norms failed to be incorporated into the popular people-related trust models predominantly used today (Davis, 1989; Mayer et al., 1995; McKnight et al., 1998). It is strongly recommended that trust research should consider the effect of subjective norms and include it in popular trust models for completeness.

In addition, the PLS-SEM analysis found subjective norms have a significant interaction effect on the relationship between technology characteristics and perceived threats to PIP. This was only found in the non-emerging technology trust model and did not have a significant interaction effect on emerging technology artefacts and perceived PIP threats. This

is likely because subjective norms for non-emerging technologies exist only because of their maturity and successful integration in society. By comparison, emerging technologies have yet to be established in existing social networks and subjective norms have not yet been able to form about PIP risks. Therefore, individuals are unable to perceive the emerging technology beliefs of those important to them and are unable act according to the social pressures they might exert or be guided by social expectations. Consequently, this interaction effect causes subjective norms to have a direct and indirect effect on perceived threats to PIP for non-emerging technologies, and only a direct effect on emerging technologies (Garson, 2016).

5.2.3. FAITH IN HUMANITY

Faith in humanity was used as a proxy for vendor-based trust with the rationale that when specific individual vendors are not identifiable or unknown in a technology trust situation, individuals' faith in humanity, as generalisation of all vendors, will influence their perceptions of trust instead. This follows the same argument as Li et al. (2008). Research has found vendor-based trust affects technology trust (McKnight et al., 1998; Pavlou, 2003; Wingreen & Baglione, 2005). However, in a study of initial technology trust formation, Li et al. (2008) failed to find significant results to support the hypothesis that vendor-based trust affects initial technology trust. It was suspected their choice of technology artefact was the cause for this. However, the PLS-SEM analysis here shows that faith in humanity had a significant predictive effect on initial technology trust in emerging technologies. This supports the argument that faith in humanity can be used to compensate for low levels of institutional-based trust or knowledge-based trust which causes uncertainty around a technology's functionality, effectiveness, reliability, or even data integrity. This finding also provides supplementary support for the experiment results which found faith in humanity had a significant covariate effect on initial technology trust in emerging technologies.

The significance of the predictive relationship from faith in humanity to initial technology trust remained the same when tested for non-emerging technologies. This indicates faith in humanity affects technology generally, and is not particular to emerging or non-emerging technologies. Interestingly though, the path-coefficient more than quadrupled from 0.12 for emerging technologies to 0.55 for non-emerging technologies. One reason for this is thought to be because individuals are first and foremost concerned with the antecedents of initial technology trust when first encountering a new technology. When this technology is an

emerging technology, there is significantly more uncertainty about its functionality, effectiveness and reliability. For non-emerging technologies, their lack of complexity reduces the uncertainty in correctly evaluating a technology's functionality, effectiveness, reliability and data integrity. There also tends to be greater second-hand knowledge that can be relied upon. Thus, individuals are more readily satisfied in their initial trust beliefs in non-emerging technologies and so become more concerned with their secondary factors. Consequently, individuals may have a hierarchy of needs for initial technology trust whereby the direct antecedents for technology-trust take precedence over any other factors. When individuals are comfortable in their beliefs of a technology artefact, then perhaps they are more likely to put more bearing on other relevant factors which affect initial trust beliefs. Research to investigate this theory would be valuable to both academics and practitioners. It seems logical to suggest this hierarchy of needs exists would exist for technologies which individuals have a relatively greater familiarity of compared to new technologies that individuals' have little experience of or have not encountered before, regardless of whether they are an emerging technology as opposed to a non-emerging technology.

The only hypothesis that could not be supported was He in the context of emerging and non-emerging technologies, theorising a positive relationship between faith in humanity and perceived threats to PIP. The PLS-SEM analysis found the path-coefficients to be insignificant for both emerging and non-emerging technologies, indicating that this relationship is not applicable in either case. Therefore, it is unlikely to be relevant for technology PIP threats in general. The most plausible explanation for this is that individuals' beliefs about perceived threats to PIP are relatively objective and therefore more resistant to influence by other variables. While perceived threats to PIP may be subjective to some extent, they are also more persistent because the risk they present is calculative, based on fact and knowledge, and therefore represent a more objective measure. Therefore, an individual's faith in humanity would not affect an individual's perceived threats to PIP. However, an individual's faith in humanity could mitigate the risk a technology may present to PIP through greater technology trust. For instance, most individuals will acknowledge the risk of driving a car and the probability of an accident. But, their belief that other drivers on the road are competent drivers, and the trust they have in their own driving ability, mitigates these concerns to the point that they safely trust cars as a mode of transport. Additional research should be conducted to validate this finding.

5.2.4. Economic Environment

The results of the PLS-SEM analysis using both emerging technologies and non-emerging technologies strongly confirmed the theory that the economic enviroment is a relevant predictor of faith in humanity in initial technology trust formation. In both cases, path coefficients were similar with 0.41 and 0.39 respectively, and significant at $p < 0.01$. Firstly, this provides strong evidence that the economic environment is a significant and relevant variable which impacts faith in humanity, with sufficent predictive validity. Secondly, it also shows that it is applicable to technologies in general, and will persist as a relevant factor for faith in humanity even as technologies transition from a emerging to non-emerging technology state.

The perceived safety of the economic environment and its effect on trust has not been considered in previous Information Systems or Psychology literature. However, it is important in all situations in which an exchange or trade occurs because of the element of self-interest intrinsic to all exchanges and how it influences economic behaviours (Burchell & Wilkinson, 1997). As a result, this is intimately related to trust. In the context of technology trust, individuals must trust that the vendors or operators of technologies will not exploit the access technologies will have to their private lives. Individuals must trust they will not betray customer loyalty or good faith to turn a quick profit using data they provided to them, data collected by the technology or data generated by the technology based on its usage. They must also trust that vendors or technology operations have not bypassed any necessary, reasonable or prudent safety or security measures in the eager attempt to quickly bring their product to market before their competitiors or to save on spending.

5.2.5. Initial Familiarity

Initial familiarity had a positive significant, although weak, path-coefficient to initial technology trust in emerging technologies. However, when tested with non-emerging technologies this was no longer significant. This indicates initial familiarity is applicable to emerging technologies as a predictor of initial technology trust formation, rather than non-emerging technologies. This was expected since more second-hand knowledge is available for non-emerging technologies for individuals to rely upon, and familiarity is formed from both first-hand experiences and second-hand knowledge (Bandura, 1997; Gefen, 2000; McKnight et al., 2014; Wingreen & Baglione, 2005). In addition, individuals are generally

more unaware about emerging technologies and recognise their greater complexity, which leads to greater uncertainty (Conger et al., 2013).

Familiarity creates a reference point for individuals without prior experience of an emerging technology by affecting their initial expectations of its functionality, reliability and effectiveness as they attempt to make sense of the uncertainty (Bandura, 1997; Gefen, 2000). The results indicate greater familiarity will lead to greater initial technology trust in emerging technologies because of the greater confidence individuals have in forming their initial trust beliefs. Consequently, when familiarity is low, individuals are stuck in a state of uncertainty. This will likely cause initial technology trust levels to remain low because no initial expectations can be set which increases an emerging technology's associated risk due to its lack of predictability.

This result supports other research which has found a positive relationship between familiarity and initial trust (Gefen, 2000; Lewicki et al., 2006; Mazey & Wingreen, 2017; McKnight et al., 2011; McKnight et al., 2014; Wingreen & Baglione, 2005). This is because when low levels of familiarity exist, individuals perceive greater uncertainty and are more sensitive to risk (Satterfield et al., 2009).

Initial familiarity was also found to have an interaction effect on the relationship between perceived threats to PIP and initial trust in emerging technologies. Considering the impact of familiarity on trust, this should not come as a surprise. Like trust, familiarity would influence the expectations of PIP threats and their likelihood, which would impact the risk calculated by individuals. Consequently, initial familiarity has a direct and indirect effect on initial trust in emerging technologies because of this interaction effect.

5.2.6. Disposition to Trust Generally & Disposition to Technology Trust

Disposition to trust in general and disposition to technology trust both had significant, but weak path-coefficients to initial technology trust in emerging technologies. Surprisingly, neither finding held for initial technology trust in non-emerging technologies with both path-coefficients no longer significant. This would suggest an individuals' disposition to trust is significant for emerging technologies, but not non-emerging technologies. This result has not been found in other technology trust, or even people-related trust, research before. Previous research has found an individual's general willingness to be vulnerable and accept risks will

affect their trust beliefs, whether this be in an initial trust formation or when a trust history already exists (H. C. Brown et al., 2004; Ellingson, 2003; Gefen, 2000; Gefen et al., 2008; Hommel & Colzato, 2015; Lewicki et al., 2006; Li et al., 2008; Li et al., 2012; Lippert & Davis, 2006; Xin Luo et al., 2010; Mayer et al., 1995; McKnight et al., 2011; McKnight & Chervany, 2001; McKnight et al., 1998; McKnight et al., 2014; Rotter, 1971; Rousseau et al., 1998). More specifically, this result is also contrary to other technology trust research which found a positive relationship between disposition to trust and technology trust and who, in some cases, also used the same instrument scale (H. C. Brown et al., 2004; Li et al., 2008; McKnight et al., 2011; Wingreen & Baglione, 2005).

5.2.7. CONCLUSION

Overall, the PLS-SEM analysis appears to support the initial technology trust model proposed for emerging technologies as compared to non-emerging technologies. While many path-coefficients were weak, this is likely because of the model's exclusion of other known technology trust antecedents. Previous research has established other antecedents to technology adoption and trust which were not tested here. These include perceived usefulness and perceived ease of use, self-efficacy, facilitating conditions and systems quality (Davis, 1989; Fathema et al., 2014; Fathema et al., 2015; Venkatesh, 2000; Venkatesh & Bala, 2008; Venkatesh & Davis, 2000). However, the purpose of this research was to explore the significance of factors not previously considered by prior research and to supplement the findings of the primary experiment.

The findings of this study offer new variables not yet previously considered in technology trust research: subjective norms, faith in humanity as a substitute for vendor-based trust, the perceived safety of the economic environment and initial familiarity, as well as perceived threats to PIP and the characteristics of emerging technology artefacts. The variance explained by these effects examined in the PLS-SEM analysis should supplement previously known effects of established technology trust research and result in stronger, more complete models. It also addresses the difference in effects of emerging and non-emerging technologies, not previously considered in prior research. In particular, the results indicate that perceived threats to PIP, familiarity and disposition to trust generally and disposition to technology trust are relevant factors for initial trust in emerging technologies but become less significant for non-emerging technologies. In addition, the characteristics of emerging technologies have a significant effect of perceived threats to PIP which do not apply to non-

emerging technology PIP threats. The results also indicate that subjective norms, faith in humanity and the economic environment are applicable to both classes of technologies. Evidence was also found to suggest that subjective norms is an antecedent to perceived threats to PIP.

5.3. Key Limitations

Several limitations exist for this research, conducted as a secondary study in this thesis. This study was planned after the completion of the first study related to the primary experiment and utilised the additional data that was collected from it. Firstly, this means that when the instruments were designed, they were not designed with the purpose of a PLS-SEM analysis in mind as the requirements they may have needed to meet to ensure reliable results. In hindsight, the measures for familiarity and the economic environment could have been designed to have included one or two more items for greater assurance of their effectiveness in capturing the constructs intended. This is because single item measures can inflate means (Ringle et al., 2012). However, Hair et al. (2011) state that PLS-SEM's less restrictive measures of constructs means that it is well equipped to handle low variable item counts.

Since the data used in the PLS-SEM was sourced from the primary experiment, the results may be less reliable given the lack of external validity in experimental research (Mook, 1983). The PLS-SEM method is supposed to address some of these issues in its method of calculation (Chin, 1998; Chin et al., 2012; Garson, 2016; Hair et al., 2011; Hair et al., 1998; Ringle et al., 2012; Wong, 2013). However, whether PLS-SEM removed this inherent characteristic of the source data completely cannot be assured and it is more likely that this limitation was mitigated rather than removed entirely.

With specific regard to PLS-SEM techniques, it is important to acknowledge that there is no single accepted measure of fit and attempts to evaluate measure of fit should be done with caution and scepticism (Hair et al., 2011). It also fails to consider bilateral relationships and is susceptible to biased component estimation of loadings and coefficients (Wong, 2013).
The initial technology trust model proposed for analysis in PLS-SEM also posed problematic given that it includes second and third latent order variables. This meant procedures had to be performed in three stages before being able to establish a complete view of the model and its results, analysing first the third order latent variables, then the second order latent variables before combining all the variables. It has been noted that efforts to evaluate the outer model

for PLS-SEM models which contain second and third order latent variables are less reliable compared to simpler first order models (Chin et al., 2012; Lowry & Gaskin, 2014). Since most PLS-SEM research generally limits itself to first order models less commentary is available about maintaining internal reliability so it is possible better methods exist to handle a multi-order latent variable model which were not included in this research.

With regard to statistical power analyses in this research, it should be noted that although there is increasing demand for such analyses in Information Systems research, there is little agreement on the best methods to determine power or how to perform power analyses, let alone with specific regard to PLS-SEM research (Chin, 1998; Cohen, 1988; Esposito Vinzi, 2010; Faul et al., 2009; Faul et al., 2007; Garson, 2016; Hair et al., 2011; Lowry & Gaskin, 2014; Miguel & Mikko, 2015; Peng & Lai, 2012). G*Power software is a popular software specialising in statistical power computation, based on the theories of Faul et al. (2007) and Faul et al. (2009) and developed by its authors. The choice of this method was intended to mitigate the risk of an unreliable power analysis procedure and increase statistical conclusion validity. However, it is possible that these methods may be found statistically inaccurate or unreliable as the research into appropriate statistical power analyses and procedures develop further.

SECTION 6. CONTRIBUTIONS

It is anticipated that the findings of this research will provide academics and practitioners with an understanding about what factors influence initial trust in new or unfamiliar technologies, with empirical support. Given our fast paced and technology driven society this could be invaluable.

Initial trust is when individuals first interact with a person or object and trust beliefs are unable to be based on any personal experience or first-hand knowledge (Li et al., 2008; McKnight et al., 1998). It is the point from which future experiences are based upon and from which trust increases or decreases over time (Gefen et al., 2008; Lewicki et al., 2006; McKnight et al., 1998; Rousseau et al., 1998). Trust motivates behaviour and influences technology adoption (Gefen et al., 2008; Li et al., 2008; Lippert & Davis, 2006; Xin Luo et al., 2010; McKnight et al., 2011; McKnight et al., 2014; Pavlou, 2003). Therefore, initial technology trust beliefs can be pivotal in establishing new expectations and patterns of behaviour for technology users going into the future. If initial trust beliefs are relatively low, individuals may be less tolerant towards uncertainty and unlikely to accept risk when deciding whether to trust something new and unfamiliar. In addition, low or negative trust beliefs may skew any positive experiences individuals may have and frame future experiences and expectations. It could even lead to distrust which promotes active avoidance behaviour (Gefen et al., 2008; Lewicki et al., 2006). Emerging technologies lack similarity to other non-emerging technologies and have unique PIP risks relating to intrusiveness, omnipotence and invisibility. Generally, when individuals are first confronted with emerging technologies in a trust situation they have little first-hand experience or knowledge of them. As such, the amount of risk and uncertainty individuals must grapple with in determining their initial trust beliefs will surely be at their highest when compared to non-emerging technologies.

For academics, this research helps to identify the different variables at play when deciding whether to trust and adopt emerging technologies. It identifies PIP threats as a significant factor in our cognitive evaluation of technology trustworthiness and supplements this with strong casual evidence using experimental procedure. This can be used to create opportunities to support an individual's transition to new technologies in technology adoption research by offering insight to the underlying trust dilemmas facing technology users. This research

consolidates and makes sense of a wide range of trust theory from a number of different academic disciplines, such as Information Systems, Psychology, Economics, Science and Legal. In this thesis, significant findings, models and literature across these disciplines are considered in the context of technology trust in this thesis, while also recognising the difference between the domains of emerging and non-emerging technologies. Additionally, by identifying the causal relationship between technology trust and specific emerging technology characteristics which pose a threat to PIP, this research succeeds in better contextualising the trust literature for the Information Systems domain and future technology trust research (Hong, Chan, Thong, Chasalow, & Gurpreet, 2014). It also provides a clear example and methodology for modelling third order PLS-SEM models.

This research contributes practical knowledge for practitioners. In particular, it offers practical insight to increase organisational technology use, IT implementation success and the acceptance and use of consumer technologies in society by providing the tools to understand and support technology trust formation. Understanding the uniqueness of initial trust formation, and how it transforms, can enable practitioners to effectively support individuals who are confronted with new emerging technologies and their associated technology dilemmas. This insight can be used to manage technology trust expectations and relationships to promote positive technology trust experiences and history over time. Conversely, this research equips practitioners with knowledge of factors which may lead to technology distrust so that they may implement procedures and controls to mitigate the technology characteristics and situations which may undermine or negatively impact trust beliefs. Consequently, practitioners are also likely to find the knowledge cultivated in this research to be relevant for change management, marketing and technology design by ensuring suitable controls are designed in technology solutions, goods, services and business processes to promote technology trust. The relative increase in technology trust may encourage greater sales, technology use, organisational reputation and brand loyalty. Effective development, management and protection of technology trust could be leveraged as a valuable competitive differentiator. Moreover, technology trust may even prove to be a useful insurance policy to mitigate the reputational and trust impacts of data breaches as technology-related incidents become a common place media headline.

Specifically, this research offers the following key contributions:

1. A framework was created to test and identify whether technologies are truly "emergent" based on the conceptualisations of Einsiedel (2008) and be classified as an "emerging technology." This framework differentiates emerging technologies from non-emerging technologies according to three unique characteristics: innovativeness, transformative and uninhibited. An emerging technology's "innovativeness" suggests that it is in the early stages of commercialisation, development state of production or not yet fully exploited because of its originality and new, novel way of existing or performing. If an emerging technology is expected to significantly change the way in which people in society live their lives, interact with each other, socialise and survive, or if it changes or disrupts economic markets and industries, or change traditional relationships in society, then it is "transformative." Finally, an emerging technology's "uninhibited" nature refers to its tendency to be relatively uncontrolled and evolutionary in their development, deployment and use, and it may therefore require restraint which triggers change to laws and regulations. The characteristics innovativeness and transformative were both validated in this research, although uninhibited was unable to be fully supported. These characteristics, and the instruments developed, have not been theorised or tested in previous research. They provide opportunity to enable more consistent use of terminology relating to emerging technologies among academics and practitioners when discussing emerging technologies as opposed to non-emerging technologies. It is expected this definition will persist over time even as the instances of emerging technologies change. An opportunity exists for academics to reuse, retest and refine these characteristics and instruments in future research.

2. Definitions were proposed for each of Conger et al. (2013)'s theorised emerging technology characteristics which present a threat to PIP. Conger et al. (2013)'s characteristic of ubiquity was severed to account for the ubiquitous physical and network states of emerging technologies. These characteristics, and their definitions, provide academics and practitioners new terminology and understanding of emerging technologies and their innate threats to PIP.

It was noted that as emerging technologies transition to a state of non-emergence, these PIP threats will remain an inherent characteristic. As the development and implementation of emerging technologies increase, emerging technologies will populate society and become the new standard of technology. Consequently, in the future these PIP threats will no longer be unique to emerging technologies as a class but rather emerging and non-emerging

technologies generally. Academics and practitioners must be considerate of this. Researchers should continue to test whether these PIP threats are unique to emerging technologies since a time will come in which today's emerging technologies transition to a non-emerging technology state. A time may also come when both classes of emerging and non-emerging technologies share an inherent PIP threat, no longer making inherent PIP threat unique to emerging technologies.

3. New privacy adapted instruments were developed to complement the existing instrumentation for the technology trust antecedents of functionality, effectiveness and reliability, and the institutional-based trust antecedents of structural assurance and situational normality. These PIP adapted instruments were validated in experimental procedure and are now available for future technology trust research to promote strong external reliability. They are also relevant for future technology trust research in emerging technologies and non-emerging technologies, albeit in separate ways. The PIP adapted instruments should be used in emerging technology trust research as originally designed in this research, with one privacy adapted instrument existing to supplement each of McKnight et al. (2011)'s technology trust antecedents. However, when modelling initial trust in non-emerging technologies, the instruments should be used together to form the newly discovered technology trust antecedent "data integrity."

4. A new technology trust antecedent called "data integrity" was discovered for non-emerging technologies. This is a significant academic contribution for technology trust research which currently fails to distinguish between emerging and non-emerging technology classes, or acknowledge that a data integrity belief exists as a relevant antecedent for non-emerging technologies. An individual's beliefs in data integrity relates to whether a technology has the ability to act according to the best interests of the user's privacy and whether it will exploit or abuse its ability to collect or share personal information. This was discovered in section 4.1.1 using exploratory factor analyses where the emerging and non-emerging technology data resulted in two different factor structures. Data integrity was only found for non-emerging technology and did not exist when tested against emerging technologies. This indicates current popular technology trust models are incomplete with the absence of the data integrity antecedent. Moreover, emerging and non-emerging technologies cannot be assumed to be the same in the context of initial trust. Instead, different cognitive processes exist when evaluating emerging and non-emerging technologies trust beliefs. When

evaluating both initial technology trust models, the experiment also suggests situational normality should be removed from both initial technology trust models, which is contrary to existing technology trust research.

5. A factor structure for Conger et al. (2013)'s characteristics of emerging technologies that present threats to PIP was discovered, which was neither predicted nor theorised. This relates to an emerging technology's intrusiveness (as invasiveness, collectability of information and wireless accessibility), omnipotence (as physical ubiquity, network ubiquity and programmability) and invisibility. This research considered the criticisms of the Kaiser criterion in current literature and its limitations relating to its objectivity, and that theoretical considerations and research context should be accounted for, and sound judgement exercised in exploratory factor analyses (Patil et al., 2007; B. Williams et al., 2010). This research provides support for this argument by accepting the invisibility factor which had a factor loading of 0.96 and Eigenvalue of 0.97. It encourages other academics to exercise more judgement and subjectivity for exploratory factor analysis in exploratory research rather than relying on the traditional Kaiser criterion which does not distinguish between exploratory and confirmatory research or consider theoretical or research context.

6. The perceived PIP threat factor structure was found to have a negative causal relationship with initial technology trust in emerging technologies in the primary experiment. The PLS-SEM analysis supported this. The experiment results suggest these PIP threats are not considered equally and some may be more important than others with each technology presenting a unique blend of perceived PIP threats. In particular, it seems individuals have a higher tolerance for invisibility related PIP threats compared to PIP threats resulting from an emerging technology's omnipotence or invasiveness. This tolerance may be useful consideration for academics in privacy paradox research (Holland, 2010; Motiwalla & Li, 2016; Norberg et al., 2007; Young & Quan-Haase, 2013). This understanding about the key PIP threats perceived by individuals is also valuable to practitioners. They can act with greater assurance that introducing additional measures, controls and functionality in technology designs and processes will mitigate perceived PIP risks. Consequently, practitioners may increase the likelihood consumers and end users will have positive initial technology trust beliefs by enabling a more transparent and trust promoting user experience and interactions with technologies.

7. A clear, structured methodology was described for the use of third order PLS-SEM modelling. Discussion about second and third order models are relatively rare in the existing literature, and clear examples and tutorials on how to perform PLS-SEM procedures for these models are rarer. This thesis provides a clear roadmap to perform third order PLS-SEM, and can be replicated in second order models, in SmartPLS 3 which is valuable for academics who are not proficient in PLS-SEM. The detail provided should also enrichen the literature by providing academics a consistent approach to increase external reliability among Information Systems research using PLS-SEM and other research disciplines.

8. The PLS-SEM analysis provided evidence for the validity and reliability of the initial technology trust model proposed. It illustrated that perceived threats to PIP, subjective norms, faith in humanity, familiarity, disposition to technology trust and disposition to trust generally all have a predictive effect on initial technology trust and that subjective norms also influence perceived threats to PIP. Additionally, the experiment showed each of these factors, as well as the economic environment, have a significant covariate effect on the casual relationship between perceived threats to PIP and initial technology trust in emerging technologies. These variables have not been theorised or proposed in technology trust research before. They offer insight into the dilemma faced by individuals when they attempt to establish initial trust levels for an emerging technology that they have no experience or limited knowledge of, and what factors influence these trust beliefs. This gives academics the opportunity to strengthen existing and future trust research, which may be relevant for people-related trust as well as technology-related trust, by validating and incorporating the use of faith in humanity, the perceived safety of the economic environment and subjective norms constructs.

9. The PLS-SEM analysis demonstrated that two very different cognitive processes exist for the initial technology trust formation in emerging and non-emerging technologies. This is contrary to existing research. Two different initial trust models exist for both types of technologies. It is theorised that a hierarchy of needs may exist for satisfying initial technology trust beliefs and that the initial technology trust antecedents of a technology artefact will take precedence over secondary factors such as faith in humanity, subjective norms, familiarity and disposition for emerging technologies as opposed to non-emerging technologies. This requires further enquiry and testing. While the model excluded many variables known to influence people related trust and technology adoption, the stark difference in significant paths is very relevant for any academics in technology trust and

adoption research. These results provide a strong argument from which academic researchers should further investigate the differences between emerging and non-emerging technologies, or any other classes of technology which may exist. Further understanding of these differences is of significant value to the academic literature as it offers contextualisation of technology trust literature across different circumstances and classes of technology (Hong et al., 2014). This will provide richer insight and understanding to academics about how technology trust beliefs form for different technologies, including what factors individuals are most concerned about and how organisations can best support initial trust formation, user experience and interaction with technology. In turn, this should prompt practitioners to better understand and empathise with their users and their priorities, and invest more appropriately for these.

A knowledge gap exists in the Information Systems trust literature regarding technology trust. This research proposes a starting point in which further trust research can be carried out by identifying factors which affect initial technology trust formation for both emerging and non-emerging technologies. This is anticipated to assist the understanding of the development of trust over time. Moreover, the discovery of the connection between trust and PIP research in technology artefacts has exposed a major gap in the existing literature and is an area that has largely been left neglected. This is surprising given the increased public attention on individual data security and the implementation of new international data protection and privacy laws, such as the European Union's General Data Protection Regulation (GDPR) in May 2018 which has disrupted many organisations and has drawn a large amount of media publicity. Additionally, at the time of this thesis, other recent changes include the draft New Zealand Privacy Bill and Indian Data Privacy Law, Australia's Privacy Amendment (Notifiable Data Breaches) Act 2017, Japan's Japanese Act on Protection of Personal Information 2017 and Brazil's General Data Protection Law 2018.

This research bought together many types of trust research, including people-related trust, knowledge-based trust, e-commerce trust and technology trust, and related this to privacy, psychology and technology adoption literature. By combining and proposing variables from each of these fields and ensuring they are congruent with one another, this research provides a more cohesive, integrated approach to understanding initial technology trust than previous research. Furthermore, the consistency of findings in this research with prior research from various disciplines affirms the external reliability of the results and the new variables

proposed in the initial technology trust model for emerging technologies. Together, this thesis provides significant theoretical, methodological and practical contributions.

SECTION 7. CONCLUSION

The purpose of this research was to address the research question: "*What influences individuals to decide whether they trust emerging technologies without prior experience or knowledge of the technology?"* In particular, it sought to determine whether perceived threats to individual's PIP would decrease their initial technology trust in emerging technologies, and vice versa, through experimental procedure and PLS-SEM analysis.

The choice in methodology was carefully chosen based on the current status of existing trust research, which mostly consisted of theoretical frameworks, surveys and field studies. As such, it offers strong external reliability by combining and proposing variables from prior research, many of which lack internal validity or reliability and overall cohesiveness regarding technology trust. It also provides a clear roadmap for how to appropriately perform and analyse PLS-SEM procedures for third order models. This is its main methodological contribution. However, it also demonstrates support for the argument that factor analyses should be interpreted with additional judgement and consideration for the type of research, its goals and context, instead of depending on the rigid, objective Kaiser criterion (Patil et al., 2007; B. Williams et al., 2010). In this case, a third factor identified in the exploratory factor analysis for PIP threats was included considering that this research was exploratory in nature, a high factor loading of 0.96 and Eigenvalue of 0.97.

Several significant academic contributions were made in this thesis. Firstly, it establishes a framework to test whether a technology is "emergent" according to the characteristics innovativeness and transformative, and provides a clear definition and standard for emerging technologies for consistent meaning and use of terminology. Previously identified PIP threats for emerging technologies were defined, further developed and validated. A factor structure for these PIP threats were discovered, identifying three primary types of PIP threats: intrusiveness (as invasiveness, collectability of information and wireless accessibility), omnipotence (as physical ubiquity, network ubiquity and programmability) and invisibility. These were found to have a negative relationship with initial technology trust in emerging technologies when testing 3D printing, autonomous cars, bionano sensors and drones as instances of emerging technologies. Results found varying levels of perceived PIP threats across emerging technologies and their impact across the initial technology trust antecedents identified by McKnight et al. (2011). It was postulated that perhaps individuals have a higher

tolerance for a technology's invisibility and the possible threat to PIP this would infer. This research also found strong evidence to suggest McKnight et al. (2011)'s popular technology model is incomplete and two different initial trust processes exist for emerging and non-emerging technologies. This was identified with the discovery of the data integrity antecedent for technology trust which only exists for non-emerging technologies. Consequently, two different models for initial technology trust beliefs were revealed for emerging and non-emerging technologies. The PLS-SEM procedures also found evidence to argue that subjective norms and faith in humanity should be included in technology trust research, as well as the safety of the economic environment which has not been tested before. It was recommended these be included in popular people-related trust models too since they generally seem to be absent.

This thesis provides practitioners insight into individuals' technology trust dilemmas and provides valuable understanding about the factors which practitioners should invest, promote and protect to encourage initial technology trust for emerging technologies which individuals' have no experience or little familiarity of. Used wisely, practitioners can use this knowledge to foster technology trust beliefs to encourage technology intentions and positive adoption behaviours, thereby increasing market uptake, organisational technology deployment and use, IT implementation success and the positive acceptance and use of consumer technologies in society. Understanding the uniqueness of initial trust formation, and how it transforms, can enable practitioners to effectively support individuals over time and more effectively manage their expectations, experiences and technology trust history in a positive way. Conversely, this research equips practitioners with knowledge of factors which may lead to technology distrust and can empower them to implement procedures and controls to mitigate the event of particular technology characteristics and situations which may undermine or negatively impact trust beliefs. Consequently, practitioners may find the knowledge cultivated in this research to be relevant for change management, marketing and technology design by ensuring suitable controls are designed in technology solutions, goods, services and business processes to promote technology trust. With the overuse of the term "emerging technology" in industry, practitioners are also encouraged to use the frameworks, definitions and benchmarks for an "emerging technology" in section 2.5.2 and section 4.1.2 for more accurate and consistent terminology.

Vance et al. (2008) stated “trust issues are on the forefront when users adopt new technologies,” which highlights the significance of this research, and its potential. Existing research has already established the importance of technology trust and further research would be invaluable (Gefen et al., 2008; Li et al., 2008; Lippert & Davis, 2006; Xin Luo et al., 2010; McKnight et al., 2011; McKnight et al., 2014; Pavlou, 2003). Building on McKnight et al. (2011)’s technology trust framework, this research has successfully shed light on the field of technology trust. It has illustrated that perceived threats to PIP has a negative relationship with initial technology trust for emerging technologies as well as several other factors which had not yet been considered in trust research. It proposed a new model for initial trust in emerging technologies and established its uniqueness from the initial trust formation in non-emerging technologies. The incoming generation of “emerging” technologies uniquely embody the characteristics of intrusiveness, omnipotence and invisibility, which simultaneously pose a threat to PIP. Eventually, these technologies will inhabit society and change our existing standard of technologies, making the significance of future applications and extensions of this research more prevalent. This research presents a cohesive starting point for future technology trust research by offering an integrated theoretical foundation for technology trust, identifying the significant relationship that exists between technology trust and perceived threats to PIP in emerging technologies, and an initial technology trust model with established significance and validity.

SECTION 8. REFERENCES

Allianz-Aktiengesellschaft, & OECD. (2005). *Opportunities and risks of nanotechnologies: report in co-operation with the OECD International Futures Programme*: Allianz Center for Technology.

Arora, S. K., Youtie, J., Shapira, P., Gao, L., & Ma, T. (2013). Entry strategies in an emerging technology: a pilot web-based study of graphene firms. *Sciencemetrics, Vol. 95*(3), 1189-1207.

Bacca, J., Baldiris, S., Fabregat, R., Graf, S., & Kinshuk. (2014). Augmented reality trends in eduction: a systematic review of research and applications. *Educational Technology & Society, Vol. 17*(2), 133-149.

Bandura, A. (1997). *Self-efficacy: the exercise of control*. New York: W.H. Freeman.

Behrang, R., Bornemann, D., Hansen, U., & Schrader, U. (2006). Consumer power: a comparison of the old economy and the internet economy. *Journal of Consumer Policy, Vol. 29*(1), 3-36.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly, Vol. 35*(4), 1017-1041.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods and Practises*: Textbook Collections; http://scholarcommons.usf.edu/oa_textbooks/3.

Brown, H. C., Poole, M. S., & Rodgers, T. L. (2004). Interpersonal traits, complementarity and trust in virtual colloboration. *Journal of Management Information Systems, Vol. 20*(4), 115-137.

Brown, M. M. (2015). Revisiting the IT productivity paradox. *American Review of Public Administration, Vol. 45*(5), 565-583.

Bryman, A., & Bell, E. (2011). *Business Reseach Methods*. USA: Oxford University Press Inc.

Burchell, B., & Wilkinson, F. (1997). Trust, business relationships and the contractual environment. *Cambridge Journal of Economics, Vol. 21*(2), 217-239.

Chen, Y.-H., & Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial Management & Data Systems, Vol. 107*(1), 21-36.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modelling. *MIS Quarterly, Vol. 22*(1), vii-xvi.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2012, December, 1996). *A partial least squares latent variable modeling approach for measuring interaction effects: results from a monte carlo simulation study and voice mail emotion/adoption study.* Paper presented at the Proceedings of the Seventeenth Internation Conference on Information Systems, Cleveland, Ohio.

Clothier, R. A., Greer, D. A., Greer, D. G., & Mehta, A. M. (2015). Risk perception and the public acceptance of drones. *Risk Analysis, Vol. 35*(6), 1167-1183.

Cobelli, N., Gill, L., Cassia, F., & Ugolini, M. (2014). Factors that influence intent to adopt a hearing aid among older people in Italy. *Health and Social Care in the Community, Vol. 22*(6), 612-622.

Cohen, J. (1988). *Statistical power analysis for the behavioural sciences*. Mahwah, NJ: Lawrence Erlbaum.

Cohen, J. (1992). A power primer. *Quantitative Methods in Psychology, Vol. 112*(1), 155-160.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal, Vol. 23*(5), 401-417.

Costello, A. B., & Osbourne, J. W. (2005). Best practises in exploratory factor analysis: four recommendations for getting the most from your analysis. *Practical Assessment, Research & Evaluation, Vol. 10*(7), 1-9.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, Vol. 13*(3), 319-340.

Delgado-Ballester, E., & Munuera-Alemán, J. L. (2001). Brand trust in the context of consumer loyalty. *European Journal of Marketing, Vol. 35*(11/12), 1238-1258.

Dick, A. S., & Basu, K. (1994). Customer loyalty: toward an integrated conceptual framework. *Journal of the Academy of Marketing Science, Vol. 22*(2), 99-113.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary - informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Information Systems Research, Vol. 26*(4), 639-655.
Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: an integrated model of privacy concerns, trust and commitment. *Journal of Business Research, Vol. 59*(8), 877-886.
Einsiedel, E. F. (2008). Emerging Technologies: From hindsight to foresight. Vancouver, BC, CAN: UBC Press.
Ellingson, G. (2003). The role of trust in knowledge management: a case study of physicians at work at the university hospital of northern norway. *Informing Science, Vol. 6*, 193-207.
Enders, C. K. (2003). Using the expectation maximization algorithm to estimate coefficient alpha for scales with item-level missing data. *Psychological Methods, Vol. 8*(3), 322-337.
Enders, C. K. (2010). *Applied missing data analysis*. New York: Guilford Press.
Esposito Vinzi, V. (2010). *Handbook of partial least squares: concepts, methods and applications*. New York, Berlin: Springer.
Fathema, N., Ross, M., & Witte, M. (2014). Student acceptnace of university web portals: a quantitative study. *International Journal of Web Portals, Vol. 6*(2), 42-58.
Fathema, N., Shannon, D., & Ross, M. (2015). Expanding the technology acceptance model (TAM) to examine faculty use of learning management systems (LMS). *Journal of Online Learning and Teaching, Vol. 11*(2), 210-233.
Faul, F., Erdfelder, E., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, Vol. 41*, 1149-1160.
Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioural, and biomedical sciences. *Behavior Research Methods, Vol. 39*, 175-191.
Fredrich, J. T., Lakshtanov, D. L., Lane, N. M., Liu, E., B, Natarajan, C. S., Ni, D. M., & Toms, J. J. (2014). Digitial rocks: developing an emerging technology through to a proven capability deployed in the business. *Society of Petroleum Engineers*.
Garson, G. D. (2016). *Partial least squares: regression & structural equation models*: Statistcial Associates Publishing.
Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega, Vol. 28*(6), 725-737.
Gefen, D., Benbasat, I., & Pavlou, P. (2008). A research agenda for trust in online environments. *Journal of Management Information Systems, Vol. 24*(4), 275-286.
Graham, J. W. (2009). Missing data analysis: making it work in the real world. *Annual Review of Psychology, Vol. 60*(1), 549-576.
Grewal, D., Roggeveen, A. L., & Nordfält, J. (2017). The future of retailing. *Journal of Retailing, Vol. 93*(1), 1-6.
Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory & Practise, Vol. 19*(2), 139-152.
Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM): an emerging tool in business research. *European Business Review, Vol. 26*(2), 106-121.
Hair, J. F., Tatham, R. L., Anderson, R. E., & Black, W. (1998). *Multivariate data analysis* (5th ed.). London: Prentice-Hall.
Hajli, M., Sims, J. M., & Ibragimov, V. (2015). Information technology (IT) productivity paradox in the 21st century. *International Journal of Productivity and Performance Management, Vol. 64*(4), 457-478.
Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, Vol. 43*(1), 115-135.
Hoe, S. L. (2008). Issues and procedures in adopting structural equation modeling technique. *Journal of Applied Quantitative Methods, Vol. 3*(1), 76-84.
Holland, H. B. (2010). Privacy paradox 2.0. *Widener Law Journal, Vol. 19*(3), 893-932.
Hommel, B., & Colzato, L. S. (2015). Interpersonal trust: an event-based account. *Frontiers in Psychology, Vol. 6*, 1-4.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Gurpreet, D. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research, Vol. 25*(1), 111-136.
Jones, R. W., & Ruffin, R. J. (2008). The technology transfer paradox. *Journal of International Economics, Vol. 75*(2), 321-328.
Jones, S. S., Heaton, P. S., Rudin, R. S., & Schneider, E. C. (2012). Unraveling the IT productivity paradox - lessons for health care. *New England Journal of Medicine, Vol. 366*(24), 2243-2245.
Kaushik, A. K., & Rahman, Z. (2015). An alternative model of self-service retail technology adoption. *Journal of Services Marketing, Vol. 29*(5), 406-420.
Lafrance, A. (2016). How self-driving cars will threaten privacy. Retrieved from https://www.theatlantic.com/technology/archive/2016/03/self-driving-cars-and-the-looming-privacy-apocalypse/474600/, published on the 21 March 2016
Lau, C. M., & Tan, C. L. C. (2006). The effects of procedural fairness and interpersonal trust on job tension in budgetting. *Management Accounting Research, Vol. 17*(2), 171-186.
Lee, J., Lee, J.-N., & Tan, B. C. Y. (2012). Antecedents of cognitive trust and affective distrust and thier mediating roles in building customer loyalty. *Information Systems Frontier, Vol. 17*(1), 159-175.
Leggett, D. (2017). *Five trends that will reshape the auto industry by 2030: How electrification, autonomous cars, urban mobility, connectivity, and emerging markets will change the auto industry*: Bromsgrove: Aroq Limited.
Lewicki, R. J., Tomlinson, E. C., & Gillespie, N. (2006). Model of interpersonal trust development: theoretical approaches, empirical evidence and future directions. *Journal of Management, Vol. 32*(6), 991-1022.
Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems, Vol. 17*(1), 39-71.
Li, X., Rong, G., & Thatcher, J. B. (2012). Does technology trust substitute interpersonal trust? Examining technology trust's influence on individual decision making. *Journal of Organizational and End User Computing, Vol. 24*(2), 18-38.
Lippert, S., & Davis, M. (2006). A conceptual model integrating trust into planned change activities to enhance technology adoption behavior. *Journal of information science, Vol. 32*(5).
Little, T. D. (2013). *The Oxford handbook of quantitative methods*. Oxford: Oxford University Press.
Lowry, P. B., & Gaskin, J. (2014). PLS SEM for building and testing behavioral causal theory. *IEEE Transactions on Professional Communication, Vol. 57*(2), 123-159.
Luo, X. (2002). Trust production and privacy concerns on the internet: a framework based on relationship marketing and social exchange theory. *Industrial Marketing Management, Vol. 31*, 111-118.
Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems, Vol. 49*(2), 222-234.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns: the construct, the scale, and a causal model". *Information Systems Research, Vol. 15*(4), 336-355.
Martin, G., Gupta, H., Wingreen, S. C., & Mills, A. M. (2015). *An analysis of personal information privacy concerns using Q-methodology*. Paper presented at the Australasian Conferencce on Information Systems, Adelaide, Australia.
Mayer, R. C., Davis, J. H., & David Schoorman, F. (1995). An integrative model of organizational trust. *Academy of Management, Vol. 20*(3), 709-734.
Mazey, N. C. H. L., & Wingreen, S. C. (2017). Perceptions of trust in bionano sensors: Is it against our better judgement? An investigation of generalised expectanices and the emerging technology trust paradox. *International Journal of Distributed Sensor Networks, Vol. 13*(7), 1-16.
Mazza, G. L., Enders, C. K., & Ruehlman, L. S. (2015). Addressing item-level missing data: a comparison of proration and full information maximum likelihood estimation. *Multivariate Behavioral Research, Vol. 50*(5), 504-519. doi:10.1080/00273171.2015.1068157

McAllister, D. (1995). Affect- and cognitive-based trust as foundations for interpersonal cooperation in organisations. *Academy of Management, Vol. 38*(1), 24-59.
McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems, Vol. 2*(2), 1-25.
McKnight, D. H., & Chervany, N. L. (2001). Trust and distrust definitions: one bite at a time *Trust in Cyber-Societies: Integrating the Human and Artifical Perspectives* (Vol. Vol. 2246, pp. 27-54): Springer Berlin Heidelberg.
McKnight, D. H., Choudhury, V., & Kacmar, C. (2000). *Trust in e-commerce vendors: a two-stage model*. Paper presented at the Proceedings of the twenty first international conference on Information systems, Brisbane, Queensland, Australia.
McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management, Vol. 23*(3), 473-490.
McKnight, D. H., Liu, P., & Pentland, B. T. (2014). *A cognitive process model of trust change*. Paper presented at the International Conference on Information Systems, Auckland, New Zealand.
Metzger, M. J. (2004). Privacy, trust, and disclosure: exploring barriers to electronic commerce. *Journal of Computer Mediated Communication, Vol. 9*(4).
MGI. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. Retrieved from https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Disruptive%20technologies/MGI_Disruptive_technologies_Executive_summary_May2013.ashx
Miguel, A.-U., & Mikko, R. (2015). Sample size determination and statistical power analysis in PLS using R: An annotated tutorial. *Communications of the Association for Information Systems, Vol. 36*(1).
Mook, D. G. (1983). In defense of external invalidity. *American Psychologist, Vol. 38*(4), 379-387.
Motiwalla, L. F., & Li, X.-B. (2016). Unveiling consumers' privacy paradox behaviour in an economic exchange. *International Journal of Business Information Systems, Vol. 23*(3), 307-329. doi:10.1504/IJBIS.2016.079523
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs, Vol. 41*(1), 100-126. doi:10.1111/j.1745-6606.2006.00070.x
Ohta, H., & Ohta, H. (2008). On the "technology transfer" paradox and "worsening terms of trade" paradox. *Asia-Pacific Journal of Accounting & Economics, Vol. 15*(1), 41.
Pappila, M. (2013). Forest certification and trust - different roles in different environments. *Forest Policy and Economics, Vol. 31*, 37-43.
Parent, M. C. (2013). Handling item-level missing data: simpler is just as good. *The Counselling Psychologist, Vol. 41*, 568-600.
Patil, V. H., Singh, S., Mishra, S., & Donavan, D. T. (2007). Efficient theory development and factor retention criteria: abandon the 'eigenvalue greater than one' criterion. *Journal of Business Research, Vol. 61*, 162-170.
Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, Vol. 7*(3), 101-134.
Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior. *MIS Quarterly, Vol. 30*(1), 115-143.
Peng, D. X., & Lai, F. (2012). Using partial least squares in operations management research: A practical guideline and summary of past research. *Journal of Operations Management, Vol. 30*, 467-480.
Pidgeon, N., Harthorn, B. H., Bryant, K., & Rogers-Hayden, T. (2009). Deliberating the risks of nanotechnologies for energy and health applications in the United States and United Kingdom. *Nature Nanotechnology, Vol. 4*, 95-98.
Porter, M. E. (2001). Strategy and the internet. *Harvard Business Review, Vol. 79*(3), 63-78.

Pycroft, L., Boccard, S. G., Owen, S. L. F., Stein, J. F., Fitzgerald, J. J., Green, A. L., & Tipu, A. (2016a). Brainjacking: implant security issues in invasive neuromodulation. *World Neurosurg, Vol. 92*, 454-462.
Pycroft, L., Boccard, S. G., Owen, S. L. F., Stein, J. F., Fitzgerald, J. J., Green, A. L., & Tipu, A. (2016b). Brainjacking: implant security issues in invasive neuromodulation. *World Neurosurg, 92*, 454-462.
Rayna, T., & Striukova, L. (2016). From rapid prototyping to home fabrication: how 3D printing is changing business model innovation. *Technological Forecasting and Social Change, Vol. 102*, 214-224.
Ringle, C. M., & Sarstedt, M. (2016). Gain more insight from your PLS-SEM results: the importance-performance map analysis. *Industrial Management & Data Systems, Vol. 116*(9), 1865-1886.
Ringle, C. M., Sarstedt, M., & Straub, D. (2012). A critical look at the use of PLS-SEM in MIS Quarterly. *MIS Quarterly, Vol. 36*(1), iii-xiv.
Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. *American Psychologist, Vol. 26*(5), 443-452.
Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: a cross discipline view of trust. *Academy of Management Review, Vol. 23*(3), 393-404.
Royal Society, & Royal Academy of Engineering. (2004). *Nanoscience and Nanotechnologies: Opportunities and Uncertainties*: Royal Society.
Satterfield, T., Kandlikar, M., Beaudrie, C., & Conti, J. (2009). Anticipating the percieved risk of nanotechnologies. *Nature Nanotechnology, Vol. 4*(752-758).
Shapiro, S. (2005). Agency theory. *Annual Review of Sociology, Vol. 31*, 263-284.
Sheth, J. N. (1983). Cross-cultural influences on the buyer-seller interaction/negotiation process. *Asia Pacific Journal of Management, Vol. 1*(1), 46-55.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, Vol. 35*(4), 989-1015.
Stewart, D. W. (1985). The application and misapplication of factor analysis in marketing research *Journal of Marketing Research, Vol. 18*, 15-62.
Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validiation guidelines for IS positivist research. *Communications of the Association for Information Systems, Vol. 13*(1), 380-427.
Thaw, Y. Y., Mahmood, A. K., & Dominic, P. D. D. (2009). A study of the factors that influence the consumers' trust on e-commerce adoption. *International Journal of Computer Science and Information Security, Vol. 4*(1), 153-159.
Touhami, A. (2014). Biosensors and nanobiosensors: design and application *Nanomedine* (pp. 374-402). Manchester: One Central Press.
Usal, M., & Nouri, H. (2014). *Optical wireless communications - an emerging technology*. Paper presented at the 16th International Conference on Transparent Optical Networks, Graz, Austria.
Vance, A., Elie-Dit-Cosaque, C. W., & Straub, D. (2008). Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture. *Journal of Management Information Systems, Vol. 24*(4), 73-100.
Venkatesh, V. (2000). Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, Vol. 11*(4), 342-365.
Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, Vol. 39*(2), 273-315.
Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science, Vol. 46*(2), 186-204.
Williams, B., Onsman, A., & Brown, T. (2010). Exploratory factor analysis: a five step guide for novices. *Journal of Emergency Primary Health Care, Vol. 8*(3), 1-13.
Williams, J. D., Han, S.-L., & Qualls, W. J. (1998). A conceptual model and study of cross-cultural business relationships. *Journal of Business Research, Vol. 42*(2), 135-143.
Wingreen, S. C., & Baglione, S. L. (2005). Untangling the antecedents and covariates of e-commerce trust: institutional trust vs. knowledge based trust. *Electronic Markets, Vol. 15*(3), 246-260.

Wong, K. K. (2013). Partial least squares structural equation modelling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin, Vol. 24*(Technical Note 1), 1-32.
Yin, R. K. (2003). *Case study research: design and methods* (Vol. 5). Thousand Oaks, Calif: Sage Publications.
Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: the Internet privacy paradox revisited. *Information Communication and Society, Vol. 16*(4), 479-500.
Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of inter-organisational and inter-personal trust. *Organization Science, Vol. 9*(2), 141-159.

SECTION 9. APPENDICES

Appendix 1. Human Ethics Research Approval

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

HUMAN ETHICS COMMITTEE

Secretary, Rebecca Robinson
Telephone: +64 03 364 2987, Extn 45588
Email: human-ethics@canterbury.ac.nz

Ref: HEC 2016/40/LR

8 July 2016

Natasha Mazey
Accounting and Information Systems
UNIVERSITY OF CANTERBURY

Dear Natasha

Thank you for submitting your low risk application to the Human Ethics Committee for the research proposal titled "Trust in Emerging Technologies".

I am pleased to advise that the application has been reviewed and approved.

With best wishes for your project.

Yours sincerely

pp. R. Robinson

Jane Maidment
Chair, Human Ethics Committee

Appendix 2. Sources & Adaption of Instruments

2.1. DEPENDENT VARIABLES

Functionality *(Vance et al. 2008)*	1. I believe that [AUTONOMOUS CARS] will be competent and effective in [DRIVING TO DESTINATIONS EFFICIENTLY AND EFFECTIVELY]
	2. I believe that [AUTONOMOUS CARS] will be competent and effective in [DRIVING SAFELY]
	3. I believe that [AUTONOMOUS CARS] will perform its role [AS A MODE OF TRANSPORT] very well
	4. Overall, I believe [AUTONOMOUS CARS] are capable and proficient
(New)	5. I believe [AUTONOMOUS CARS] will be equipped with the capabilities to protect my personal information
Reliability *(Vance et al. 2008)*	6. I believe [AUTONOMOUS CARS] will not fail in its meeting its general purpose or performing tasks
	7. I believe [AUTONOMOUS CARS] will not malfunction for me
	8. I believe [AUTONOMOUS CARS] are a very reliable piece of technology
	9. I believe [AUTONOMOUS CARS] are extremely dependable
(New)	10. I believe [AUTONOMOUS CARS] could be relied upon to always protect the personal information it would collect about me
Effectiveness *(Vance et al. 2008)*	11. I believe [AUTONOMOUS CARS] will serve my best interests
	12. I believe [AUTONOMOUS CARS] will put my interests first
	13. I believe [AUTONOMOUS CARS] will be designed to learn and consider my needs and preferences when it operates
(New)	14. I believe [AUTONOMOUS CARS] will be designed to look after my privacy and will not be used against me
Structural assurance *(McKnight et al. 2011)*	15. Favourable-to-consumer legal statutes and processes make me feel secure in using [AUTONOMOUS CARS]
	16. I feel okay using [AUTONOMOUS CARS] because they are backed by vendor protections
	17. I believe effective product guarantees exist that make it feel all right to use [AUTONOMOUS CARS]
(New)	18. Privacy laws and regulations will protect my personal information collected by [AUTONOMOUS CARS]
Situational normality *(McKnight et al. 2011)*	19. I feel very good about how things will go when I use new technologies that I have not used before
	20. I am totally confident working with new technologies that I have not used before
	21. I feel very good about how things go when I use new technologies that I have not used before
	22. I believe that things will be fine when I utilised new technologies that I have not used before
(New))	23. I believe all new technologies will have effective privacy controls that make me safe

2.2. EMERGING TECHNOLOGY CHARACTERISTICS

Theory *(Sourced/Adapted from)*	**Experiment Instrument**
Not yet fully exploited *(New)*	I believe this technology is not yet fully utilised in the market place, businesses and everyday individuals in regards to its potential uses
Developmental stage of production *(New)*	I believe this technology has a long way to go in regards to development before it can be commercialised
Early stages of commercialisation *(New)*	I believe this technology is yet to reach maturity and still has a lot of potential to grow (e.g. cell phones today can access the internet, play apps and monitor your location compare to 20 years ago)
Revolutionary *(New)*	I believe this technology will be revolutionary in our everyday lives and will change the way we behave, interact and do things (e.g. cell phones have changed how we communicate and can remote control other devices)

Capacity to change a wide range of sectors *(New)*	I believe this technology will trigger changes in other industries (e.g. cell phones have changed the watch, camera, entertainment and telecommunications industries)
Change traditional relationships *(New)*	I believe this technology will trigger changes in traditional relationships (e.g. cell phones mean we can order goods and services over the phone or no longer need face to face contact to interact)
Trigger new institutional rules and arrangements *(New)*	I believe this technology will trigger changes in laws and regulations (e.g. cell phones have caused new manufacturer safety laws and have special consideration in privacy and surveillance laws)

Note: All instruments were based on the Einsiedel (2008) theory of emerging technologies.

2.3. INDEPENDENT VARIABLES/ MANIPULATION VALIDITY

Physical ubiquity *(New)*	In the future, I believe this technology will be very visible in everyday life and I will be aware of its presence
Network ubiquity *(New)*	I believe that I could identify the other organisations and systems who could view, use and record information collected by this technology (e.g. third party data collection agencies, app providers)
Invisibility *(New)*	I believe the use of this technology has the ability to operate independently without disrupting my daily activities and can be easily forgotten
Invasiveness *(New)*	The use of this technology will give it great access to information about me, my personal life and daily activities which it could potentially learn
Collectability of information *(New)*	I believe the use of this technology has the ability to collect a wide range of information about me, how it is used and the environment it is in
Programmability *(New)*	I believe that I will be able to exercise a high degree of control over this technology and its performance
Wireless accessibility *(New)*	This technology has the ability to access information from the internet, transfer information to it and communicate with other wireless devices

2.4. COVARIATES

Faith in general technology *(McKnight et al. 2011)*	1. A large majority of technologies are excellent 2. I believe that most technologies are effective at what they are designed to do 3. I think most technologies enable me to do what I need to do and effectively carry out tasks for me 4. Most technologies have the features needed to fit their purpose
Technology trust stance *(McKnight et al. 2011)*	5. I generally give a technology the benefit of the doubt the first time I use it 6. I usually trust a technology until it gives me a reason not to trust it 7. My typical approach is to trust new technologies until they prove to me I should not trust them
Faith in humanity - **Benevolence** *(Li et al. 2008)*	8. In general, vendors really do care about the well-being of others 9. The typical vendor is sincerely concerned about the problems of their customers 10. Most of the time, people care enough to try to be helpful, rather than just looking out for themselves
- **Competence** *(Li et al. 2008)*	11. I believe that most professional people do a very good job at their work 12. Most professional people are very knowledgeable in their chosen fields 13. The large majority of professional people are competent in their areas of expertise 14. In general, most vendors keep their keep their promises

- **Integrity** *(Li et al. 2008)*	15. I think vendors generally try back their words with actions 16. Most vendors are honest in their dealings with others
Subjective norms *(New)*	17. I believe that a significant number of other people will want to use this technology in their everyday life
Economic environment *(Mazey)*	18. I believe the New Zealand economic environment and the technology industry is a safe, reliable place for consumers to buy goods and with reliable consumer protections
Disposition to trust *(Wingreen & Baglione 2005/ Chen & Barnes 2007)*	19. I tend to trust a person/thing, even though I have little knowledge of it 20. It is easy for me to trust a person/thing 21. My tendency to trust a person/thing is high 22. Trusting someone or something is not difficult
Initial awareness of technologies *(New)*	23. Before reading these articles, I was very well informed about this technology, how it works, its risks and benefits

Notes to the instrumentation:

1. Given the technology trust framework adopted by McKnight et al. (2011), it was preferable that the instruments for the technology trust antecedents were also adopted. However, some instruments were insufficient and did not address the needs of this research suitably. Instead, the instruments by Vance et al. (2008) were adopted to measure the functionality and effectiveness technology trust beliefs. The measure for reliability was not adopted from Vance et al. (2008) because it only included one instrument, casting doubts over its content and construct validity. Therefore, reliability, structural assurance and situational normality were sourced from McKnight et al. (2011).
2. The use of situational normality was adapted in a slightly different manner than the rest of its counterparts. Given the nature of what situational normality is purported to measure, it did not make sense to have each of the instrumentation relate to the specific type of technology at hand, or its relevant class of technology, because similar types of used technology do not currently exist which could be fairly evaluated against as being normal. Hence, comparing situational normality to new technologies in general was considered most appropriate, given its element of uncertainty.
3. The covariate for faith in in humanity was included following a recent unpublished study conducted at the University of Canterbury. This suggested a very significant relationship exists between vendor intentions in regards to a consumer's PIP and trust. Instruments to were adapted from Li et al. (2008) and changed to refer to vendor faith rather than others in general. These instruments were adopted because they separated vendor trust into three dimensions based on the three people-related trust dimensions' benevolence, integrity and competence. It was concluded that this held greater content validity than other measures.

Appendix 3. Experiment Treatments

3.1. AUTONOMOUS CARS

EMERGING TECHNOLOGY RESEARCH

Part 1 – Please answer the general questions below.

The following questions are general questions about you and whether you knew about the contents of this research prior to participating in it.

– No information collected in this research will be personally identifiable. All data will be anonymous.

1. For keying purposes only – please write the first four letters of your surname, followed by the 4 letters of your student ID. e.g. SMIT3599

_/

2. General demographic data
   a. What year of study are you at University?
      - 1st year
      - 2nd year
      - 3rd year
      - 4th year or higher

   b. What is your age?

   c. What gender are you?
      - Male
      - Female

3. Did you speak with any of your classmates about this research, the questionnaire or the technology that was described at the beginning of this questionnaire, before participating in this research?
   - Yes
   - No

4. What class were you in when participating in this research?
   - Monday, 1pm
   - Monday, 2pm
   - Monday, 3pm
   - Tuesday, 11am
   - Tuesday, 12pm
   - Tuesday, 1pm
   - Wednesday, 10am
   - Wednesday, 11am

The following questions are about your beliefs in general.

	Strongly Disagree		*Disagree*		*Agree*		*Strongly Agree*
1. Most of the time, people care enough to try to be helpful, rather than just looking out for themselves	*1*	*2*	*3*	*4*	*5*	*6*	*7*
2. I generally give a technology the benefit of the doubt the first time I use it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
3. It is easy for me to trust a person/thing	*1*	*2*	*3*	*4*	*5*	*6*	*7*
4. Trusting someone or something is not difficult	*1*	*2*	*3*	*4*	*5*	*6*	*7*
5. Most technologies have the features needed to fit their purpose	*1*	*2*	*3*	*4*	*5*	*6*	*7*
6. The large majority of professional people are competent in their area of expertise	*1*	*2*	*3*	*4*	*5*	*6*	*7*
7. My tendency to trust a person/thing is high	*1*	*2*	*3*	*4*	*5*	*6*	*7*
8. A large majority of technologies are excellent	*1*	*2*	*3*	*4*	*5*	*6*	*7*
9. I think vendors generally try back their words with actions	*1*	*2*	*3*	*4*	*5*	*6*	*7*
10. I usually trust a technology until it gives me a reason not to trust it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
11. The typical vendor is sincerely concerned about the problems of their customers	*1*	*2*	*3*	*4*	*5*	*6*	*7*
12. I believe that most technologies are effective at what they are designed to do	*1*	*2*	*3*	*4*	*5*	*6*	*7*
13. I think most technologies enable me to do what I need to do and effectively carry out tasks for me	*1*	*2*	*3*	*4*	*5*	*6*	*7*
14. In general, vendors really do care about the well-being of others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
15. Most vendors are honest in their dealings with others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
16. My typical approach is to trust new technologies until they prove to me I should not trust them	*1*	*2*	*3*	*4*	*5*	*6*	*7*
17. Most professional people are very knowledgeable in their chosen fields	*1*	*2*	*3*	*4*	*5*	*6*	*7*
18. I tend to trust a person/thing, even though I have little knowledge of it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
19. I believe the New Zealand economic environment and the technology industry is a safe, reliable place for consumers to buy goods with reliable consumer protections compared to other places	*1*	*2*	*3*	*4*	*5*	*6*	*7*
20. In general, most vendors keep their promises	*1*	*2*	*3*	*4*	*5*	*6*	*7*
21. I believe that most professional people do a very good job at their work	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Part 2 – Please read the article extracts on the next page carefully, before answering the questions that follow.

Autonomous Cars

There have been rapid advances in vehicle technology, with an increased use of sensors and faster computer processing in vehicles. In the past few years, vehicles that can drive themselves have gone from science fiction to reality. With full self-driving autonomous cars, drivers are not expected to take control at any time. Vehicles are designed to perform all safety-critical functions and monitor road conditions for an entire trip. Users can still expect to maintain some control and be able to override some default settings, such as travel routes.
– Adapted from http://www.transport.govt.nz/ourwork/technology/specific-transport-technologies/road-vehicle/autonomous-vehicles/, last updated 7th March 2016

Automated vehicle technology offers several benefits: without driver error, fewer vehicle crashes will result; the young, the elderly, and the disabled can be more mobile; traffic flow could be more efficient; vehicle occupants could spend travel time engaged in other activities, and; more efficient travel routes will increase fuel efficiency.
– Adapted from http://www.rand.org/pubs/research_reports/RR443-2.html accessed 10th June 2016

The car picked us up. We wanted coffee. It suggested Peet's. But if we'd stopped to look at the map on the screen when this happened, we might have noticed that Peet's wasn't actually the most efficient place to stop, nor was it on your list of preferred coffee shops, which the car's machine-learning algorithm developed over time. Peet's was, instead, a sponsored destination—not unlike a sponsored search result on Google. The car went ever-so-slightly out of the way to take you there. Same goes for your dry cleaner's. The only reason you dropped off your clothes there in the first place was that the car suggested it. As for the lunch special, that really is a favorite restaurant of yours—but the car has never driven you there before. It knows your preferences because the vehicle has combed through your emails, identified key words, and assessed related messages for emotional tone. Similarly, the car knew which sale items to show you from the grocery store because it reviewed your past shopping activity. Plus, there was that one time you told a friend who was sitting in the car with you how much you liked a particular beer you'd tried the night before. The car heard your conversation, picked up on brand keywords, and knew to suggest the same beer for your shopping list when it went on sale.
– Adapted from http://www.theatlantic.com/technology/archive/2016/03/self-driving-cars-and-the-looming-privacy-apocalypse/474600/, accessed 29th June 2016

Automakers already collect and store location and driving data from millions of cars on the road today. In the approaching era of self-driving vehicles, privacy advocates fear the data collection will grow more intrusive. The more sensitive the data, the more lucrative it might be. Once this technology is widely adopted, they'll have all sorts of information on where you're driving, how fast you're going, and there's no control over what they might do with it. A report issued by the Government Accountability Office last year found there were not adequate consumer protections in place for automakers. Will information about how often you drive to a liquor store be provided to your insurance company? Will information about where you spend your Saturday nights be subpoenaed in a divorce proceeding?
– Adapted from http://www.autoblog.com/2015/05/12/self-driving-cars-privacy-bigger-concern-than-safety/, accessed 29th June 2016

AUTONOMOUS CARS

After readings all of the articles provided on the previous page, please answer all of the questions below. Remember, the best thing you can do as a participant is to take your time, read the questionnaire carefully and provide honest, thoughtful answers to all the questions.

1. Did you read all the article extracts provided about autonomous cars on the previous page? (select one)
- ☐ *Yes*
- ☐ *No*

2. Select all the types of information which were included in the article extracts
- ☐ *Potential uses and applications of the technology*
- ☐ *The technology's ability to download information from wireless networks and/or devices*
- ☐ *How to buy the technology*

3. To what extent do you agree with these statements:

	Strongly Disagree		*Disagree*		*Agree*		*Strongly Agree*
i. In the future, a significant number of other people will want to use this technology in their everyday life	*1*	*2*	*3*	*4*	*5*	*6*	*7*
ii. Before reading these articles, I was very well informed about this technology, how it works, its risks and benefits	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Answer the following questions with reference to the information you were provided about autonomous cars

	Strongly Disagree		*Disagree*			*Agree*	*Strongly Agree*
1. I believe that autonomous cars will be competent and effective in driving to destinations efficiently and effectively	1	2	3	4	5	6	7
2. I believe autonomous cars will be designed to look after my privacy and will not be used against me	1	2	3	4	5	6	7
3. I believe all new technologies will have effective privacy controls that make me safe	1	2	3	4	5	6	7
4. I believe autonomous cars will not fail in meeting its general purpose or performing tasks	1	2	3	4	5	6	7
5. Favourable-to-consumer legal statutes and processes make me feel secure in using autonomous cars	1	2	3	4	5	6	7
6. I believe that autonomous cars will be competent and effective in driving safely	1	2	3	4	5	6	7
7. Privacy laws and regulations will protect my personal information which is collected by autonomous cars	1	2	3	4	5	6	7
8. I believe autonomous cars will be designed to learn and understand my needs and preferences	1	2	3	4	5	6	7
9. I always feel confident the right things will happen when I use new technologies that I have not used before	1	2	3	4	5	6	7
10. I believe that autonomous cars will perform its role as a mode of transport very well	1	2	3	4	5	6	7
11. I believe autonomous cars will put my interests first	1	2	3	4	5	6	7
12. I believe autonomous cars will be equipped with the capabilities to protect my personal information	1	2	3	4	5	6	7
13. I believe autonomous cars will serve my best interests	1	2	3	4	5	6	7
14. I believe that things will be fine when I utilise new technologies that I have not used before	1	2	3	4	5	6	7
15. I believe autonomous cars are a very reliable piece of technology	1	2	3	4	5	6	7
16. I am totally confident working with new technologies that I have not used before	1	2	3	4	5	6	7
17. I believe effective product guarantees exist that make it feel all right to use autonomous cars	1	2	3	4	5	6	7
18. Overall, I believe autonomous cars are capable and proficient	1	2	3	4	5	6	7
19. I feel very good about how things will go when I use new technologies that I have not used before	1	2	3	4	5	6	7
20. I believe autonomous cars will not malfunction for me	1	2	3	4	5	6	7
21. I feel okay using autonomous cars because they are backed by vendor protections	1	2	3	4	5	6	7
22. I believe autonomous cars could be relied upon to always protect the personal information it would collect about me	1	2	3	4	5	6	7
23. I believe autonomous cars are extremely dependable	1	2	3	4	5	6	7

The following questions are about the degree to which you consider autonomous cars to be an "emerging technology"

	Strongly Disagree		*Disagree*			*Agree*	*Strongly Agree*
1. I believe this technology is not yet fully utilised in the market place, businesses and everyday individuals in regards to its potential uses	1	2	3	4	5	6	7
2. I believe this technology has a long way to go in regards to development before it can be commercialised	1	2	3	4	5	6	7
3. I believe this technology is yet to reach maturity and still has a lot of potential to grow (e.g. cell phones today can access the internet, play apps and monitor your location compare to 20 years ago)	1	2	3	4	5	6	7
4. I believe this technology will be revolutionary in our everyday lives and will change the way we behave, interact and do things (e.g. cell phones have changed how we communicate and can remote control other devices)	1	2	3	4	5	6	7
5. I believe this technology will trigger changes in other industries (e.g. cell phones have changed the watch, camera, entertainment and telecommunications industries)	1	2	3	4	5	6	7
6. I believe this technology will trigger changes in traditional relationships (e.g. cell phones mean we can order goods and services over the phone or no longer need face to face contact to interact)	1	2	3	4	5	6	7
7. I believe this technology will trigger changes in laws and regulations (e.g. cell phones have caused new manufacturer safety laws and have special consideration in privacy and surveillance laws)	1	2	3	4	5	6	7

The following questions ask you to provide your beliefs about various characteristics of autonomous cars

	Strongly Disagree		*Disagree*			*Agree*	*Strongly Agree*
1. In the future, I believe this technology will be very visible in everyda life and I will be aware of its presence	1	2	3	4	5	6	7
2. I believe that I could identify the other organisations and systems wh could view, use and record information collected by this technology (e.g. third party data collection agencies, app providers)	1	2	3	4	5	6	7
3. I believe the use of this technology has the ability to operate independently without disrupting my daily activities and can be easily forgotten	1	2	3	4	5	6	7
4. I believe the use of this technology will give it great access to information about me, my personal life and daily activities which it could potentially learn	1	2	3	4	5	6	7
5. I believe the use of this technology has the ability to collect a wide range of information about me, how it is used and the environment it is in	1	2	3	4	5	6	7
6. I believe that I will be able to exercise a high degree of control over this technology and its performance	1	2	3	4	5	6	7
7. I believe this technology has the ability to access information from th internet, transfer information to it and communicate with other wireless devices	1	2	3	4	5	6	7

3.2. *BIONANO SENSORS*

EMERGING TECHNOLOGY RESEARCH

Part 1 – Please answer the general questions below.

The following questions are general questions about you and whether you knew about the contents of this research prior to participating in it.

– No information collected in this research will be personally identifiable. All data will be anonymous.

1. For keying purposes only – please write the first four letters of your surname, followed by the 4 letters of your student ID. e.g. SMIT3599

_/

2. General demographic data
   a. What year of study are you at University?
      - 1st year
      - 2nd year
      - 3rd year
      - 4th year or higher

   b. What is your age?

   c. What gender are you?
      - Male
      - Female

3. Did you speak with any of your classmates about this research, the questionnaire or the technology that was described at the beginning of this questionnaire, before participating in this research?
   - Yes
   - No

4. What class were you in when participating in this research?
   - Monday, 1pm
   - Monday, 2pm
   - Monday, 3pm
   - Tuesday, 11am
   - Tuesday, 12pm
   - Tuesday, 1pm
   - Wednesday, 10am
   - Wednesday, 11am

The following questions are about your beliefs in general.

	Strongly Disagree						*Strongly Agree*
1. Most of the time, people care enough to try to be helpful, rather than just looking out for themselves	*1*	*2*	*3*	*4*	*5*	*6*	*7*
2. I generally give a technology the benefit of the doubt the first time I use it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
3. It is easy for me to trust a person/thing	*1*	*2*	*3*	*4*	*5*	*6*	*7*
4. Trusting someone or something is not difficult	*1*	*2*	*3*	*4*	*5*	*6*	*7*
5. Most technologies have the features needed to fit their purpose	*1*	*2*	*3*	*4*	*5*	*6*	*7*
6. The large majority of professional people are competent in their area of expertise	*1*	*2*	*3*	*4*	*5*	*6*	*7*
7. My tendency to trust a person/thing is high	*1*	*2*	*3*	*4*	*5*	*6*	*7*
8. A large majority of technologies are excellent	*1*	*2*	*3*	*4*	*5*	*6*	*7*
9. I think vendors generally try back their words with actions	*1*	*2*	*3*	*4*	*5*	*6*	*7*
10. I usually trust a technology until it gives me a reason not to trust it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
11. The typical vendor is sincerely concerned about the problems of their customers	*1*	*2*	*3*	*4*	*5*	*6*	*7*
12. I believe that most technologies are effective at what they are designed to do	*1*	*2*	*3*	*4*	*5*	*6*	*7*
13. I think most technologies enable me to do what I need to do and effectively carry out tasks for me	*1*	*2*	*3*	*4*	*5*	*6*	*7*
14. In general, vendors really do care about the well-being of others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
15. Most vendors are honest in their dealings with others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
16. My typical approach is to trust new technologies until they prove to me I should not trust them	*1*	*2*	*3*	*4*	*5*	*6*	*7*
17. Most professional people are very knowledgeable in their chosen fields	*1*	*2*	*3*	*4*	*5*	*6*	*7*
18. I tend to trust a person/thing, even though I have little knowledge of it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
19. I believe the New Zealand economic environment and the technology industry is a safe, reliable place for consumers to buy goods with reliable consumer protections compared to other places	*1*	*2*	*3*	*4*	*5*	*6*	*7*
20. In general, most vendors keep their promises	*1*	*2*	*3*	*4*	*5*	*6*	*7*
21. I believe that most professional people do a very good job at their work	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Part 2 – Please read the article extracts on the next page carefully, before answering the questions that follow.

Bionano Sensors

Modern society relies on sensors. Sensors in the road detect cars at traffic lights and adjust traffic flow. Sensors in shops detect your presence and open doors for you. Nanosensors work the same way but detect minute particles of something and communicate this to an information system and can act according to user instructions.
– *Adapted from http://www.azonano.com/article.aspx?ArticleID=1840, accessed 18th June 2016*

Nanosensors could transform conventional medical devices by giving them sensors - nanosensors - that can determine a problem and respond to it if and when it arises. Titanium hip implants with nanosensor materials on its surface have been used to sense what type of cells attach to its surface. The sensors can tell whether cells attaching to the implant are bone cells, bacteria or inflammatory cells. Inbuilt into the sensor is a radio frequency that sends signals to an external computer, from which a clinician can access all of the information transmitted by the sensor. From this a clinician can see whether the implant is free from bacteria or if antibiotic treatment is needed before infections can take hold.
– *Adapted from http://www.medicalnewstoday.com/articles/299663.php, accessed on 20th June 2016*

The long term effects of nanoparticles on human health are poorly understood. Current studies are investigating links between nanoparticles and neurodegenerative, Alzheimer's and Parkinson's disease. Harald Krug is concerned with nanoparticle testing and how it is being reported. Of 6,660 studies of nanoparticle uptake, he found that most have serious errors and researchers aren't carrying out true toxicity tests. The European Commission funded a freely available handbook of standard procedures for nanoparticle testing. But, 'The European Commission do not state that researchers have to use these handbooks. So the same mistakes that were made 10 years ago are being repeated again and again,' say Krug.
– *Adapted from http://www.rsc.org/chemistryworld/2015/04/nanoparticle-toxicology, accessed on 20th June 2016*

Combined with IT systems, it is possible that nanosensors might limit individual privacy by covert surveillance, collecting and distributing personal information, such as health or genetic profiles, without adequate consent. The ETC Group claim they could be used to monitor every aspect of the economy and society. A National Consumer Council briefing highlights concerns such as: the potential to link personal information (for example, through credit cards) to particular places or products could allow individuals to be profiled, tracked and marketed to on an individual basis; increased individual data collection; and the inability of individuals to detect sensing devices. Its anticipated nanosensors will be used in day to day devices. For instance, to measure heart rates, dehydration and glucose levels for diabetics in combination with technology like FitBit or mobile phone tooth implants to enable hands-free talking. Their use is not yet widespread. But, its potential raises questions about the current regulatory frameworks and mechanisms for ensuring privacy protection in society.
– *Adapted from http://www.raeng.org.uk/publications/reports/nanoscience-and-nanotechnologies-opportunities, accessed on 18th June 2016*

BIONANO SENSORS

After readings all of the articles provided on the previous page, please answer all of the questions below. Remember, the best thing you can do as a participant is to take your time, read the questionnaire carefully and provide honest, thoughtful answers to all the questions.

1. Did you read all the article extracts provided about bionano sensors on the previous page? (select one)

- ☐ *Yes*
- ☐ *No*

2. Select all the types of information which were included in the article extracts

- ☐ *Potential uses and applications of the technology*
- ☐ *The technology's ability to download information from wireless networks and/or devices*
- ☐ *How to buy the technology*

3. To what extent do you agree with these statements:

	Strongly Disagree		*Disagree*		*Agree*		*Strongly Agree*
i. In the future, a significant number of other people will want to use this technology in their everyday life	*1*	*2*	*3*	*4*	*5*	*6*	*7*
ii. Before reading these articles, I was very well informed about this technology, how it works, its risks and benefits	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Answer the following questions with reference to the information you were provided about bionano sensors

	Strongly Disagree		*Disagree*			*Agree*	*Strongly Agree*
1. I believe that bionano sensors will be competent and effective in identifying relevant information, objects or matter	1	2	3	4	5	6	7
2. I believe bionano sensors will be designed to look after my privacy and will not be used against me	1	2	3	4	5	6	7
3. I believe all new technologies will have effective privacy controls that make me safe	1	2	3	4	5	6	7
4. I believe bionano sensors will not fail in meeting its general purpose or performing tasks	1	2	3	4	5	6	7
5. Favourable-to-consumer legal statutes and processes make me feel secure in using bionano sensors	1	2	3	4	5	6	7
6. I believe that bionano sensors will be competent and effective in communicating useful information which is relevant for the purposes it was designed	1	2	3	4	5	6	7
7. Privacy laws and regulations will protect my personal information which is collected by bionano sensors	1	2	3	4	5	6	7
8. I believe bionano sensors will be designed to learn and understand my needs and preferences	1	2	3	4	5	6	7
9. I always feel confident the right things will happen when I use new technologies that I have not used before	1	2	3	4	5	6	7
10. I believe that bionano sensors will perform its role as a sensory identification and communication device well	1	2	3	4	5	6	7
11. I believe bionano sensors will put my interests first	1	2	3	4	5	6	7
12. I believe bionano sensors will be equipped with the capabilities to protect my personal information	1	2	3	4	5	6	7
13. I believe bionano sensors will serve my best interests	1	2	3	4	5	6	7
14. I believe that things will be fine when I utilise new technologies that I have not used before	1	2	3	4	5	6	7
15. I believe bionano sensors are a very reliable piece of technology	1	2	3	4	5	6	7
16. I am totally confident working with new technologies that I have not used before	1	2	3	4	5	6	7
17. I believe effective product guarantees exist that make it feel all right to use bionano sensors	1	2	3	4	5	6	7
18. Overall, I believe bionano sensors are capable and proficient	1	2	3	4	5	6	7
19. I feel very good about how things will go when I use new technologies I have not used before	1	2	3	4	5	6	7
20. I believe bionano sensors will not malfunction for me	1	2	3	4	5	6	7
21. I feel okay using bionano sensors because they are backed by vendor protections	1	2	3	4	5	6	7
22. I believe bionano sensors could be relied upon to always protect the personal information it would collect about me	1	2	3	4	5	6	7
23. I believe bionano sensors are extremely dependable	1	2	3	4	5	6	7

The following questions are about the degree to which you consider bionano sensors to be an "emerging technology"

	Strongly Disagree		*Disagree*			*Agree*	*Strongly Agree*
1. I believe this technology is not yet fully utilised in the market place, businesses and everyday individuals in regards to its potential uses	1	2	3	4	5	6	7
2. I believe this technology has a long way to go in regards to development before it can be commercialised	1	2	3	4	5	6	7
3. I believe this technology is yet to reach maturity and still has a lot of potential to grow (e.g. cell phones today can access the internet, play apps and monitor your location compare to 20 years ago)	1	2	3	4	5	6	7
4. I believe this technology will be revolutionary in our everyday lives and will change the way we behave, interact and do things (e.g. cell phones have changed how we communicate and can remote control other devices)	1	2	3	4	5	6	7
5. I believe this technology will trigger changes in other industries (e.g. cell phones have changed the watch, camera, entertainment and telecommunications industries)	1	2	3	4	5	6	7
6. I believe this technology will trigger changes in traditional relationships (e.g. cell phones mean we can order goods and services over the phone or no longer need face to face contact to interact)	1	2	3	4	5	6	7
7. I believe this technology will trigger changes in laws and regulations (e.g. cell phones have caused new manufacturer safety laws and have special consideration in privacy and surveillance laws)	1	2	3	4	5	6	7

The following questions ask you to provide your beliefs about various characteristics of bionano sensors

	Strongly Disagree		*Disagree*			*Agree*	*Strongly Agree*
1. In the future, I believe this technology will be very visible in everyda life and I will be aware of its presence	1	2	3	4	5	6	7
2. I believe that I could identify the other organisations and systems wh could view, use and record information collected by this technology (e.g. third party data collection agencies, app providers)	1	2	3	4	5	6	7
3. I believe the use of this technology has the ability to operate independently without disrupting my daily activities and can be easily forgotten	1	2	3	4	5	6	7
4. I believe the use of this technology will give it great access to information about me, my personal life and daily activities which it could potentially learn	1	2	3	4	5	6	7
5. I believe the use of this technology has the ability to collect a wide range of information about me, how it is used and the environment it is in	1	2	3	4	5	6	7
6. I believe that I will be able to exercise a high degree of control over this technology and its performance	1	2	3	4	5	6	7
7. I believe this technology has the ability to access information from th internet, transfer information to it and communicate with other wireless devices	1	2	3	4	5	6	7

3.3. *DRONES*

EMERGING TECHNOLOGY RESEARCH

Part 1 – Please answer the general questions below.

The following questions are general questions about you and whether you knew about the contents of this research prior to participating in it.

– No information collected in this research will be personally identifiable. All data will be anonymous.

1. For keying purposes only – please write the first four letters of your surname, followed by the 4 letters of your student ID. e.g. SMIT3599

_/

2. General demographic data
   a. What year of study are you at University?
      - 1st year
      - 2nd year
      - 3rd year
      - 4th year or higher

   b. What is your age?

   c. What gender are you?
      - Male
      - Female

3. Did you speak with any of your classmates about this research, the questionnaire or the technology that was described at the beginning of this questionnaire, before participating in this research?
   - Yes
   - No

4. What class were you in when participating in this research?
   - Monday, 1pm
   - Monday, 2pm
   - Monday, 3pm
   - Tuesday, 11am
   - Tuesday, 12pm
   - Tuesday, 1pm
   - Wednesday, 10am
   - Wednesday, 11am

The following questions are about your beliefs in general.

	Strongly Disagree		*Disagree*		*Agree*		*Strongly Agree*
1. Most of the time, people care enough to try to be helpful, rather than just looking out for themselves	*1*	*2*	*3*	*4*	*5*	*6*	*7*
2. I generally give a technology the benefit of the doubt the first time I use it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
3. It is easy for me to trust a person/thing	*1*	*2*	*3*	*4*	*5*	*6*	*7*
4. Trusting someone or something is not difficult	*1*	*2*	*3*	*4*	*5*	*6*	*7*
5. Most technologies have the features needed to fit their purpose	*1*	*2*	*3*	*4*	*5*	*6*	*7*
6. The large majority of professional people are competent in their area of expertise	*1*	*2*	*3*	*4*	*5*	*6*	*7*
7. My tendency to trust a person/thing is high	*1*	*2*	*3*	*4*	*5*	*6*	*7*
8. A large majority of technologies are excellent	*1*	*2*	*3*	*4*	*5*	*6*	*7*
9. I think vendors generally try back their words with actions	*1*	*2*	*3*	*4*	*5*	*6*	*7*
10. I usually trust a technology until it gives me a reason not to trust it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
11. The typical vendor is sincerely concerned about the problems of their customers	*1*	*2*	*3*	*4*	*5*	*6*	*7*
12. I believe that most technologies are effective at what they are designed to do	*1*	*2*	*3*	*4*	*5*	*6*	*7*
13. I think most technologies enable me to do what I need to do and effectively carry out tasks for me	*1*	*2*	*3*	*4*	*5*	*6*	*7*
14. In general, vendors really do care about the well-being of others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
15. Most vendors are honest in their dealings with others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
16. My typical approach is to trust new technologies until they prove to me I should not trust them	*1*	*2*	*3*	*4*	*5*	*6*	*7*
17. Most professional people are very knowledgeable in their chosen fields	*1*	*2*	*3*	*4*	*5*	*6*	*7*
18. I tend to trust a person/thing, even though I have little knowledge of it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
19. I believe the New Zealand economic environment and the technology industry is a safe, reliable place for consumers to buy goods with reliable consumer protections compared to other places	*1*	*2*	*3*	*4*	*5*	*6*	*7*
20. In general, most vendors keep their promises	*1*	*2*	*3*	*4*	*5*	*6*	*7*
21. I believe that most professional people do a very good job at their work	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Part 2 – Please read the article extracts on the next page carefully, before answering the questions that follow.

Drones

Drones are unmanned aircraft system without a human pilot aboard and can operate with various degrees of autonomy: from remote control to full autonomy, using onboard computers, sophisticated programmes or artificial intelligence.
– *Adapted from https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle, accessed on 29th June 2016*

Drone surveillance can gain intelligence against enemy targets by government agencies, against business competitors for high-level competitive intelligence and for national surveillance, including law enforcement, private investigation, spying, disaster recovery, search and rescue, drone journalism, photography, Lidar surveys and military reconnaissance and may have weaponized features. Surveillance drones are currently being trialled and used by state and government agencies and are becoming available to use commercially. They may even become available for domestic use and household security.
– *Adapted from http://whatis.techtarget.com/definition/drone-surveillance, accessed on 29th June 2016*

Drones can operate at altitudes that are high enough to silently enable coverage of an entire city, at a distance invisible to the human eye, and low enough to easily collect and convey detailed images of everything in view. What, exactly, will these drones be able to see? A lot, as it turns out. They will record the route and speed of every vehicle on the streets. They will observe the movements of pedestrians. They will capture the precise moments when the lights in living rooms and bedrooms are turned on and off. You won't even know they are there. Networked to sophisticated surveillance systems, the data they acquire, correlated with information from mobile devices and smart meters, will become an important component of the growing digital record of nearly everything you.
– *Adapted from http://blogs.scientificamerican.com/guest-blog/high-altitude-surveillance-drones-coming-to-a-sky-near-you/, accessed on 29th June 2016*

Surveillance drones raise significant issues for privacy and civil liberties. Drones already in use by law enforcement can carry various types of equipment including live-feed video cameras, infrared cameras, heat sensors, radar and facial recognition. Some can stay in air the hours for hours or days at a time, and their high-tech cameras can scan entire cities, or alternatively, zoom in and read a milk carton from 60,000 feet. They can carry wifi crackers and fake cell phone towers to determine your location or intercept your texts and phone calls. Drone manufacturers even admit they are made to carry "less lethal" weapons such as tasers or rubber bullets. Privacy laws have not kept up with the rapid pace of drone technology, and police may believe they can use drones to spy on citizens with no warrant or legal process whatsoever. As the numbers of entities authorized to fly drones accelerates in the coming years—it's estimated as many as 30,000 drones could be flying in US skies by 2020.
– *Adapted from https://www.eff.org/issues/surveillance-drones, accessed on 29th June 2016*

DRONES

After readings all of the articles provided on the previous page, please answer all of the questions below. Remember, the best thing you can do as a participant is to take your time, read the questionnaire carefully and provide honest, thoughtful answers to all the questions.

1. Did you read all the article extracts provided about drones on the previous page? (select one)
- ☐ *Yes*
- ☐ *No*

2. Select all the types of information which were included in the articls extracts
- ☐ *Potential uses and applications of the technology*
- ☐ *The technology's ability to download information from wireless networks and/or devices*
- ☐ *How to buy the technology*

3. To what extent do you agree with these statements:

	Strongly Disagree		*Disagree*		*Agree*		*Strongly Agree*
i. In the future, a significant number of other people will want to use this technology in their everyday life	*1*	*2*	*3*	*4*	*5*	*6*	*7*
ii. Before reading these articles, I was very well informed about this technology, how it works, its risks and benefits	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Answer the following questions with reference to the information you were provided about drones

	Strongly Disagree			*Disagree*			*Agree*	*Strongly Agree*
1. I believe drones will be competent and effective in identifying relevant humans, animals, objects, matter and activities	1	2	3	4	5	6	7	
2. I believe drones will be designed to look after my privacy and will not be used against me	1	2	3	4	5	6	7	
3. I believe all new technologies will have effective privacy controls that make me safe	1	2	3	4	5	6	7	
4. I believe drones will not fail in meeting its general purpose or performing tasks	1	2	3	4	5	6	7	
5. Favourable-to-consumer legal statutes and processes make me feel secure in the use of drones	1	2	3	4	5	6	7	
6. I believe drones will be competent and effective in communicating useful information which is relevant for the purpose it was designed	1	2	3	4	5	6	7	
7. Privacy laws and regulations will protect my personal information which is collected by drones	1	2	3	4	5	6	7	
8. I believe drones will be designed to learn and understand my needs and preferences	1	2	3	4	5	6	7	
9. I always feel confident the right things will happen when I use new technologies that I have not used before	1	2	3	4	5	6	7	
10. I believe that drones will perform its role as a surveillance tool well	1	2	3	4	5	6	7	
11. I believe drones will put my interests first	1	2	3	4	5	6	7	
12. I believe drones will be equipped with the capabilities to protect my personal information	1	2	3	4	5	6	7	
13. I believe drones will serve my best interests	1	2	3	4	5	6	7	
14. I believe that things will be fine when I utilise new technologies I have not used before	1	2	3	4	5	6	7	
15. I believe drones are a very reliable piece of technology	1	2	3	4	5	6	7	
16. I am totally confident working with new technologies that I have not used before	1	2	3	4	5	6	7	
17. I believe effective product guarantees exist that make it feel all right to use drones	1	2	3	4	5	6	7	
18. Overall, I believe drones are capable and proficient	1	2	3	4	5	6	7	
19. I feel very good about how things will go when I use new technologies that I have not used before	1	2	3	4	5	6	7	
20. I believe drones will not malfunction for me	1	2	3	4	5	6	7	
21. I feel okay using drones because they are backed by vendor protections	1	2	3	4	5	6	7	
22. I believe drones could be relied upon to always protect the personal information it would collect about me	1	2	3	4	5	6	7	
23. I believe drones are extremely dependable	1	2	3	4	5	6	7	

The following questions are about the degree to which you consider drones to be an "emerging technology"

	Strongly Disagree			*Disagree*			*Agree*	*Strongly Agree*
1. I believe this technology is not yet fully utilised in the market place, businesses and everyday individuals in regards to its potential uses	1	2	3	4	5	6	7	
2. I believe this technology has a long way to go in regards to development before it can be commercialised	1	2	3	4	5	6	7	
3. I believe this technology is yet to reach maturity and still has a lot of potential to grow (e.g. cell phones today can access the internet, play apps and monitor your location compare to 20 years ago)	1	2	3	4	5	6	7	
4. I believe this technology will be revolutionary in our everyday lives and will change the way we behave, interact and do things (e.g. cell phones have changed how we communicate and can remote control other devices)	1	2	3	4	5	6	7	
5. I believe this technology will trigger changes in other industries (e.g. cell phones have changed the watch, camera, entertainment and telecommunications industries)	1	2	3	4	5	6	7	
6. I believe this technology will trigger changes in traditional relationships (e.g. cell phones mean we can order goods and services over the phone or no longer need face to face contact to interact)	1	2	3	4	5	6	7	
7. I believe this technology will trigger changes in laws and regulations (e.g. cell phones have caused new manufacturer safety laws and have special consideration in privacy and surveillance laws)	1	2	3	4	5	6	7	

The following questions ask you to provide your beliefs about various characteristics of drones

	Strongly Disagree			*Disagree*			*Agree*	*Strongly Agree*
1. In the future, I believe this technology will be very visible in everyda life and I will be aware of its presence	1	2	3	4	5	6	7	
2. I believe that I could identify the other organisations and systems wh could view, use and record information collected by this technology (e.g. third party data collection agencies, app providers)	1	2	3	4	5	6	7	
3. I believe the use of this technology has the ability to operate independently without disrupting my daily activities and can be easily forgotten	1	2	3	4	5	6	7	
4. I believe the use of this technology will give it great access to information about me, my personal life and daily activities which it could potentially learn	1	2	3	4	5	6	7	
5. I believe the use of this technology has the ability to collect a wide range of information about me, how it is used and the environment it is in	1	2	3	4	5	6	7	
6. I believe that I will be able to exercise a high degree of control over this technology and its performance	1	2	3	4	5	6	7	
7. I believe this technology has the ability to access information from th internet, transfer information to it and communicate with other wireless devices	1	2	3	4	5	6	7	

3.4. 3D PRINTING

EMERGING TECHNOLOGY RESEARCH

Part 1 – Please answer the general questions below.

The following questions are general questions about you and whether you knew about the contents of this research prior to participating in it.

– No information collected in this research will be personally identifiable. All data will be anonymous.

1. For keying purposes only – please write the first four letters of your surname, followed by the 4 letters of your student ID. e.g. SMIT3599

_/

2. General demographic data
   a. What year of study are you at University?
      - 1st year
      - 2nd year
      - 3rd year
      - 4th year or higher

   b. What is your age?

   c. What gender are you?
      - Male
      - Female

3. Did you speak with any of your classmates about this research, the questionnaire or the technology that was described at the beginning of this questionnaire, before participating in this research?
   - Yes
   - No

4. What class were you in when participating in this research?
   - Monday, 1pm
   - Monday, 2pm
   - Monday, 3pm
   - Tuesday, 11am
   - Tuesday, 12pm
   - Tuesday, 1pm
   - Wednesday, 10am
   - Wednesday, 11am

The following questions are about your beliefs in general.

	Strongly Disagree		*Disagree*		*Agree*		*Strongly Agree*
1. Most of the time, people care enough to try to be helpful, rather than just looking out for themselves	*1*	*2*	*3*	*4*	*5*	*6*	*7*
2. I generally give a technology the benefit of the doubt the first time I use it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
3. It is easy for me to trust a person/thing	*1*	*2*	*3*	*4*	*5*	*6*	*7*
4. Trusting someone or something is not difficult	*1*	*2*	*3*	*4*	*5*	*6*	*7*
5. Most technologies have the features needed to fit their purpose	*1*	*2*	*3*	*4*	*5*	*6*	*7*
6. The large majority of professional people are competent in their area of expertise	*1*	*2*	*3*	*4*	*5*	*6*	*7*
7. My tendency to trust a person/thing is high	*1*	*2*	*3*	*4*	*5*	*6*	*7*
8. A large majority of technologies are excellent	*1*	*2*	*3*	*4*	*5*	*6*	*7*
9. I think vendors generally try back their words with actions	*1*	*2*	*3*	*4*	*5*	*6*	*7*
10. I usually trust a technology until it gives me a reason not to trust it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
11. The typical vendor is sincerely concerned about the problems of their customers	*1*	*2*	*3*	*4*	*5*	*6*	*7*
12. I believe that most technologies are effective at what they are designed to do	*1*	*2*	*3*	*4*	*5*	*6*	*7*
13. I think most technologies enable me to do what I need to do and effectively carry out tasks for me	*1*	*2*	*3*	*4*	*5*	*6*	*7*
14. In general, vendors really do care about the well-being of others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
15. Most vendors are honest in their dealings with others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
16. My typical approach is to trust new technologies until they prove to me I should not trust them	*1*	*2*	*3*	*4*	*5*	*6*	*7*
17. Most professional people are very knowledgeable in their chosen fields	*1*	*2*	*3*	*4*	*5*	*6*	*7*
18. I tend to trust a person/thing, even though I have little knowledge of it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
19. I believe the New Zealand economic environment and the technology industry is a safe, reliable place for consumers to buy goods with reliable consumer protections compared to other places	*1*	*2*	*3*	*4*	*5*	*6*	*7*
20. In general, most vendors keep their promises	*1*	*2*	*3*	*4*	*5*	*6*	*7*
21. I believe that most professional people do a very good job at their work	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Part 2 – Please read the article extracts on the next page carefully, before answering the questions that follow.

3D Printing

3D printing offers the possibility to print almost everything we want. From office supplies to, home décor items, to toys and even shoes, 3D printing could just be the revolution many of us waited for so long. As more and more people get access to 3D printing and show interest for the newish technology, it won't be long until every home will have a 3D printer to print almost everything they will need, individually customised, at any time of the day, printed from any wifi device.
– *Adapted from http://www.gambody.com/blog/benefits-3d-printing-home/, accessed on 15th June 2016*

HP's Multi Jet Fusion [3D printer] will be especially well suited for creating high-quality, customizable parts for industries such as aerospace, healthcare and automotive. For example, in the healthcare industry, surgical guides or implants can be shaped to a patient's specific anatomy; a patient's hip ball and joint can be scanned and then recreated to exacting specifications. The automotive industry could use the industrial printer to create custom cars, so buyers could specify changes to the body or interior and an automaker could then create those requirements during the manufacturing process. In aerospace, 3D printers can make parts lighter but adding enough scaffolding to ensure stability without unnecessary added weight.
– *Sourced from http://www.computerworld.com/article/3042983/3d-printing/hps-industrial-3d-printer-on-track-to-ship-this-year.html, accessed on 15th June 2016*

When Australian police stormed a suspected meth lab last December, they were surprised and unnerved to find an American 3D-printed Liberator pistol. Arizona border patrol agents had a similar experience when they caught a man attempting to smuggle a 3D-modded assault rifle across the Mexican border. As 3D-printed firearms, with their blueprints readily available across the internet, continue to turn up in criminal situations, one thing is becoming clear: Gun control laws aren't stopping 3D printers from churning out weaponry.
– *Adapted from https://www.inverse.com/article/11709-the-3d-printed-gun-debate-is-turning-into-a-live-fire-exercise, accessed on 15th June 2016*

3D PRINTING

After readings all of the articles provided on the previous page, please answer all of the questions below. Remember, the best thing you can do as a participant is to take your time, read the questionnaire carefully and provide honest, thoughtful answers to all the questions.

1. Did you read all the article extracts provided about 3D printing on the previous page? (select one)
- ☐ *Yes*
- ☐ *No*

2. Select all the types of information which were included in the article extracts
- ☐ *Potential uses and applications of the technology*
- ☐ *The technology's ability to download information from wireless networks and/or devices*
- ☐ *How to buy the technology*

3. To what extent do you agree with these statements:

	Strongly Disagree		*Disagree*		*Agree*		*Strongly Agree*
i. In the future, a significant number of other people will want to use this technology in their everyday life	*1*	*2*	*3*	*4*	*5*	*6*	*7*
ii. Before reading these articles, I was very well informed about this technology, how it works, its risks and benefits	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Answer the following questions with reference to the information you were provided about 3D printing

	Strongly Disagree			*Disagree*			*Agree*	*Strongly Agree*
1. I believe that 3D printers will be competent and effective in producing objects that I request	1	2	3	4	5	6	7	
2. I believe 3D printers will be designed to look after my privacy and will not be used against me	1	2	3	4	5	6	7	
3. I believe all new technologies will have effective privacy controls that make me safe	1	2	3	4	5	6	7	
4. I believe 3D printers will not fail in meeting its general purpose or performing tasks	1	2	3	4	5	6	7	
5. Favourable-to-consumer legal statutes and processes make me feel secure in using 3D printers	1	2	3	4	5	6	7	
6. I believe that 3D printers will be competent and effective in producing objects correctly and efficiently	1	2	3	4	5	6	7	
7. Privacy laws and regulations will protect my personal information which is collected by 3D printers	1	2	3	4	5	6	7	
8. I believe 3D printers will be designed to learn and understand my needs and preferences	1	2	3	4	5	6	7	
9. I always feel confident the right things will happen when I use new technologies that I have not used before	1	2	3	4	5	6	7	
10. I believe that 3D printers will perform its role as product manufacturer very well	1	2	3	4	5	6	7	
11. I believe 3D printers will put my interests first	1	2	3	4	5	6	7	
12. I believe 3D printers will be equipped with the capabilities to protect my personal information	1	2	3	4	5	6	7	
13. I believe 3D printers will serve my best interests	1	2	3	4	5	6	7	
14. I believe that things will be fine when I utilise new technologies that I have not used before	1	2	3	4	5	6	7	
15. I believe 3D printers are a very reliable piece of technology	1	2	3	4	5	6	7	
16. I am totally confident working with new technologies that I have not used before	1	2	3	4	5	6	7	
17. I believe effective product guarantees exist that make it feel all right to use 3D printers	1	2	3	4	5	6	7	
18. Overall, I believe 3D printers are capable and proficient	1	2	3	4	5	6	7	
19. I feel very good about how things will go when I use new technologies that I have not used before	1	2	3	4	5	6	7	
20. I believe 3D printers will not malfunction for me	1	2	3	4	5	6	7	
21. I feel okay using 3D printers because they are backed by vendor protections	1	2	3	4	5	6	7	
22. I believe 3D printers could be relied upon to always protect the personal information it would collect about me	1	2	3	4	5	6	7	
23. I believe 3D printers are extremely dependable	1	2	3	4	5	6	7	

The following questions are about the degree to which you consider 3D printing to be an "emerging technology"

	Strongly Disagree			*Disagree*			*Agree*	*Strongly Agree*
1. I believe this technology is not yet fully utilised in the market place, businesses and everyday individuals in regards to its potential uses	1	2	3	4	5	6	7	
2. I believe this technology has a long way to go in regards to development before it can be commercialised	1	2	3	4	5	6	7	
3. I believe this technology is yet to reach maturity and still has a lot of potential to grow (e.g. cell phones today can access the internet, play apps and monitor your location compare to 20 years ago)	1	2	3	4	5	6	7	
4. I believe this technology will be revolutionary in our everyday lives and will change the way we behave, interact and do things (e.g. cell phones have changed how we communicate and can remote control other devices)	1	2	3	4	5	6	7	
5. I believe this technology will trigger changes in other industries (e.g. cell phones have changed the watch, camera, entertainment and telecommunications industries)	1	2	3	4	5	6	7	
6. I believe this technology will trigger changes in traditional relationships (e.g. cell phones mean we can order goods and services over the phone or no longer need face to face contact to interact)	1	2	3	4	5	6	7	
7. I believe this technology will trigger changes in laws and regulations (e.g. cell phones have caused new manufacturer safety laws and have special consideration in privacy and surveillance laws)	1	2	3	4	5	6	7	

The following questions ask you to provide your beliefs about various characteristics of 3D printers

	Strongly Disagree			*Disagree*			*Agree*	*Strongly Agree*
1. In the future, I believe this technology will be very visible in everyda life and I will be aware of its presence	1	2	3	4	5	6	7	
2. I believe that I could identify the other organisations and systems wh could view, use and record information collected by this technology (e.g. third party data collection agencies, app providers)	1	2	3	4	5	6	7	
3. I believe the use of this technology has the ability to operate independently without disrupting my daily activities and can be easily forgotten	1	2	3	4	5	6	7	
4. I believe the use of this technology will give it great access to information about me, my personal life and daily activities which it could potentially learn	1	2	3	4	5	6	7	
5. I believe the use of this technology has the ability to collect a wide range of information about me, how it is used and the environment it is in	1	2	3	4	5	6	7	
6. I believe that I will be able to exercise a high degree of control over this technology and its performance	1	2	3	4	5	6	7	
7. I believe this technology has the ability to access information from th internet, transfer information to it and communicate with other wireless devices	1	2	3	4	5	6	7	

3.5. EMAIL

EMERGING TECHNOLOGY RESEARCH

Part 1 – Please answer the general questions below.

The following questions are general questions about you and whether you knew about the contents of this research prior to participating in it.

– No information collected in this research will be personally identifiable. All data will be anonymous.

1. For keying purposes only – please write the first four letters of your surname, followed by the 4 letters of your student ID. e.g. SMIT3599

_/

2. General demographic data
   a. What year of study are you at University?
      - 1st year
      - 2nd year
      - 3rd year
      - 4th year or higher

   b. What is your age?

   c. What gender are you?
      - Male
      - Female

3. Did you speak with any of your classmates about this research, the questionnaire or the technology that was described at the beginning of this questionnaire, before participating in this research?
   - Yes
   - No

4. What class were you in when participating in this research?
   - Monday, 1pm
   - Monday, 2pm
   - Monday, 3pm
   - Tuesday, 11am
   - Tuesday, 12pm
   - Tuesday, 1pm
   - Wednesday, 10am
   - Wednesday, 11am

The following questions are about your beliefs in general.

	Strongly Disagree		*Disagree*		*Agree*		*Strongly Agree*
1. Most of the time, people care enough to try to be helpful, rather than just looking out for themselves	*1*	*2*	*3*	*4*	*5*	*6*	*7*
2. I generally give a technology the benefit of the doubt the first time I use it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
3. It is easy for me to trust a person/thing	*1*	*2*	*3*	*4*	*5*	*6*	*7*
4. Trusting someone or something is not difficult	*1*	*2*	*3*	*4*	*5*	*6*	*7*
5. Most technologies have the features needed to fit their purpose	*1*	*2*	*3*	*4*	*5*	*6*	*7*
6. The large majority of professional people are competent in their area of expertise	*1*	*2*	*3*	*4*	*5*	*6*	*7*
7. My tendency to trust a person/thing is high	*1*	*2*	*3*	*4*	*5*	*6*	*7*
8. A large majority of technologies are excellent	*1*	*2*	*3*	*4*	*5*	*6*	*7*
9. I think vendors generally try back their words with actions	*1*	*2*	*3*	*4*	*5*	*6*	*7*
10. I usually trust a technology until it gives me a reason not to trust it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
11. The typical vendor is sincerely concerned about the problems of their customers	*1*	*2*	*3*	*4*	*5*	*6*	*7*
12. I believe that most technologies are effective at what they are designed to do	*1*	*2*	*3*	*4*	*5*	*6*	*7*
13. I think most technologies enable me to do what I need to do and effectively carry out tasks for me	*1*	*2*	*3*	*4*	*5*	*6*	*7*
14. In general, vendors really do care about the well-being of others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
15. Most vendors are honest in their dealings with others	*1*	*2*	*3*	*4*	*5*	*6*	*7*
16. My typical approach is to trust new technologies until they prove to me I should not trust them	*1*	*2*	*3*	*4*	*5*	*6*	*7*
17. Most professional people are very knowledgeable in their chosen fields	*1*	*2*	*3*	*4*	*5*	*6*	*7*
18. I tend to trust a person/thing, even though I have little knowledge of it	*1*	*2*	*3*	*4*	*5*	*6*	*7*
19. I believe the New Zealand economic environment and the technology industry is a safe, reliable place for consumers to buy goods with reliable consumer protections compared to other places	*1*	*2*	*3*	*4*	*5*	*6*	*7*
20. In general, most vendors keep their promises	*1*	*2*	*3*	*4*	*5*	*6*	*7*
21. I believe that most professional people do a very good job at their work	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Part 2 – Please read the article extracts on the next page carefully, before answering the questions that follow.

Email

Electronic mail is a method of exchanging digital messages between computer users; such messaging first entered substantial use in the 1960s and by the 1970s had taken the form now recognised as email. Email operates across computer networks, now primarily the Internet…Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to a mail server, for as long as it takes to send or receive messages.
– Sourced from https://en.wikipedia.org/wiki/Email, accessed 20th June 2016

Email has many advantages. They can be delivered extremely fast, sent 24 hours a day, 365 days a year, from anywhere with internet access. It is cheap – effectively free when using broadband – and can be sent to multiple people at once. It is not limited to computer devices, by can be sent and received from many other devices including mobile phones, games consoles, TVs and public kiosks. On the other hand, for it to be effective, recipients need access to the internet and must log in and check their email. So there is no guarantee sent emails will be read promptly. Emails can contain viruses and be used to spam and facilitate phishing scams which can trick users into giving away personal information for identity theft using bogus websites and links. However, most email providers scan emails for spam, viruses and potential phishing scams.
– Adapted from http://www.bbc.co.uk/schools/gcsebitesize/ict/datacomm/1emailrev2.shtml, accessed on 26th June

Email usually has to go through potentially untrusted intermediate computers (email servers, ISPs) before reaching its final destination, and there is no way to tell if it was accessed by an unauthorized entity enroute. Email is like a postcard whose contents are visible to everyone who handles it. This is different from a letter sealed in an envelope, where close inspection of the envelope might tell if someone opened it. There are technical workarounds to ensure the privacy of email communication, including the use of encryption and the development of secure messaging architectures by email providers.
– Adapted from https://en.wikipedia.org/wiki/Email_privacy, accessed 26th June 2016

Many email platforms, like Microsoft Exchange Server, have a number of built-in email protection features. These include anti-spam and antivirus as well as integrated filtering and multi-engine scanning capabilities, deigned to provide advanced protection. The email platform might also have compliance controls, to help firms meet legal and regulatory compliance requirements. Microsoft Exchange Server now also have confidential messaging features to encrypt internal and Internet-based messages to help protect the confidentiality of email messages in transit.
– Adapted from http://www.computerweekly.com/feature/Email-security-Essential-Guide, accessed 26th June 2016

EMAIL

After readings all of the articles provided on the previous page, please answer all of the questions below. Remember, the best thing you can do as a participant is to take your time, read the questionnaire carefully and provide honest, thoughtful answers to all the questions.

1. Did you read all the article extracts provided about email on the previous page? (select one)
- ☐ *Yes*
- ☐ *No*

2. Select all the types of information which were included in the article extracts
- ☐ *Potential uses and applications of the technology*
- ☐ *The technology's ability to download information from wireless networks and/or devices*
- ☐ *How to buy the technology*

3. To what extent do you agree with these statements:

	Strongly Disagree		*Disagree*		*Agree*		*Strongly Agree*
i. In the future, a significant number of other people will want to use this technology in their everyday life	*1*	*2*	*3*	*4*	*5*	*6*	*7*
ii. Before reading these articles, I was very well informed about this technology, how it works, its risks and benefits	*1*	*2*	*3*	*4*	*5*	*6*	*7*

Answer the following questions with reference to the information you were provided about email

	Strongly Disagree			*Disagree*			*Agree*	*Strongly Agree*
1. I believe that email will be competent and effective in sending and communicating my information to my intended recipient	1	2	3	4	5	6	7	
2. I believe email is designed to look after my privacy and will not be used against me	1	2	3	4	5	6	7	
3. I believe all new technologies will have effective privacy controls that make me safe	1	2	3	4	5	6	7	
4. I believe email will not fail in meeting its general purpose or performing tasks	1	2	3	4	5	6	7	
5. Favourable-to-consumer legal statutes and processes make me feel secure in using email	1	2	3	4	5	6	7	
6. I believe that email will be competent and effective in receiving and communicating information that someone has sent me	1	2	3	4	5	6	7	
7. Privacy laws and regulations will protect my personal information which is collected by email	1	2	3	4	5	6	7	
8. I believe email is designed to learn and understand my needs and preferences	1	2	3	4	5	6	7	
9. I always feel confident the right things will happen when I use new technologies I have not used before	1	2	3	4	5	6	7	
10. I believe that email will perform its role as a communication system well	1	2	3	4	5	6	7	
11. I believe email puts my interests first	1	2	3	4	5	6	7	
12. I believe email is equipped with the capabilities to protect my personal information	1	2	3	4	5	6	7	
13. I believe email serves my best interests	1	2	3	4	5	6	7	
14. I believe that things will be fine when I utilise new technologies I have not used before	1	2	3	4	5	6	7	
15. I believe email is a very reliable piece of technology	1	2	3	4	5	6	7	
16. I am totally confident working with new technologies I have not used before	1	2	3	4	5	6	7	
17. I believe effective product guarantees exist that make it feel all right to use email	1	2	3	4	5	6	7	
18. Overall, I believe email is capable and proficient	1	2	3	4	5	6	7	
19. I feel very good about how things will go when I use new technologies I have not used before	1	2	3	4	5	6	7	
20. I believe email will not malfunction for me	1	2	3	4	5	6	7	
21. I feel okay using email because they are backed by vendor protections	1	2	3	4	5	6	7	
22. I believe email could be relied upon to always protect the personal information it would collect about me	1	2	3	4	5	6	7	
23. I believe email is extremely dependable	1	2	3	4	5	6	7	

The following questions are about the degree to which you consider email to be an "emerging technology"

	Strongly Disagree			*Disagree*			*Agree*	*Strongly Agree*
1. I believe this technology is not yet fully utilised in the market place, businesses and everyday individuals in regards to its potential uses	1	2	3	4	5	6	7	
2. I believe this technology has a long way to go in regards to development before it can be commercialised	1	2	3	4	5	6	7	
3. I believe this technology is yet to reach maturity and still has a lot of potential to grow (e.g. cell phones today can access the internet, play apps and monitor your location compare to 20 years ago)	1	2	3	4	5	6	7	
4. I believe this technology will be revolutionary in our everyday lives and will change the way we behave, interact and do things (e.g. cell phones have changed how we communicate and can remote control other devices)	1	2	3	4	5	6	7	
5. I believe this technology will trigger changes in other industries (e.g. cell phones have changed the watch, camera, entertainment and telecommunications industries)	1	2	3	4	5	6	7	
6. I believe this technology will trigger changes in traditional relationships (e.g. cell phones mean we can order goods and services over the phone or no longer need face to face contact to interact)	1	2	3	4	5	6	7	
7. I believe this technology will trigger changes in laws and regulations (e.g. cell phones have caused new manufacturer safety laws and have special consideration in privacy and surveillance laws)	1	2	3	4	5	6	7	

The following questions ask you to provide your beliefs about various characteristics of email

	Strongly Disagree			*Disagree*			*Agree*	*Strongly Agree*
1. In the future, I believe this technology will be very visible in everyda life and I will be aware of its presence	1	2	3	4	5	6	7	
2. I believe that I could identify the other organisations and systems wh could view, use and record information collected by this technology (e.g. third party data collection agencies, app providers)	1	2	3	4	5	6	7	
3. I believe the use of this technology has the ability to operate independently without disrupting my daily activities and can be easily forgotten	1	2	3	4	5	6	7	
4. I believe the use of this technology will give it great access to information about me, my personal life and daily activities which it could potentially learn	1	2	3	4	5	6	7	
5. I believe the use of this technology has the ability to collect a wide range of information about me, how it is used and the environment it is in	1	2	3	4	5	6	7	
6. I believe that I will be able to exercise a high degree of control over this technology and its performance	1	2	3	4	5	6	7	
7. I believe this technology has the ability to access information from th internet, transfer information to it and communicate with other wireless devices	1	2	3	4	5	6	7	

Appendix 4. Experiment Results

4.1. EXPLORATORY FACTOR ANALYSIS ON PIP THREATS

Communalities

	Initial	Extraction
Physical ubiquity	1.000	0.66
Network ubiquity	1.000	0.61
Invisibility	1.000	0.95
Invasiveness	1.000	0.76
Collectability of information	1.000	0.78
Programmability	1.000	0.66
Wireless accessibility	1.000	0.44

Total Variance Explained

Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
Physical ubiquity	2.08	29.71	29.71	2.08	29.71	29.71	2.02	28.80	28.80
Network ubiquity	1.78	25.70	55.41	1.80	25.70	55.41	1.81	25.89	54.69
Invisibility	0.97	13.91	69.32	0.97	13.91	69.32	1.02	14.63	69.32
Invasiveness	0.73	10.41	79.73						
Collectability of information	0.58	8.32	88.04						
Programmability	0.54	7.69	95.73						
Wireless accessibility	0.30	4.23	100.00						

Component Matrix

	Component		
	Omnipotence	Intrusiveness	Invisibility
Physical ubiquity	0.48	0.56	-0.34
Network ubiquity	0.33	0.71	0.00
Invisibility	0.33	0.13	0.91
Invasiveness	0.75	-0.45	0.01
Collectability of information	0.82	-0.33	-0.05
Programmability	0.08	0.80	0.07
Wireless accessibility	0.64	-0.00	-0.17

Rotated Component Matrix

	Component		
	Omnipotence	Intrusiveness	Invisibility
Physical ubiquity	0.28	0.74	-0.19
Network ubiquity	0.04	0.77	0.13
Invisibility	0.12	0.10	0.96
Invasiveness	0.85	-0.17	0.12
Collectability of information	0.88	-0.02	0.08
Programmability	-0.23	0.76	0.16
Wireless accessibility	0.62	0.25	-0.04

Component Transformation Matrix

Component	Omnipotence	Intrusiveness	Invisibility
Omnipotence	0.92	0.34	0.20
Intrusiveness	-0.37	0.93	0.09
Invisibility	-0.15	-0.15	0.98

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

4.2. MANOVA: EFFECT OF PIP THREATS ON TRUST

Descriptive Statistics

PIP Threat	Group	Mean	Std. Deviation	N
Intrusiveness	3D printing	4.58	0.96	57
	Autonomous cars	5.34	0.90	60
	Bionano sensors	5.16	0.94	57
	Drones	5.36	0.88	54
	Email	4.73	0.86	62
	Total	5.03	0.96	290
Omnipotence	3D printing	4.72	0.75	57
	Autonomous cars	4.49	0.95	60
	Bionano sensors	4.03	1.16	57
	Drones	4.11	1.28	54
	Email	4.60	0.76	62
	Total	4.40	1.03	290
Invisibility	3D printing	4.44	1.24	57

Descriptive Statistics

PIP Threat	Group	Mean	Std. Deviation	N
	Autonomous cars	4.27	1.41	60
	Bionano sensors	4.89	1.06	57
	Drones	4.98	1.24	54
	Email	4.53	1.41	62
	Total	4.61	1.30	290

Box's Test of Equality of Covariance Matrices

Box's M	67.62
F	2.75
df1	24.00
df2	220513.19
Sig.	0.00

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.98	4740.57	3.00	283.00	0.00	0.98
	Wilks' Lambda	0.02	4740.57	3.00	283.00	0.00	0.98
	Hotelling's Trace	50.25	4740.57	3.00	283.00	0.00	0.98
	Roy's Largest Root	50.25	4740.57	3.00	283.00	0.00	0.98
Groups	Pillai's Trace	0.24	6.22	12.00	855.00	0.00	0.08
	Wilks' Lambda	0.77	6.48	12.00	749.04	0.00	0.08
	Hotelling's Trace	0.28	6.67	12.00	845.00	0.00	0.09
	Roy's Largest Root	0.22	15.58[c]	4.00	285.00	0.00	0.18

Levene's Test of Equality of Error Variances

	F	df1	df2	Sig.
Intrusiveness	.33	4.00	285.00	0.86
Omnipotence	5.57	4.00	285.00	0.00
Invisibility	2.03	4.00	285.00	0.09

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Intrusiveness	30.23[a]	4.00	7.56	9.18	0.00	0.11
	Omnipotence	21.023[b]	4.00	5.26	5.30	0.00	0.07
	Invisibility	21.19[c]	4.00	5.30	3.22	0.01	0.04
Intercept	Intrusiveness	7333.10	1.00	7333.10	8902.67	0.00	0.97
	Omnipotence	5573.91	1.00	5573.91	5616.95	0.00	0.95
	Invisibility	6183.25	1.00	6183.25	3752.98	0.00	0.93
Groups	Intrusiveness	30.23	4.00	7.56	9.18	0.00	0.11
	Omnipotence	21.03	4.00	5.26	5.30	0.00	0.07
	Invisibility	21.19	4.00	5.30	3.22	0.01	0.04
Error	Intrusiveness	234.75	285	0.82			
	Omnipotence	282.82	285	0.99			
	Invisibility	469.55	285	1.65			
Total	Intrusiveness	7598.56	290				
	Omnipotence	5909.44	290				
	Invisibility	6664.00	290				
Corrected Total	Intrusiveness	264.98	289				
	Omnipotence	303.84	289				
	Invisibility	490.75	289				

a. R Squared = .114 (Adjusted R Squared = .102)
b. R Squared = .069 (Adjusted R Squared = .056)
c. R Squared = .043 (Adjusted R Squared = .030)

Estimated Marginal Means – Technology Groups
Estimates

Dependent Variable	Groups	Mean	Std. Error	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Intrusiveness	3D printing	4.58	0.12	4.34	4.82
	Autonomous cars	5.34	0.12	5.11	5.58
	Bionano sensors	5.16	0.12	4.92	5.40
	Drones	5.36	0.12	5.12	5.61
	Email	4.73	0.12	4.50	4.95
Omnipotence	3D printing	4.72	0.13	4.46	4.98
	Autonomous cars	4.49	0.13	4.24	4.74
	Bionano sensors	4.03	0.13	3.77	4.29
	Drones	4.11	0.14	3.84	4.38
	Email	4.60	0.13	4.35	4.85
Invisibility	3D printing	4.44	0.17	4.10	4.77
	Autonomous cars	4.27	0.17	3.94	4.59
	Bionano sensors	4.90	0.17	4.56	5.23
	Drones	4.98	0.18	4.64	5.33
	Email	4.53	0.16	4.21	4.85

Pairwise Comparisons

Dependent Variable	Groups	Comparison Group	Mean Difference	Std. Error	Sig.	95% Confidence Interval for Difference[b] Lower Bound	Upper Bound
Intrusiveness	3D printing	Autonomous cars	**-0.765**	0.168	0.000	-1.240	-0.291
		Bionano sensors	**-0.579**	0.170	0.008	-1.060	-0.098
		Drones	**-0.785**	0.172	0.000	-1.273	-0.298
		Email	-0.147	0.167	1.000	-0.618	0.324
	Autonomous cars	3D printing	**0.765**	0.168	0.000	0.291	1.240
		Bionano sensors	0.187	0.168	1.000	-0.288	0.661
		Drones	-0.020	0.170	1.000	-0.501	0.462
		Email	**0.619**	0.164	0.002	0.154	1.084
	Bionano sensors	3D printing	**0.579**	0.170	0.008	0.098	1.060
		Autonomous cars	-0.187	0.168	1.000	-0.661	0.288
		Drones	-0.206	0.172	1.000	-0.694	0.281
		Email	0.432	0.167	0.100	-0.039	0.903
	Drones	3D printing	**0.785**	0.172	0.000	0.298	1.273
		Autonomous cars	0.020	0.170	1.000	-0.462	0.501
		Bionano sensors	0.206	0.172	1.000	-0.281	0.694
		Email	**0.638**	0.169	0.002	0.160	1.116
	Email	3D printing	0.147	0.167	1.000	-0.324	0.618
		Autonomous cars	**-0.619**	0.164	0.002	-1.084	-0.154
		Bionano sensors	-0.432	0.167	0.100	-0.903	0.039
		Drones	**-0.638**	0.169	0.002	-1.116	-0.160
Omnipotence	3D printing	Autonomous cars	0.230	0.184	1.000	-0.291	0.752
		Bionano sensors	**0.690**	0.187	0.003	0.162	1.218
		Drones	**0.608**	0.189	0.015	0.073	1.143
		Email	0.123	0.183	1.000	-0.395	0.640
	Autonomous cars	3D printing	-0.230	0.184	1.000	-0.752	0.291
		Bionano sensors	0.460	0.184	0.132	-0.062	0.981
		Drones	0.378	0.187	0.441	-0.151	0.906
		Email	-0.108	0.180	1.000	-0.618	0.402
	Bionano sensors	3D printing	**-0.690**	0.187	0.003	-1.218	-0.162
		Autonomous cars	-0.460	0.184	0.132	-0.981	0.062
		Drones	-0.082	0.189	1.000	-0.617	0.453
		Email	**-0.568**	0.183	0.021	-1.085	-0.050
	Drones	3D printing	**-0.608**	0.189	0.015	-1.143	-0.073
		Autonomous cars	-0.378	0.187	0.441	-0.906	0.151
		Bionano sensors	0.082	0.189	1.000	-0.453	0.617
		Email	-0.486	0.185	0.093	-1.010	0.039
	Email	3D printing	-0.123	0.183	1.000	-0.640	0.395
		Autonomous cars	0.108	0.180	1.000	-0.402	0.618
		Bionano sensors	**0.568**	0.183	0.021	0.050	1.085
		Drones	0.486	0.185	0.093	-0.039	1.010
Invisibility	3D printing	Autonomous cars	0.172	0.237	1.000	-0.500	0.844
		Bionano sensors	-0.456	0.240	0.588	-1.136	0.224
		Drones	-0.543	0.244	0.267	-1.232	0.147
		Email	-0.094	0.236	1.000	-0.760	0.573
	Autonomous cars	3D printing	-0.172	0.237	1.000	-0.844	0.500
		Bionano sensors	-0.628	0.237	0.086	-1.300	0.044
		Drones	**-0.715**	0.241	0.032	-1.396	-0.034
		Email	-0.266	0.232	1.000	-0.923	0.392
	Bionano sensors	3D printing	0.456	0.240	0.588	-0.224	1.136
		Autonomous cars	0.628	0.237	0.086	-0.044	1.300
		Drones	-0.087	0.244	1.000	-0.776	0.603
		Email	0.362	0.236	1.000	-0.304	1.029
	Drones	3D printing	0.543	0.244	0.267	-0.147	1.232
		Autonomous cars	**0.715**	0.241	0.032	0.034	1.396
		Bionano sensors	0.087	0.244	1.000	-0.603	0.776
		Email	0.449	0.239	0.611	-0.227	1.125
	Email	3D printing	0.094	0.236	1.000	-0.573	0.760
		Autonomous cars	0.266	0.232	1.000	-0.392	0.923
		Bionano sensors	-0.362	0.236	1.000	-1.029	0.304
		Drones	-0.449	0.239	0.611	-1.125	0.227

The mean difference is significant at the .05 level.
Adjustment for multiple comparisons: Bonferroni.

Multiple Comparisons

Dependent Variable	Groups	Comparison Group	Mean Difference	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Intrusiveness	3D printing	Autonomous cars	**-0.766**	0.168	0.000	-1.226	-0.766
		Bionano sensors	**-0.579**	0.170	0.007	-1.046	-0.579
		Drones	**-0.785**	0.172	0.000	-1.258	-0.785
		Email	-0.147	0.167	0.903	-0.604	-0.147
	Autonomous cars	3D printing	**0.766**	0.168	0.000	0.305	0.766
		Bionano sensors	0.187	0.168	0.801	-0.274	0.187
		Drones	-0.020	0.170	1.000	-0.487	-0.020
		Email	**0.619**	0.164	0.002	0.167	0.619
	Bionano sensors	3D printing	**0.579**	0.170	0.007	0.112	0.579
		Autonomous cars	-0.187	0.168	0.801	-0.647	-0.187
		Drones	-0.206	0.172	0.753	-0.680	-0.206
		Email	0.432	0.167	0.074	-0.025	0.432
	Drones	3D printing	**0.785**	0.172	0.000	0.312	0.785
		Autonomous cars	0.020	0.170	1.000	-0.448	0.020
		Bionano sensors	0.206	0.172	0.753	-0.267	0.206
		Email	**0.638**	0.169	0.002	0.175	0.638
	Email	3D printing	0.147	0.167	0.903	-0.310	0.147
		Autonomous cars	**-0.619**	0.164	0.002	-1.070	-0.618
		Bionano sensors	-0.432	0.167	0.074	-0.889	-0.432
		Drones	**-0.638**	0.169	0.002	-1.102	-0.638
Omnipotence	3D printing	Autonomous cars	0.230	0.184	0.722	-0.275	0.230
		Bionano sensors	**0.690**	0.187	0.002	0.178	0.690
		Drones	**0.608**	0.189	0.013	0.089	0.608
		Email	0.123	0.183	0.963	-0.379	0.123
	Autonomous cars	3D printing	-0.230	0.184	0.722	-0.736	-0.230
		Bionano sensors	0.460	0.184	0.095	-0.046	0.460
		Drones	0.378	0.187	0.258	-0.135	0.378
		Email	-0.108	0.180	0.975	-0.603	-0.108
	Bionano sensors	3D printing	**-0.690**	0.187	0.002	-1.202	-0.690
		Autonomous cars	-0.460	0.184	0.095	-0.965	-0.460
		Drones	-0.082	0.189	0.993	-0.601	-0.082
		Email	**-0.568**	0.183	0.018	-1.069	-0.568
	Drones	3D printing	**-0.608**	0.189	0.013	-1.128	-0.608
		Autonomous cars	-0.378	0.187	0.258	-0.891	-0.378
		Bionano sensors	0.082	0.189	0.993	-0.437	0.082
		Email	-0.486	0.185	0.070	-0.995	-0.486
	Email	3D printing	-0.123	0.183	0.963	-0.624	-0.123
		Autonomous cars	0.108	0.180	0.975	-0.387	0.108
		Bionano sensors	**0.568**	0.183	0.018	0.066	0.568
		Drones	0.486	0.185	0.070	-0.023	0.486
Invisibility	3D printing	Autonomous cars	0.172	0.237	0.951	-0.480	0.172
		Bionano sensors	-0.456	0.240	0.321	-1.116	-0.456
		Drones	-0.543	0.244	0.173	-1.212	-0.543
		Email	-0.094	0.236	0.995	-0.740	-0.094
	Autonomous cars	3D printing	-0.172	0.237	0.951	-0.824	-0.172
		Bionano sensors	-0.628	0.237	0.065	-1.280	-0.628
		Drones	**-0.715**	0.241	0.027	-1.376	-0.715
		Email	-0.266	0.232	0.784	-0.904	-0.266
	Bionano sensors	3D printing	0.456	0.240	0.321	-0.204	0.456
		Autonomous cars	0.628	0.237	0.065	-0.024	0.628
		Drones	-0.087	0.244	0.997	-0.756	-0.087
		Email	0.363	0.236	0.538	-0.284	0.363
	Drones	3D printing	0.543	0.244	0.173	-0.126	0.543
		Autonomous cars	**0.715**	0.241	0.027	0.054	0.715
		Bionano sensors	0.087	0.244	0.997	-0.582	0.087
		Email	0.449	0.239	0.330	-0.207	0.449
	Email	3D printing	0.094	0.236	0.995	-0.553	0.094
		Autonomous cars	0.266	0.232	0.784	-0.373	0.266
		Bionano sensors	-0.363	0.236	0.538	-1.009	-0.363
		Drones	-0.449	0.239	0.330	-1.105	-0.449

The error term is Mean Square(Error) = 1.648.
The mean difference is significant at the .05 level.

Multivariate Tests

	Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Pillai's trace	0.24	6.22	12.00	855.00	0.00	0.08
Wilks' lambda	0.77	6.48	12.00	749.04	0.00	0.08
Hotelling's trace	0.28	6.67	12.00	845.00	0.00	0.09
Roy's largest root	0.22	15.58	4.00	285.00	0.00	0.18

Univariate Tests

Dependent Variable		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Intrusiveness	Contrast	30.23	4.00	7.56	9.18	0.00	.12
	Error	234.75	285.00	0.82			
Omnipotence	Contrast	21.03	4.00	5.26	5.30	0.00	.07
	Error	282.82	285.00	0.99			
Invisibility	Contrast	21.19	4.00	5.30	3.22	0.01	.04
	Error	469.55	285.00	1.65			

Post Hoc Test - Homogeneous Subsets (Using Tukey HSD)

Intrusiveness

		Subset		
Groups	N	1	2	3
3D printing	57	4.58		
Email	62	4.73	4.73	
Bionano sensors	57		5.16	5.16
Autonomous cars	60			5.34
Drones	54			5.36
Sig.		0.91	0.08	0.74

The error term is Mean Square(Error) = .824.
a. Uses Harmonic Mean Sample Size = 57.869.
b. The group sizes are unequal. The harmonic mean of the group size is used. Type 1 error levels are not guaranteed.
c. Alpha = .05.

Omnipotence

		Subset		
Group	N	1	2	3
Bionano sensors	57	4.03		
Drones	54	4.11	4.11	
Autonomous cars	60	4.49	4.49	4.49
Email	62		4.60	4.6
3D printing	57			4.72
Sig.		0.10	0.07	0.73

The error term is Mean Square(Error) = .992.
a. Uses Harmonic Mean Sample Size = 57.869.
b. The group sizes are unequal. The harmonic mean of the group size is used. Type 1 error levels are not guaranteed.
c. Alpha = .05.

Invisibility

		Subset	
Group	N	1	2
Autonomous cars	60	4.27	
3D printing	57	4.44	4.44
Email	62	4.53	4.53
Bionano sensors	57	4.89	4.89
Drones	54		4.98
Sig.		0.07	0.16

The error term is Mean Square(Error) = 1.648.
a. Uses Harmonic Mean Sample Size = 57.869.
b. The group sizes are unequal. The harmonic mean of the group size is used. Type 1 error levels are not guaranteed.
c. Alpha = .05.

4.3. MANCOVA: EFFECT OF COVARIATES ON INITIAL TECHNOLOGY TRUST

4.3.1. Faith in General Technology

Box's Test of Equality of Covariance Matrices

Box's M	93.49
F	1.50
df1	60
df2	160715.42
Sig.	0.01

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.31	24.71	5.00	279.00	0.31	0.31
	Wilks' Lambda	0.69	24.71	5.00	279.00	0.31	0.31
	Hotelling's Trffe	0.44	24.71	5.00	279.00	0.31	0.31
	Roy's Largest Root	0.44	24.71	5.00	279.00	0.31	0.31
Faith in General Technology	Pillai's Trace	0.15	9.92	5.00	279.00	0.15	0.15
	Wilks' Lambda	0.85	9.92	5.00	279.00	0.15	0.15
	Hotelling's Trace	0.18	9.92	5.00	279.00	0.15	0.15
	Roy's Largest Root	0.18	9.92	5.00	279.00	0.15	0.15
Group	Pillai's Trace	0.31	4.75	20.00	1128.00	0.08	0.08
	Wilks' Lambda	0.71	5.02	20.00	926.29	0.08	0.08
	Hotelling's Trace	0.38	5.24	20.00	1110.00	0.09	0.09
	Roy's Largest Root	0.28	15.80	5.00	282.00	0.22	0.22

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Functionality	32.28[a]	5.00	6.46	10.89	0.00	0.16
	Reliability	31.49[b]	5.00	6.30	9.61	0.00	0.15
	Effectiveness	21.39[c]	5.00	4.28	4.90	0.00	0.08
	Structural Assurance	32.35[d]	5.00	6.47	9.14	0.00	0.14
	Situational Normality	32.30[e]	5.00	6.46	9.38	0.00	0.14
Intercept	Functionality	73.54	1.00	73.54	124.09	0.00	0.31
	Reliability	34.76	1.00	34.76	53.03	0.00	0.16
	Effectiveness	36.17	1.00	36.17	41.41	0.00	0.13
	Structural Assurance	22.78	1.00	22.78	32.17	0.00	0.10
	Situational Normality	13.90	1.00	13.90	20.18	0.00	0.07
Faith in General Technology	Functionality	4.40	1.00	4.40	7.42	0.01	0.03
	Reliability	10.62	1.00	10.62	16.20	0.00	0.05
	Effectiveness	8.32	1.00	8.32	9.53	0.00	0.03
	Structural Assurance	18.13	1.00	18.13	25.62	0.00	0.08
	Situational Normality	29.16	1.00	29.16	42.35	0.00	0.13
Group	Functionality	26.15	4.00	6.54	11.03	0.00	0.14
	Reliability	17.97	4.00	4.49	6.85	0.00	0.09
	Effectiveness	11.71	4.00	2.93	3.35	0.01	0.05
	Structural Assurance	12.03	4.00	3.01	4.25	0.00	0.06
	Situational Normality	1.79	4.00	0.45	0.65	0.63	0.01
Error	Functionality	167.72	283.00	0.59			
	Reliability	185.49	283.00	0.66			
	Effectiveness	247.18	283.00	0.87			
	Structural Assurance	200.34	283.00	0.71			
	Situational Normality	194.90	283.00	0.69			
Total	Functionality	7064.61	289.00				
	Reliability	5254.36	289.00				
	Effectiveness	5025.51	289.00				
	Structural Assurance	5122.91	289.00				
	Situational Normality	5211.97	289.00				
Corrected Total	Functionality	200.00	288.00				
	Reliability	216.98	288.00				
	Effectiveness	268.57	288.00				
	Structural Assurance	232.69	288.00				
	Situational Normality	227.20	288.00				

a. R Squared = 0.161 (Adjusted R Squared = 0.147)
b. R Squared = 0.145 (Adjusted R Squared = 0.130)
c. R Squared = 0.080 (Adjusted R Squared = 0.063)
d. R Squared = 0.139 (Adjusted R Squared = 0.124)
e. R Squared = 0.142 (Adjusted R Squared = 0.127)

4.3.2. Technology Trust Stance

Box's Test of Equality of Covariance Matrices

Box's M	93.49
F	1.50
df1	60
df2	160715.42
Sig.	0.01

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.45	45.21	5.00	279.00	0.45	0.45
	Wilks' Lambda	0.55	45.21	5.00	279.00	0.45	0.45
	Hotelling's Trace	0.81	45.21	5.00	279.00	0.45	0.45
	Roy's Largest Root	0.81	45.21	5.00	279.00	0.45	0.45
Technology Trust Stance	Pillai's Trace	0.17	11.00	5.00	279.00	0.17	0.17
	Wilks' Lambda	0.84	11.00	5.00	279.00	0.17	0.17
	Hotelling's Trace	0.20	11.00	5.00	279.00	0.17	0.17
	Roy's Largest Root	0.20	11.00	5.00	279.00	0.17	0.17
Group	Pillai's Trace	0.31	4.80	20.00	1128.00	0.08	0.08
	Wilks' Lambda	0.71	5.08	20.00	926.29	0.08	0.08
	Hotelling's Trace	0.38	5.31	20.00	1110.00	0.09	0.09
	Roy's Largest Root	0.28	16.01	5.00	282.00	0.22	0.22

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Functionality	32.83[a]	5.00	6.57	11.12	0.00	0.16
	Reliability	30.10[b]	5.00	6.02	9.12	0.00	0.14
	Effectiveness	25.81[c]	5.00	5.16	6.02	0.00	0.10
	Structural Assurance	23.72[d]	5.00	4.74	6.43	0.00	0.10
	Situational Normality	39.68[e]	5.00	7.94	11.98	0.00	0.18
Intercept	Functionality	131.29	1.00	131.29	222.25	0.00	0.44
	Reliability	75.66	1.00	75.66	114.57	0.00	0.29
	Effectiveness	61.62	1.00	61.62	71.83	0.00	0.20
	Structural Assurance	71.97	1.00	71.97	97.47	0.00	0.26
	Situational Normality	32.21	1.00	32.21	48.61	0.00	0.15
Technology Trust Stance	Functionality	4.95	1.00	4.95	8.38	0.00	0.03
	Reliability	9.23	1.00	9.23	13.97	0.00	0.05
	Effectiveness	12.74	1.00	12.74	14.86	0.00	0.05
	Structural Assurance	9.51	1.00	9.51	12.88	0.00	0.04
	Situational Normality	36.55	1.00	36.55	55.15	0.00	0.16
Group	Functionality	27.72	4.00	6.93	11.73	0.00	0.14
	Reliability	20.09	4.00	5.02	7.61	0.00	0.10
	Effectiveness	11.72	4.00	2.93	3.42	0.01	0.05
	Structural Assurance	13.90	4.00	3.47	4.71	0.00	0.06
	Situational Normality	2.83	4.00	0.71	1.07	0.37	0.02
Error	Functionality	167.17	283.00	0.59			
	Reliability	186.88	283.00	0.66			
	Effectiveness	242.76	283.00	0.86			
	Structural Assurance	208.96	283.00	0.74			
	Situational Normality	187.52	283.00	0.66			
Total	Functionality	7064.61	289.00				
	Reliability	5254.36	289.00				
	Effectiveness	5025.51	289.00				
	Structural Assurance	5122.91	289.00				
	Situational Normality	5211.97	289.00				
Corrected Total	Functionality	200.00	288.00				
	Reliability	216.98	288.00				
	Effectiveness	268.57	288.00				
	Structural Assurance	232.69	288.00				
	Situational Normality	227.20	288.00				

a. R Squared = 0.164 (Adjusted R Squared = 0.149)
b. R Squared = 0.139 (Adjusted R Squared = 0.124)
c. R Squared = 0.096 (Adjusted R Squared = 0.080)
d. R Squared = 0.102 (Adjusted R Squared = 0.086)
e. R Squared = 0.175 (Adjusted R Squared = 0.160)

4.3.3. Disposition to Trust

Box's Test of Equality of Covariance Matrices

Box's M	93.49
F	1.50
df1	60
df2	160715.42
Sig.	0.01

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.68	117.40	5.00	279.00	0.00	0.68
	Wilks' Lambda	0.32	117.40	5.00	279.00	0.00	0.68
	Hotelling's Trace	2.10	117.40	5.00	279.00	0.00	0.68
	Roy's Largest Root	2.10	117.40	5.00	279.00	0.00	0.68
Disposition to Trust	Pillai's Trace	0.14	8.69	5.00	279.00	0.00	0.14
	Wilks' Lambda	0.87	8.69	5.00	279.00	0.00	0.14
	Hotelling's Trace	0.16	8.69	5.00	279.00	0.00	0.14
	Roy's Largest Root	0.16	8.69	5.00	279.00	0.00	0.14
Group	Pillai's Trace	0.32	4.83	20.00	1128.00	0.00	0.08
	Wilks' Lambda	0.71	5.12	20.00	926.29	0.00	0.08
	Hotelling's Trace	0.39	5.34	20.00	1110.00	0.00	0.09
	Roy's Largest Root	0.28	16.00	5.00	282.00	0.00	0.22

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Functionality	31.36[a]	5.00	6.27	10.53	0.00	0.16
	Reliability	35.92[b]	5.00	7.18	11.23	0.00	0.17
	Effectiveness	23.58[c]	5.00	4.72	5.45	0.00	0.09
	Structural Assurance	24.81[d]	5.00	4.96	6.75	0.00	0.11
	Situational Normality	29.62[e]	5.00	5.92	8.48	0.00	0.13
Intercept	Functionality	333.23	1.00	333.23	559.22	0.00	0.66
	Reliability	180.22	1.00	180.22	281.68	0.00	0.50
	Effectiveness	184.08	1.00	184.08	212.63	0.00	0.43
	Structural Assurance	189.93	1.00	189.93	258.56	0.00	0.48
	Situational Normality	146.70	1.00	146.70	210.11	0.00	0.43
Disposition to Trust	Functionality	3.49	1.00	3.49	5.85	0.02	0.02
	Reliability	15.04	1.00	15.04	23.51	0.00	0.08
	Effectiveness	10.51	1.00	10.51	12.14	0.00	0.04
	Structural Assurance	10.59	1.00	10.59	14.42	0.00	0.05
	Situational Normality	26.48	1.00	26.48	37.93	0.00	0.12
Group	Functionality	27.98	4.00	7.00	11.74	0.00	0.14
	Reliability	20.73	4.00	5.18	8.10	0.00	0.10
	Effectiveness	12.70	4.00	3.18	3.67	0.01	0.05
	Structural Assurance	14.78	4.00	3.70	5.03	0.00	0.07
	Situational Normality	3.18	4.00	0.79	1.14	0.34	0.02
Error	Functionality	168.64	283.00	0.60			
	Reliability	181.07	283.00	0.64			
	Effectiveness	245.00	283.00	0.87			
	Structural Assurance	207.88	283.00	0.74			
	Situational Normality	197.58	283.00	0.70			
Total	Functionality	7064.61	289.00				
	Reliability	5254.36	289.00				
	Effectiveness	5025.51	289.00				
	Structural Assurance	5122.91	289.00				
	Situational Normality	5211.97	289.00				
Corrected Total	Functionality	200.00	288.00				
	Reliability	216.98	288.00				
	Effectiveness	268.57	288.00				
	Structural Assurance	232.69	288.00				
	Situational Normality	227.20	288.00				

a. R Squared = 0.157 (Adjusted R Squared = 0.142)
b. R Squared = 0.166 (Adjusted R Squared = 0.151)
c. R Squared = 0.088 (Adjusted R Squared = 0.072)
d. R Squared = 0.107 (Adjusted R Squared = 0.091)
e. R Squared = 0.130 (Adjusted R Squared = 0.115)

4.3.4. Faith in Humanity (Benevolence)

Box's Test of Equality of Covariance Matrices

Box's M	93.49
F	1.50
df1	60
df2	160715.42
Sig.	0.01

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.53	63.823	5.00	279.00	0.00	0.53
	Wilks' Lambda	0.47	63.823	5.00	279.00	0.00	0.53
	Hotelling's Trace	1.14	63.823	5.00	279.00	0.00	0.53
	Roy's Largest Root	1.14	63.823	5.00	279.00	0.00	0.53
Faith in Humanity (Benevolence)	Pillai's Trace	0.15	9.47	5.00	279.00	0.00	0.15
	Wilks' Lambda	0.86	9.47	5.00	279.00	0.00	0.15
	Hotelling's Trace	0.17	9.47	5.00	279.00	0.00	0.15
	Roy's Largest Root	0.17	9.47	5.00	279.00	0.00	0.15
Group	Pillai's Trace	0.31	4.77	20.00	1128.00	0.00	0.08
	Wilks' Lambda	0.71	5.05	20.00	926.29	0.00	0.08
	Hotelling's Trace	0.38	5.28	20.00	1110.00	0.00	0.09
	Roy's Largest Root	0.28	15.97	5.00	282.00	0.00	0.22

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Functionality	31.23a	5.00	6.25	10.48	0.00	0.16
	Reliability	38.82b	5.00	7.76	12.33	0.00	0.18
	Effectiveness	33.21c	5.00	6.64	7.99	0.00	0.12
	Structural Assurance	31.53d	5.00	6.31	8.87	0.00	0.14
	Situational Normality	20.54e	5.00	4.11	5.62	0.00	0.09
Intercept	Functionality	178.31	1.00	178.31	299.01	0.00	0.51
	Reliability	77.71	1.00	77.71	123.43	0.00	0.30
	Effectiveness	67.39	1.00	67.39	81.03	0.00	0.22
	Structural Assurance	75.72	1.00	75.72	106.52	0.00	0.27
	Situational Normality	77.72	1.00	77.72	106.43	0.00	0.27
Faith in Humanity (Benevolence)	Functionality	3.35	1.00	3.35	5.62	0.02	0.02
	Reliability	17.95	1.00	17.95	28.51	0.00	0.09
	Effectiveness	20.14	1.00	20.14	24.22	0.00	0.08
	Structural Assurance	17.32	1.00	17.32	24.36	0.00	0.08
	Situational Normality	17.41	1.00	17.41	23.83	0.00	0.08
Group	Functionality	27.42	4.00	6.86	11.50	0.00	0.14
	Reliability	19.25	4.00	4.81	7.65	0.00	0.10
	Effectiveness	11.28	4.00	2.82	3.39	0.01	0.05
	Structural Assurance	13.01	4.00	3.25	4.58	0.00	0.06
	Situational Normality	2.59	4.00	0.65	0.89	0.47	0.01
Error	Functionality	168.77	283.00	0.60			
	Reliability	178.16	283.00	0.63			
	Effectiveness	235.36	283.00	0.83			
	Structural Assurance	201.16	283.00	0.71			
	Situational Normality	206.66	283.00	0.73			
Total	Functionality	7064.61	289.00				
	Reliability	5254.36	289.00				
	Effectiveness	5025.51	289.00				
	Structural Assurance	5122.91	289.00				
	Situational Normality	5211.97	289.00				
Corrected Total	Functionality	200.00	288.00				
	Reliability	216.98	288.00				
	Effectiveness	268.57	288.00				
	Structural Assurance	232.69	288.00				
	Situational Normality	227.20	288.00				

a. R Squared = 0.156 (Adjusted R Squared = 0.141)
b. R Squared = 0.179 (Adjusted R Squared = 0.164)
c. R Squared = 0.124 (Adjusted R Squared = 0.108)
d. R Squared = 0.135 (Adjusted R Squared = 0.120)
e. R Squared = 0.090 (Adjusted R Squared = 0.074)

4.3.5. Faith in Humanity (Competence)

Box's Test of Equality of Covariance Matrices

Box's M	91.78
F	1.50
df1	60
df2	157801.57
Sig.	0.01

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.39	35.79	5.00	276.00	0.00	0.39
	Wilks' Lambda	0.61	35.79	5.00	276.00	0.00	0.39
	Hotelling's Trace	0.65	35.79	5.00	276.00	0.00	0.39
	Roy's Largest Root	0.65	35.79	5.00	276.00	0.00	0.39
Faith in Humanity (Competence)	Pillai's Trace	0.10	6.23	5.00	276.00	0.00	0.10
	Wilks' Lambda	0.90	6.23	5.00	276.00	0.00	0.10
	Hotelling's Trace	0.11	6.23	5.00	276.00	0.00	0.10
	Roy's Largest Root	0.11	6.23	5.00	276.00	0.00	0.10
Group	Pillai's Trace	0.32	4.89	20.00	1116.00	0.00	0.08
	Wilks' Lambda	0.70	5.18	20.00	916.34	0.00	0.09
	Hotelling's Trace	0.39	5.40	20.00	1098.00	0.00	0.09
	Roy's Largest Root	0.29	15.964c	5.00	279.00	0.00	0.22

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Functionality	37.55a	5.00	7.51	13.00	0.00	0.19
	Reliability	34.01b	5.00	6.80	10.51	0.00	0.16
	Effectiveness	30.48c	5.00	6.10	7.24	0.00	0.11
	Structural Assurance	32.82d	5.00	6.56	9.24	0.00	0.14
	Situational Normality	13.08e	5.00	2.62	3.44	0.01	0.06
Intercept	Functionality	94.82	1.00	94.82	164.21	0.00	0.37
	Reliability	52.77	1.00	52.77	81.51	0.00	0.23
	Effectiveness	44.92	1.00	44.92	53.31	0.00	0.16
	Structural Assurance	42.97	1.00	42.97	60.48	0.00	0.18
	Situational Normality	59.64	1.00	59.64	78.54	0.00	0.22
Faith in Humanity (Competence)	Functionality	9.53	1.00	9.53	16.51	0.00	0.06
	Reliability	13.85	1.00	13.85	21.39	0.00	0.07
	Effectiveness	15.96	1.00	15.96	18.94	0.00	0.06
	Structural Assurance	18.34	1.00	18.34	25.81	0.00	0.08
	Situational Normality	10.22	1.00	10.22	13.46	0.00	0.05
Group	Functionality	27.29	4.00	6.82	11.81	0.00	0.14
	Reliability	18.99	4.00	4.75	7.33	0.00	0.10
	Effectiveness	13.72	4.00	3.43	4.07	0.00	0.06
	Structural Assurance	14.12	4.00	3.53	4.97	0.00	0.07
	Situational Normality	2.54	4.00	0.63	0.84	0.50	0.01
Error	Functionality	161.69	280.00	0.58			
	Reliability	181.28	280.00	0.65			
	Effectiveness	235.93	280.00	0.84			
	Structural Assurance	198.92	280.00	0.71			
	Situational Normality	212.61	280.00	0.76			
Total	Functionality	6988.89	286.00				
	Reliability	5186.40	286.00				
	Effectiveness	4978.07	286.00				
	Structural Assurance	5063.72	286.00				
	Situational Normality	5142.61	286.00				
Corrected Total	Functionality	199.23	285.00				
	Reliability	215.29	285.00				
	Effectiveness	266.41	285.00				
	Structural Assurance	231.74	285.00				
	Situational Normality	225.69	285.00				

a. R Squared = 0.188 (Adjusted R Squared = 0.174)
b. R Squared = 0.158 (Adjusted R Squared = 0.143)
c. R Squared = 0.114 (Adjusted R Squared = 0.099)
d. R Squared = 0.142 (Adjusted R Squared = 0.126)
e. R Squared = 0.058 (Adjusted R Squared = 0.041)

4.3.6. Faith in Humanity (Integrity)

Box's Test of Equality of Covariance Matrices

Box's M	93.49
F	1.50
df1	60
df2	160715.42
Sig.	0.01

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.46	48.37	5.00	279.00	0.00	0.46
	Wilks' Lambda	0.54	48.37	5.00	279.00	0.00	0.46
	Hotelling's Trace	0.87	48.37	5.00	279.00	0.00	0.46
	Roy's Largest Root	0.87	48.37	5.00	279.00	0.00	0.46
Faith in Humanity (Integrity)	Pillai's Trace	0.12	7.73	5.00	279.00	0.00	0.12
	Wilks' Lambda	0.88	7.73	5.00	279.00	0.00	0.12
	Hotelling's Trace	0.14	7.73	5.00	279.00	0.00	0.12
	Roy's Largest Root	0.14	7.73	5.00	279.00	0.00	0.12
Group	Pillai's Trace	0.32	4.93	20.00	1128.00	0.00	0.08
	Wilks' Lambda	0.70	5.22	20.00	926.29	0.00	0.09
	Hotelling's Trace	0.39	5.45	20.00	1110.00	0.00	0.09
	Roy's Largest Root	0.29	16.33	5.00	282.00	0.00	0.23

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Functionality	34.49a	5.00	6.90	11.80	0.00	0.17
	Reliability	36.98b	5.00	7.40	11.63	0.00	0.17
	Effectiveness	28.55c	5.00	5.71	6.73	0.00	0.11
	Structural Assurance	35.99d	5.00	7.20	10.36	0.00	0.16
	Situational Normality	18.45e	5.00	3.69	5.00	0.00	0.08
Intercept	Functionality	133.77	1.00	133.77	228.74	0.00	0.45
	Reliability	65.97	1.00	65.97	103.72	0.00	0.27
	Effectiveness	61.88	1.00	61.88	72.96	0.00	0.21
	Structural Assurance	53.35	1.00	53.35	76.76	0.00	0.21
	Situational Normality	66.63	1.00	66.63	90.33	0.00	0.24
Faith in Humanity (Integrity)	Functionality	6.61	1.00	6.61	11.31	0.00	0.04
	Reliability	16.11	1.00	16.11	25.33	0.00	0.08
	Effectiveness	15.48	1.00	15.48	18.25	0.00	0.06
	Structural Assurance	21.78	1.00	21.78	31.34	0.00	0.10
	Situational Normality	15.32	1.00	15.32	20.77	0.00	0.07
Group	Functionality	29.49	4.00	7.37	12.61	0.00	0.15
	Reliability	22.59	4.00	5.65	8.88	0.00	0.11
	Effectiveness	11.68	4.00	2.92	3.44	0.01	0.05
	Structural Assurance	14.75	4.00	3.69	5.31	0.00	0.07
	Situational Normality	3.99	4.00	1.00	1.35	0.25	0.02
Error	Functionality	165.51	283.00	0.59			
	Reliability	180.00	283.00	0.64			
	Effectiveness	240.02	283.00	0.85			
	Structural Assurance	196.69	283.00	0.70			
	Situational Normality	208.75	283.00	0.74			
Total	Functionality	7064.61	289.00				
	Reliability	5254.36	289.00				
	Effectiveness	5025.51	289.00				
	Structural Assurance	5122.91	289.00				
	Situational Normality	5211.97	289.00				
Corrected Total	Functionality	200.00	288.00				
	Reliability	216.98	288.00				
	Effectiveness	268.57	288.00				
	Structural Assurance	232.69	288.00				
	Situational Normality	227.20	288.00				

a. R Squared = 0.172 (Adjusted R Squared = 0.158)
b. R Squared = 0.170 (Adjusted R Squared = 0.156)
c. R Squared = 0.106 (Adjusted R Squared = 0.091)
d. R Squared = 0.155 (Adjusted R Squared = 0.140)
e. R Squared = 0.081 (Adjusted R Squared = 0.065)

4.3.7. Subjective Norms

Box's Test of Equality of Covariance Matrices

Box's M	78.18
F	1.23
df1	60
df2	65505.86
Sig.	0.11

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.70	82.95	5.00	177.00	0.00	0.70
	Wilks' Lambda	0.30	82.95	5.00	177.00	0.00	0.70
	Hotelling's Trace	2.34	82.95	5.00	177.00	0.00	0.70
	Roy's Largest Root	2.34	82.95	5.00	177.00	0.00	0.70
Subjective Norms	Pillai's Trace	0.17	7.03	5.00	177.00	0.00	0.17
	Wilks' Lambda	0.83	7.03	5.00	177.00	0.00	0.17
	Hotelling's Trace	0.20	7.03	5.00	177.00	0.00	0.17
	Roy's Largest Root	0.20	7.03	5.00	177.00	0.00	0.17
Group	Pillai's Trace	0.27	2.55	20.00	720.00	0.00	0.07
	Wilks' Lambda	0.75	2.66	20.00	587.99	0.00	0.07
	Hotelling's Trace	0.31	2.75	20.00	702.00	0.00	0.07
	Roy's Largest Root	0.24	8.52	5.00	180.00	0.00	0.19

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Functionality	25.83a	5.00	5.17	10.55	0.00	0.23
	Reliability	15.50b	5.00	3.10	4.57	0.00	0.11
	Effectiveness	18.89c	5.00	3.78	4.69	0.00	0.12
	Structural Assurance	15.89d	5.00	3.18	4.65	0.00	0.11
	Situational Normality	5.05e	5.00	1.01	1.17	0.33	0.03
Intercept	Functionality	181.05	1.00	181.05	369.60	0.00	0.67
	Reliability	147.05	1.00	147.05	216.56	0.00	0.55
	Effectiveness	111.42	1.00	111.42	138.31	0.00	0.43
	Structural Assurance	128.45	1.00	128.45	187.97	0.00	0.51
	Situational Normality	160.14	1.00	160.14	184.76	0.00	0.51
Subjective Norms	Functionality	14.72	1.00	14.72	30.06	0.00	0.14
	Reliability	7.55	1.00	7.55	11.12	0.00	0.06
	Effectiveness	14.09	1.00	14.09	17.49	0.00	0.09
	Structural Assurance	10.04	1.00	10.04	14.69	0.00	0.08
	Situational Normality	4.44	1.00	4.44	5.13	0.03	0.03
Group	Functionality	10.69	4.00	2.67	5.46	0.00	0.11
	Reliability	6.74	4.00	1.69	2.48	0.05	0.05
	Effectiveness	4.08	4.00	1.02	1.27	0.29	0.03
	Structural Assurance	3.35	4.00	0.84	1.23	0.30	0.03
	Situational Normality	0.84	4.00	0.21	0.24	0.92	0.01
Error	Functionality	88.67	181.00	0.49			
	Reliability	122.91	181.00	0.68			
	Effectiveness	145.80	181.00	0.81			
	Structural Assurance	123.68	181.00	0.68			
	Situational Normality	156.87	181.00	0.87			
Total	Functionality	4537.00	187.00				
	Reliability	3416.54	187.00				
	Effectiveness	3168.71	187.00				
	Structural Assurance	3241.06	187.00				
	Situational Normality	3396.24	187.00				
Corrected Total	Functionality	114.50	186.00				
	Reliability	138.41	186.00				
	Effectiveness	164.70	186.00				
	Structural Assurance	139.57	186.00				
	Situational Normality	161.92	186.00				

a. R Squared = 0.226 (Adjusted R Squared = 0.204)
b. R Squared = 0.112 (Adjusted R Squared = 0.087)
c. R Squared = 0.115 (Adjusted R Squared = 0.090)
d. R Squared = 0.114 (Adjusted R Squared = 0.089)
e. R Squared = 0.031 (Adjusted R Squared = 0.004)

4.3.8. Perceived Safety of the Economic Environment

Box's Test of Equality of Covariance Matrices

Box's M	93.49
F	1.50
df1	60
df2	160715.42
Sig.	0.01

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.54	65.77	5.00	279.00	0.00	0.54
	Wilks' Lambda	0.46	65.77	5.00	279.00	0.00	0.54
	Hotelling's Trace	1.18	65.77	5.00	279.00	0.00	0.54
	Roy's Largest Root	1.18	65.77	5.00	279.00	0.00	0.54
Faith in Economic Environment	Pillai's Trace	0.09	5.73	5.00	279.00	0.00	0.09
	Wilks' Lambda	0.91	5.73	5.00	279.00	0.00	0.09
	Hotelling's Trace	0.10	5.73	5.00	279.00	0.00	0.09
	Roy's Largest Root	0.10	5.73	5.00	279.00	0.00	0.09
Group	Pillai's Trace	0.31	4.80	20.00	1128.00	0.00	0.08
	Wilks' Lambda	0.71	5.09	20.00	926.29	0.00	0.08
	Hotelling's Trace	0.38	5.32	20.00	1110.00	0.00	0.09
	Roy's Largest Root	0.29	16.14	5.00	282.00	0.00	0.22

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Functionality	38.43a	5.00	7.69	13.46	0.00	0.19
	Reliability	24.36b	5.00	4.87	7.16	0.00	0.11
	Effectiveness	23.31c	5.00	4.66	5.38	0.00	0.09
	Structural Assurance	25.74d	5.00	5.15	7.04	0.00	0.11
	Situational Normality	10.64e	5.00	2.13	2.78	0.02	0.05
Intercept	Functionality	169.26	1.00	169.26	296.47	0.00	0.51
	Reliability	145.00	1.00	145.00	213.04	0.00	0.43
	Effectiveness	107.12	1.00	107.12	123.61	0.00	0.30
	Structural Assurance	106.97	1.00	106.97	146.27	0.00	0.34
	Situational Normality	123.61	1.00	123.61	161.54	0.00	0.36
Faith in Economic Environment	Functionality	10.55	1.00	10.55	18.47	0.00	0.06
	Reliability	3.48	1.00	3.48	5.12	0.02	0.02
	Effectiveness	10.24	1.00	10.24	11.82	0.00	0.04
	Structural Assurance	11.52	1.00	11.52	15.76	0.00	0.05
	Situational Normality	7.51	1.00	7.51	9.81	0.00	0.03
Group	Functionality	26.65	4.00	6.66	11.67	0.00	0.14
	Reliability	19.76	4.00	4.94	7.26	0.00	0.09
	Effectiveness	11.48	4.00	2.87	3.31	0.01	0.05
	Structural Assurance	12.82	4.00	3.21	4.38	0.00	0.06
	Situational Normality	2.55	4.00	0.64	0.83	0.51	0.01
Error	Functionality	161.57	283.00	0.57			
	Reliability	192.63	283.00	0.68			
	Effectiveness	245.26	283.00	0.87			
	Structural Assurance	206.95	283.00	0.73			
	Situational Normality	216.56	283.00	0.77			
Total	Functionality	7064.61	289.00				
	Reliability	5254.36	289.00				
	Effectiveness	5025.51	289.00				
	Structural Assurance	5122.91	289.00				
	Situational Normality	5211.97	289.00				
Corrected Total	Functionality	200.00	288.00				
	Reliability	216.98	288.00				
	Effectiveness	268.57	288.00				
	Structural Assurance	232.69	288.00				
	Situational Normality	227.20	288.00				

a. R Squared = 0.192 (Adjusted R Squared = 0.178)
b. R Squared = 0.112 (Adjusted R Squared = 0.097)
c. R Squared = 0.087 (Adjusted R Squared = 0.071)
d. R Squared = 0.111 (Adjusted R Squared = 0.095)
e. R Squared = 0.047 (Adjusted R Squared = 0.030)

4.3.9. Initial Familiarity of Technology

Box's Test of Equality of Covariance Matrices

Box's M	83.22
F	1.31
df1	60
df2	84805.27
Sig.	0.05

Multivariate Tests

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0.83	190.46	5.00	202.00	0.00	0.83
	Wilks' Lambda	0.18	190.46	5.00	202.00	0.00	0.83
	Hotelling's Trace	4.71	190.46	5.00	202.00	0.00	0.83
	Roy's Largest Root	4.71	190.46	5.00	202.00	0.00	0.83
Initial Technology Awareness	Pillai's Trace	0.13	6.05	5.00	202.00	0.00	0.13
	Wilks' Lambda	0.87	6.05	5.00	202.00	0.00	0.13
	Hotelling's Trace	0.15	6.05	5.00	202.00	0.00	0.13
	Roy's Largest Root	0.15	6.05	5.00	202.00	0.00	0.13
Group	Pillai's Trace	0.30	3.34	20.00	820.00	0.00	0.08
	Wilks' Lambda	0.72	3.47	20.00	670.91	0.00	0.08
	Hotelling's Trace	0.36	3.56	20.00	802.00	0.00	0.08
	Roy's Largest Root	0.24	9.98	5.00	205.00	0.00	0.20

Tests of Between-Subjects Effects

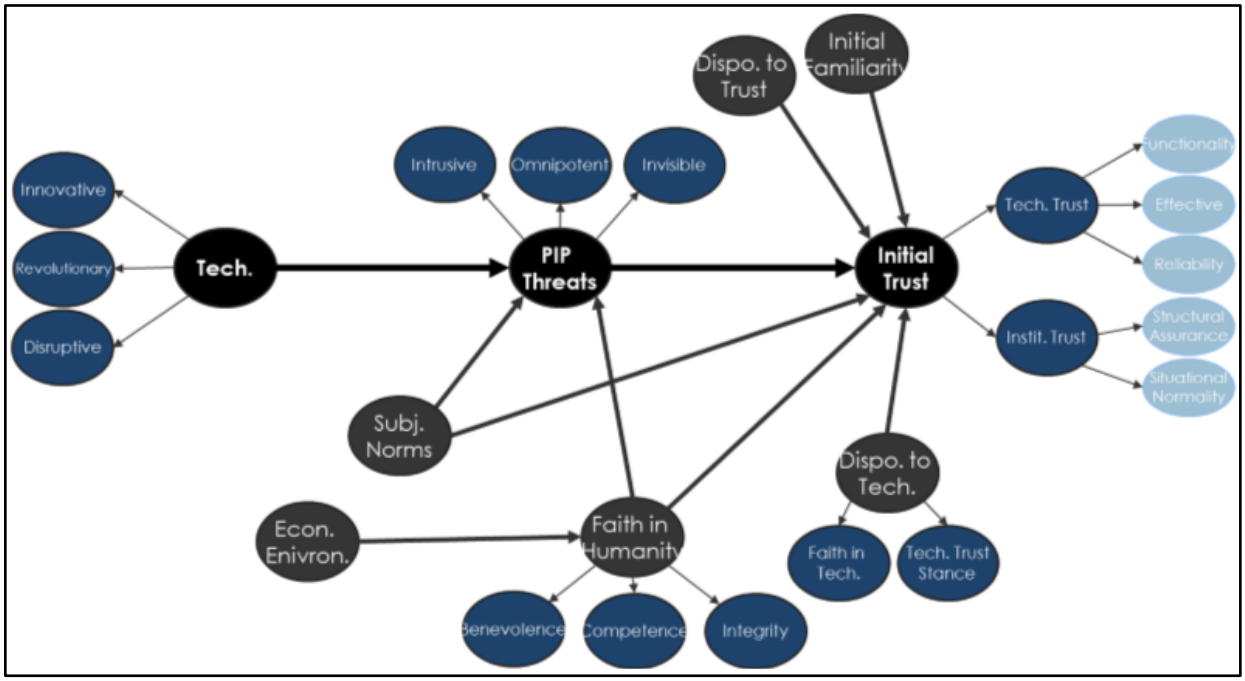
Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Functionality	24.67a	5.00	4.93	7.88	0.00	0.16
	Reliability	19.82b	5.00	3.96	5.47	0.00	0.12
	Effectiveness	15.33c	5.00	3.07	3.67	0.00	0.08
	Structural Assurance	14.14d	5.00	2.83	3.69	0.00	0.08
	Situational Normality	24.46e	5.00	4.89	6.21	0.00	0.13
Intercept	Functionality	557.51	1.00	557.51	890.30	0.00	0.81
	Reliability	387.17	1.00	387.17	533.93	0.00	0.72
	Effectiveness	335.77	1.00	335.77	401.41	0.00	0.66
	Structural Assurance	376.13	1.00	376.13	490.06	0.00	0.70
	Situational Normality	300.53	1.00	300.53	381.26	0.00	0.65
Initial Technology Awareness	Functionality	4.57	1.00	4.57	7.30	0.01	0.03
	Reliability	5.93	1.00	5.93	8.18	0.01	0.04
	Effectiveness	9.20	1.00	9.20	11.00	0.00	0.05
	Structural Assurance	4.66	1.00	4.66	6.08	0.02	0.03
	Situational Normality	22.95	1.00	22.95	29.12	0.00	0.12
Group	Functionality	11.44	4.00	2.86	4.57	0.00	0.08
	Reliability	8.01	4.00	2.00	2.76	0.03	0.05
	Effectiveness	10.31	4.00	2.58	3.08	0.02	0.06
	Structural Assurance	5.54	4.00	1.38	1.80	0.13	0.03
	Situational Normality	3.57	4.00	0.89	1.13	0.34	0.02
Error	Functionality	129.00	206.00	0.63			
	Reliability	149.38	206.00	0.73			
	Effectiveness	172.32	206.00	0.84			
	Structural Assurance	158.11	206.00	0.77			
	Situational Normality	162.38	206.00	0.79			
Total	Functionality	5140.44	212.00				
	Reliability	3828.67	212.00				
	Effectiveness	3581.65	212.00				
	Structural Assurance	3655.36	212.00				
	Situational Normality	3799.93	212.00				
Corrected Total	Functionality	153.67	211.00				
	Reliability	169.20	211.00				
	Effectiveness	187.65	211.00				
	Structural Assurance	172.25	211.00				
	Situational Normality	186.84	211.00				

a. R Squared = 0.161 (Adjusted R Squared = 0.140)
b. R Squared = 0.117 (Adjusted R Squared = 0.096)
c. R Squared = 0.082 (Adjusted R Squared = 0.059)
d. R Squared = 0.082 (Adjusted R Squared = 0.060)
e. R Squared = 0.131 (Adjusted R Squared = 0.110)

Appendix 5. SmartPLS 3 Model Development (as per Lowry & Gaskin (2014))

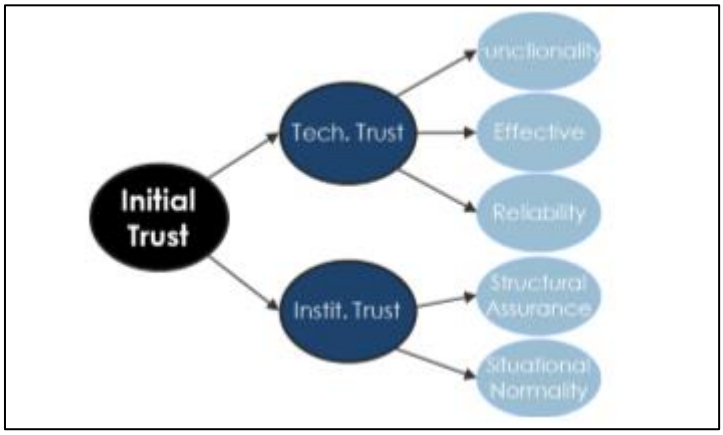
5.1. PLS Model for Analysis

The following diagram illustrates the complete initial technology trust model that was modelled in SmartPLS3. The third order latent variables are represented by light blue circles. The second order latent variables are represented by dark blue circles. The first order latent variables are represented by the grey and black circles, with the black variables illustrating the core relationship investigated as part of this thesis and tested in the primary experiment (Study 1).



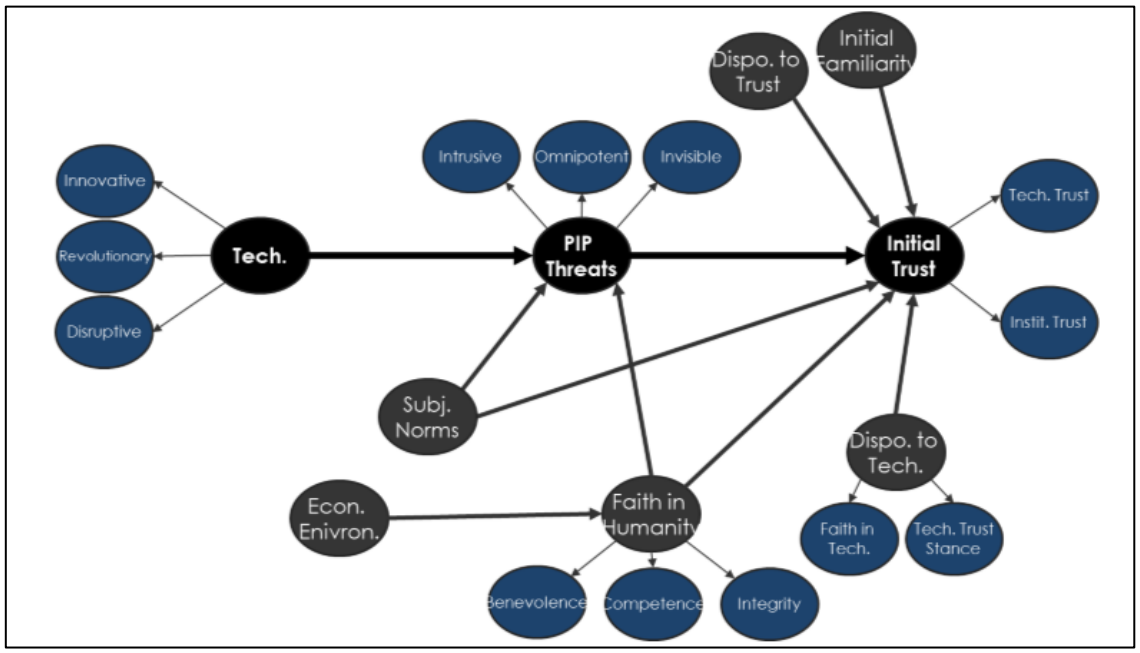
5.2. Third Order Variables to Test Outer Model Reliability

The third order variables were tested first. The PLS results generated were used to assess outer model reliability and the latent variables scores calculated for technology trust and institutional-based trust were extracted and inputted as the latent variable values for technology trust and institutional-based trust in the second phase (described in Appendix 5.3.)



5.3. Second and First Order Variables to Test Outer Model Reliability

The second and first order latent variables were analysed with the previously calculated latent variables scores for technology trust and institutional-based trust for the respective latent variables. The results generated were used to assess outer model reliability. The latent variable scores were extracted for each first order variable and inputted as the latent variables values for the third phase of analysis (described in Appendix 5.4.).



5.4. Second and First Order Variables to Test Inner Model Reliability

The second and first order latent variables were analysed using the previously calculated latent variable scores as their latent variable values for the last part of the PLS analysis. The results of the PLS procedure was then used to test the inner model reliability.