INFORMATION
&
MANAGEMENT
THE INTERNATIONAL JOURNAL OF INFORMATION SYSTEMS APPLICATIONS

Privacy and the Internet of Things – An Experiment in Discrete Choice

David Goad (Conceptualization) (Methodology) (Investigation) (Formal analysis) (Data curation) (Writing - original draft) (Visualization), Andrew Collins (Methodology) (Software) (Formal analysis) (Validation) (Writing - review and editing) (Visualization), Uri Gal (Writing - review and editing)

PII:	S0378-7206(18)31055-3
DOI:	https://doi.org/10.1016/j.im.2020.103292
Reference:	INFMAN 103292
To appear in:	*Information & Management*
Received Date:	19 December 2018
Revised Date:	28 February 2020
Accepted Date:	29 February 2020

Please cite this article as: Goad D, Collins A, Gal U, Privacy and the Internet of Things – An Experiment in Discrete Choice, *Information and amp; Management* (2020), doi: https://doi.org/10.1016/j.im.2020.103292

Privacy and the Internet of Things – An Experiment in Discrete Choice

Full Length Article

David Goad (david.goad@sydney.edu.au)* , Andrew Collins and Uri Gal University
of Sydney Business School, University of Sydney Abercrombie Streets and
Codrington Streets, Darlington NSW 2006 Sydney Australia

Abstract

The Internet of Things (IoT) is the concept that everyday devices are connected to the Internet generating data about us and the world around us. With the number of devices connected directly to the Internet expected to be three times the number of people by 2020, the potential for a reduction in personal privacy is evident. This research fills a gap in the literature by conducting a quantitative analysis of people's privacy preferences as it relates to the IoT. Our findings provide potential guidance to practitioners in their IoT architectural design and increase our understanding of privacy preference overall.

Keywords: Internet of Things, IoT, Privacy, Discrete Choice Methods

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Contents

Introduction and Background

The Internet of Things (IoT) can be defined as everyday devices connected to the Internet providing highly useful integrated data about us and the world around us. It is expected that 20 Billion "Things" will be connected to the Internet by 2020, [1] which could exceed the number of people connected to the Internet by three to five times. These Things include but are not limited to wearable devices, newly purchased automobiles and smart home devices, such as smart speakers and smart TVs.

There have been many conceptualizations and definitions of the concept of *Privacy* in the literature. These include but are not limited to the right to be left alone, the ability to limit access to the self, secrecy and the concealment of matters from others, control over one's personal information, the protection of one's individuality and the ability to limit access to the intimate aspects of one's life [2]. For the purposes of this research, we define Privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [3].

Since its inception, the Internet has generated concerns about privacy as users trade information about themselves for access to the services that the Internet can provide. Yet these same users often do not know how that information will be used or where it will end up. In a recent survey, 74% of the respondents indicated that it was "very important" for them to be in control of who can get information about them [4]. Other cross-national surveys have demonstrated that most people (from 74% to 90% depending on the country) believe that laws that prohibit the buying and selling of information about them by businesses should be put into place [5].

The IoT promises to increase these previously held information privacy concerns with the Internet, in that the average number of Internet-enabled devices or "Things" in the home is projected to grow from 10 to 50 by 2020, bringing the level of available personal data to an all-time high [6]. Wearable devices that track our activities and vital health statistics are expected to be a $61.7 Billion market by 2020 [7]. Many organizations generate significant revenue from the personal data that they collect about the people that use their products and services, which in turn encourages the collection of even more data [8]. A recent survey demonstrated that geospatial data collected from people's movement, which is often derived from IoT devices, was the third largest category of Big Data being collected [9].

Against this backdrop, organizations deploying IoT solutions are facing increasing expectations from governments in terms of IoT privacy. For example, the Australian government recently enacted privacy legislation, which included a comprehensive duty to report any data breaches including the cause of the breach, and what has happened to that data [10]. Similarly the General Data Protection Regulation legislation enforced in the EU in 2018 has had and will have significant impacts, as it establishes whole new sets of expectations on organizations that collect personal data [11]. Meeting these expectations comes at increasing costs. Rising privacy regulations are expected to increase the amount businesses spend on privacy by 20% from 2016 to 2019 [12]. Global privacy legislation is already estimated to cost multinational organizations an average of $3.5 million per year per organization [13]. The impact on small and medium businesses will be disproportionate with an expected rise from 16% to 40% in those organizations' IT budgets due to increased privacy legislation [14].

Organizations will face technical challenges in addressing these increasing privacy concerns. Security and privacy in IoT are known challenges due to the limited resources of the many different "Things" in the IoT [15]. The "Things" in the IoT are commonly designed with limited memory, computational power and storage, to reduce cost, and achieve ubiquity of use. This means that standard security and privacy tools and protocols are often not natively present in these devices, which increases their vulnerability. By some estimates, by 2020 more than 50% of IoT implementations are likely to expose sensitive information due to inadequate controls [16].

Given the increasing costs and technical difficulties involved in complying with this new privacy regulation, which in general does not take into account the challenges of the IoT, a critical question to ask is "Which types of privacy and privacy-protection mechanisms are more important than others to users in the domain of the IoT?" To effectively debate this question one must first appropriately assess the value placed on privacy in an IoT context. This is of particular importance in light of the well-known Privacy Paradox, wherein individuals' revealed privacy preferences are often much lower than their stated privacy preferences [4, 5]. Research has also shown that increased privacy often does not create benefit for the person retaining the private information or society in general [17]. Consequently, the costs required to achieve these increases in privacy driven by these most recent legislations may not necessarily outweigh the actual value people associate with that increased privacy in the first place.

To address this question, we have adopted Discrete Choice Experiment (DCE) techniques to analyze and quantify individuals' IoT privacy preferences and the valuation of privacy in an IoT context. We have done so by constructing a realistic IoT scenario, the purchase of an Internet connected everyday common fitness tracker. We asked survey participants to choose which of two presented fitness trackers they would purchase, wherein each tracker has a different set of attributes that affects privacy differently and a different purchase price. By having to trade-off between the purchase price and the tracker features, with their associated privacy implications, a monetary valuation for privacy can be assigned. In this way we quantified, in monetary terms, peoples' Willingness To Accept (WTA) clear infringements on their privacy. In a similar fashion but using different attributes, we also quantified their Willingness to Pay (WTP) for beneficial tracker features that inherently improve privacy. Further, we analyzed the impact of a number of respondent characteristics and types of private information on WTA and WTP. In some cases our research confirms previous findings in the literature regarding privacy preference and valuation in the context of the Internet and IoT, and in other cases it suggests that there are differences in privacy preference and privacy valuation specific to the IoT.

We acknowledge that there is already a growing body of literature on the quantitative analysis of privacy preference in the context of the IoT [18-21]. By using DCE techniques to conduct our analysis, we add to this literature by using methods, which are consistent with theories of consumer behavior. Privacy preference is expressed through a choice between alternative products as opposed to a stated preference for privacy, which may be an inaccurate representation of privacy preference [20, 22-24]. The DCE method allows for the quantification of preference and monetary values of privacy preference within various contexts of the IoT. Compared to the rankings or rating responses of Conjoint Analysis (CA) [57], the choice response better matches market decisions (i.e., purchasing an IoT device), and results in less respondent burden. While novel to the use of privacy preference analysis in the IoT, these techniques are well established in the academic literature, [25, 26] and provide the ability to assess a commercial value to privacy preference and to observe how that commercial value is influenced by various factors and attributes. In this way, not only do we add to the growing academic literature around privacy in the IoT, but we also help facilitate a discussion around the importance that users place on different types of privacy and privacy-protection mechanisms in the domain of the IoT. Thus, we provide guidance to practitioners on what types of information should require stronger privacy controls based on their perceived value and in what context these controls should be increased with a view to optimizing IoT security and privacy investments. In addition to these contributions, we also suggest avenues for further research into IoT privacy preference.

Unpacking the Concept of Privacy

Privacy is a complex concept, but one that is relatively well developed in the literature. To build an effective scaffold upon which to base our subsequent experimental design and analysis, we first review the existing literature on privacy in the IoT. Then, we define the concept of privacy that we use for our analysis. We then discuss the relationship between a person's observed behavior and the influences that affect this behavior in the context of privacy, the IoT, and our proposed DCE. To do this, we draw on sources both from the privacy literature [27, 28] and the DCE literature [25, 29] . We then explore several theoretical models of privacy preference with a view to informing our research design. As our focus is to quantify people's WTA a loss of privacy from a monetary perspective, we review previous quantitative studies on privacy valuation that have used other statistical techniques to provide a starting point for our analysis. After this, we go on to define our experimental design, our process for data collection and analysis, and then present our results.

Exploring Privacy and the Internet of Things in the Literature

Given the rapid increase in the amount of available data due to the IoT, it is not surprising that there is a rapidly developing body of literature related to understanding the impact of IoT on privacy preference. The current literature has developed along three broad themes: 1) understanding the impact of IoT on privacy concern and stated privacy preference; 2) understanding the antecedents, contributory factors, and privacy calculus that contribute to the creation of IoT privacy preference, and; 3) research into the development of tools and tactics (both technical and regulatory) to address the concern for privacy within the IoT.

First, regarding the impact IoT has on privacy preference, several authors have used IoT-based scenarios [20, 30] or vignettes, [19] to survey respondents on their stated privacy preference within a variety of IoT contexts. This research has concluded that respondents' stated privacy preferences are diverse, context–

dependent, and highly personal, but that there is a high degree of consistency when an individual respondent is presented with different contexts but which have similar attributes and are asked to state their privacy preference [19, 20]. This line of research has also identified the need for technology that can provide an awareness of data collection, as awareness is considered an important factor in IoT privacy preference formation [19]. We will come back to this concept later when we discuss our research design and our inclusion of a feature in the fitness tracker that provides users with the ability to track the usage of data collected by the tracker. Consistent with these survey results, models have been developed which demonstrate that "tolerance or requirements with respect to privacy/security issues may not necessarily be the same across individuals and their associated IoT devices across different points in time" and that there is benefit to social welfare of privacy differentiation in the IoT [31]. This potentially supports a view that "more privacy is not always better" and that there is an appropriate level of privacy based on the value attached to privacy by the individual in a specific context. We will explore this point more fully later in the paper when we develop our research design. This issue of the impact of IoT on privacy concern and privacy preference has also been investigated in a number of specific IoT contexts. For example there is an increasing body of literature on privacy preference specific to the "smart home" segment of the IoT [32-34]. Similarly, there has also been research into IoT privacy preference in the Health Care space [35]. All evaluate the influence of various IoT scenarios on privacy preference.

Second, regarding the antecedents, contributory factors, and calculus that contributes to IoT privacy preference, a number of articles have examined the antecedents and factors that contribute to stated privacy preference to unpack the privacy calculus that people undertake within the IoT [18, 21, 36]. For example, believing that a high degree of the benefit from an IoT device is derived from the direct and indirect network externalities[37] that it provides and the majority of the risk associated with the IoT derives from the Concern for Information Privacy (CFIP)[27] that it creates, one group of researchers [18] use structural equation modeling and a combination of online surveys and interviews to build a model, which can predict intention to use an IoT device. Notably, in their investigations, the CFIP had less effect than the network externalities on the intention to use the device and most of CFIP-derived information was from improper access and unauthorized secondary use and not the actual collection of the data itself. Building on previous research [18], there have been attempts [21] to build a more refined risk versus benefits model, which includes information sensitivity, trust, the number of IoT services, perception of critical mass, perception of compatibility, and perception of complementarity as the independent variables and willingness to provide the private information as dependent variables. This study's conclusions confirm previous research that privacy risk factors, such as information sensitivity and trust, do not have a statistically significant impact on an individual's intention to use an IoT device. Finally, other research has demonstrated that influencers such as friends and privacy experts [36] can have a significant impact on the intention to use an IoT device, and that any perceived benefit from reduced privacy seems to have a positive effect on the willingness to provide private information [21].

Third, acknowledging the increased concern for privacy with the IoT, there have been several studies on how privacy related to the IoT might actually be achieved. Some authors [38] have broken down the typical IoT architecture used in industry into an application layer, transport layer, network layer, and perception layer. They analyzed the architectural and technology privacy issues related to each layer and identified a number of opportunities for increased privacy through an improved technical architecture. Other authors [39] have looked at architectural issues for specific types of IoT devices (e.g., fitness trackers) to improve privacy. Still other authors [40] have looked at the issue of user interface (UI) design to improve privacy. By using machine learning to group the potentially large number of IoT privacy choice settings, they aimed to create a more user friendly UI for improved device adoption and a closer fit to a user's privacy preference. Finally, other authors have considered the role that legislation will play in achieving privacy preference. For example, recent research which considers current privacy regulation in Australia has concluded that it does not effectively cover many IoT scenarios and made several suggestions for revision [41].

Summarizing the current state of the literature, it is possible to conclude that the role that privacy has in one's decision to use an IoT device is inconclusive and requires further study. Furthermore, privacy preferences related to the IoT are very personal, highly variable, and context specific, and there is a high potential for design solutions that can provide a personalized privacy solution for IoT use. Thus, there is an opportunity to further understand privacy preference in the IoT and to assign a valuation to that preference with a view to influence future investments into IoT privacy (both regulatory and technical).

The Relationship between Influences and Behaviors in a Consumer Choice Process that involves Privacy and the IoT

There is a complex interplay between influences and behaviors in an IoT-based consumer privacy choice process. We illustrate these processes in Figure 1 and discuss these processes through the lens of Privacy Concern and Discrete Choice in the following sections.

Privacy Concern as it relates to the Consumer Choice Process

Privacy Concern derives from one's desire for *Privacy* and is defined as a person's concerns associated with loss of privacy or loss of control over their personal information [42]. Measures of *Privacy Concern* in the literature have varied, e.g., "Willingness to provide privacy information" [21] and "Continued intention to use" [18] , and whether they would allow data collection [19]. They are commonly Likert scale responses integrated into structural equation models, and sometimes a mix of machine learning and statistical techniques. These may be expressed in the context of an individual's exposure to IoT devices at the time of the study [18], a single IoT device scenario [21], or combinations of privacy related information that is systematically varied by the researcher [19]. In analyzing *Privacy Concern,* it is important to note that there are a number of *Influences* that can impact on the level of concern, and therefore the degree to which a person wants to control their personal information. This will influence their choice of IoT device. These *Influences* can include but are not limited to product features, personal dispositions, covariates (such as age, sex, etc.) and contextual variables [28].

In undertaking product choices in relation to *Privacy Concern*, individuals undertake complex internal calculations around the potential benefit and risks associated with disclosing private personal information. This process is called the *Privacy Calculus* [42]. This Privacy Calculus then leads to a demonstrated *Privacy Preference*. We provide a detailed discussion of the various proposed theoretical models for how this *Privacy Calculus* is undertaken by an individual in a subsequent section.

As preference is a process, which involves the choice between alternatives [43], we define *Privacy Preference* as the choice between alternatives as they relate to decisions about controlling information about oneself. *Privacy Valuation* is the monetary value, which an individual assigns to a *Privacy*

Preference and is essentially one form of quantification of that preference. The assignment of a monetary value to both privacy preference and product features results is an observed choice between alternatives when a consumer is asked to make a purchase decision. By including the purchase price as one of the features of the product and observing the choice between features, we can assign an inferred value to both privacy preference and product features. The purchase and subsequent use of an IoT device is a useful and consequential measure of the extent to which privacy is traded off with other benefits and risks. If the various benefits outweigh the risk, including privacy impacts and the cost of the device, then an IoT device will be purchased and used.

Discrete Choice Theory as it relates to the Consumer Choice Process

We can draw upon the consumer behavior literature, which recognizes that goods are purchased because of the utility provided by their characteristics and features [44, 45]. Conceptual models developed in this stream of scholarly work have been adopted by the discrete choice literature [46].

The literature [25] has detailed how the various conceptual models of choice can be operationalized with discrete choice models. These choice models link product features to choice through the estimation of latent (dis)utility values that capture the preferences of decision makers for or against those features.

We extend the privacy calculus discussed in other studies and consider the calculus in a broader purchase/use calculus that includes privacy dimensions as well as other product features such as cost. Of particular interest is the trade-off between privacy features and product cost, as this allows WTP measures to be derived for privacy in a way that does not rely on directly stated WTP measures.

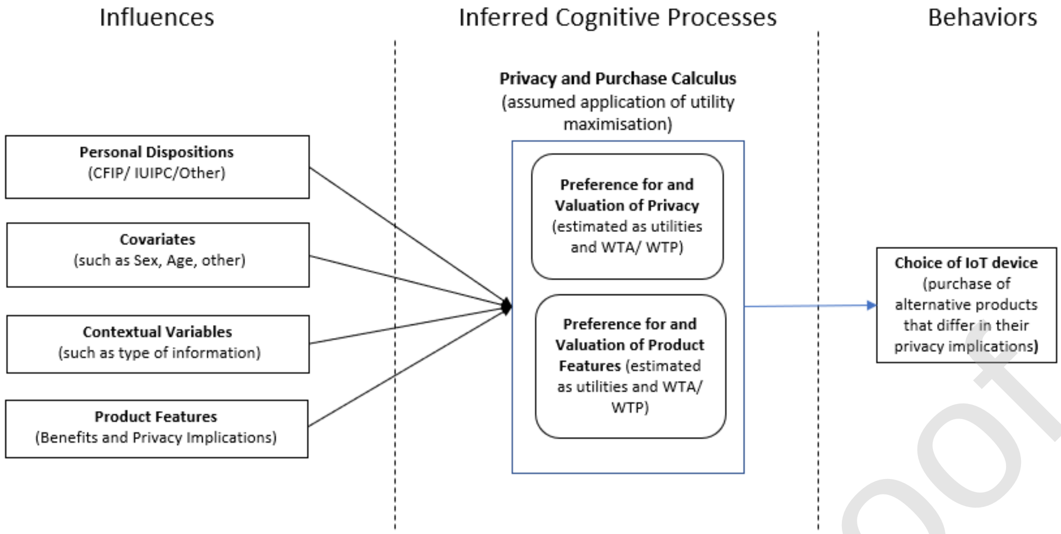

Influences
Inferred Cognitive Processes
Behaviors
Personal Dispositions (CFIP/ IUIPC/Other)
Covariates (such as Sex, Age, other)
Contextual Variables (such as type of information)
Product Features (Benefits and Privacy Implications)
Privacy and Purchase Calculus (assumed application of utility maximisation)
Preference for and Valuation of Privacy (estimated as utilities and WTA/ WTP)
Preference for and Valuation of Product Features (estimated as utilities and WTA/ WTP)
Choice of IoT device (purchase of alternative products that differ in their privacy implications)

Figure 1: The Relationship between Influences and Behaviors in a Consumer Choice Process that involves Privacy and the IoT

A Summary of the Consumer Choice Process that involves Privacy and the IoT

This proposed model for consumer choice in an IoT/privacy context extends on models from the existing general privacy literature for measuring privacy preference [27, 28] and models from the IoT privacy literature for measuring IoT privacy attitudes [18, 21] by using consumer choice concepts from the existing DCE literature [25]. In this way, we measure privacy preference through an observed choice as opposed to a stated preference, which avoids many of the well-documented challenges in the literature [20, 22-24] with using stated privacy preference. In so doing, we are able to observe both a utility and a monetary valuation associated to privacy as a function of various covariates, contextual variables, product features, and privacy preferences.

Privacy Theoretical Underpinnings and their Implications for IoT Privacy Research Design

Privacy Calculus Models and their impact on Privacy Research Design

A variety of *Privacy Calculus* models have been introduced in the literature to explain privacy preference in traditional IT or Internet information scenarios. One author [42] identified 15 distinct privacy-related theories in the literature. We select for our review and incorporation into our study theoretical models that focus on the individual factors that influence privacy preference and therefore privacy valuation. We do this for two reasons. First, the implementation of privacy regulation discussed above is mostly framed around concerns for individual privacy. Therefore, it is important to understand how individuals consider privacy. Second, the impact of the loss of privacy in an IoT environment mostly affects individuals rather than organizations or institutions. Based on these selection criteria and considerations, we specifically consider Protection Motivation Theory, Information Boundary Theory, Social Cognitive Theory and Personality Theory in our literature review as they address the individual factors that may affect IoT privacy preference and therefore privacy valuation. We subsequently incorporate the learnings from these theories into our research design.

Protection Motivation Theory considers an individual's intent to protect against threats [47]. This theory asserts that individuals conduct a threat appraisal and a coping appraisal assessing the degree of threat and their ability to address that threat when evaluating what actions they intend to take. Thus, an individual will consider the context in which the information he or she discloses will be used, and the potential threats that arise from this disclosure. This theory indicates that the type of private information disclosed would have an impact on the individual's perceived threat. We factor this into our research design by analyzing a number of different types of private information across a number of different contexts as these may impact the privacy preference and therefore privacy valuation.

Information Boundary Theory states that individuals set boundaries around themselves, which determine what information can be shared to other individuals or organizations [48]. Individuals and organizations that attempt to penetrate those boundaries are perceived as a threat. The theory posits that boundaries are regulated by issues such as the cost-benefit of releasing personal information and the context as to why it is being released. Therefore, this theory supports the idea that personal benefit is a key input into any individual's privacy calculus, which then impacts privacy preference and therefore privacy valuation. These considerations will be factored into our research design as well by using realistic scenarios that generate personal benefit from disclosing private information as well as scenarios, which attempt to generate no personal benefit such that we can assess to what degree personal benefit impacts privacy valuation.

In our research design, we also draw on social cognitive theory as it relates specifically to privacy [49]. This theory posits that an individual's knowledge acquisition is related to their observations of others, direct experiences as well as outside media influence. This theory also identifies previous experiences with privacy breach and previous news media exposure around privacy breach as influential in an individual's calculus around the disclosure of private information. We include these factors into our research design by asking our respondents about their previous experiences with privacy breach and news media exposure, to see what effect these influencers have on their privacy concern and therefore privacy preference and valuation.

Finally, we also draw on the personality theory [50]. This theory posits that an individual's personal attributes - such as agreeableness, conscientiousness, neuroticism, and intellect - will contribute to their natural disposition toward privacy. We mention this theory because it highlights the need to have a methodology for analyzing privacy preference, which addresses unmeasured heterogeneity in the sample population and can account for unforeseen influences. As we will be discussing later, one of the reasons why we chose DCE techniques was specifically because of their ability to handle this type of heterogeneity.

The Privacy Paradox and its impact on Privacy Research Design

Having discussed Privacy Preference models and their impact on privacy valuation, we now consider another significant theme in the literature called the Privacy Paradox. The Privacy Paradox is defined as the discrepancy between people's stated and revealed privacy preferences [51]. When asked to state their privacy preference, individuals would indicate a higher preference for privacy than they would reveal in their everyday actions. Initial studies on the topic hypothesized that this difference exists because of differences in the perception of *Risk* and *Trust* at the time the question is asked versus the time the action needs to be taken. Some [52] argue that the *Privacy Paradox* is a result of *bounded rationality* (limited information) in the individuals decision-making process. Accordingly, because of the Privacy Paradox, other researchers [53] have stated that "experiments should be conducted in realistic settings that provide a rich and relevant context" and "survey research should take into account the fact that self-reports on privacy behavior are unreliable."

We conclude from this research that it is preferable to design privacy preference studies that use realistic scenarios that require participants to make a choice between the benefits and potential losses associated with disclosing private information, and weigh the tradeoffs of privacy decisions. As we will discuss in the research design section, the novel use of a DCE and a realistic IoT-based scenario (the purchase of a fitness tracker) to evaluate privacy preference, effectively addresses the identified concerns related to the Privacy Paradox and privacy studies regarding an individual's privacy calculus. It does so by forcing the participant to choose between two proposed and realistic scenarios forcing them to balance the risks versus benefits and make a choice. This represents a significant contribution to the existing literature on IoT Privacy Valuation.

The Variable Nature of Privacy Valuation and its impact on Privacy Research Design

Another important issue to take into consideration regarding our research design is whether more privacy will always be perceived positively to a survey respondent. While there is general consensus that legislation to improve privacy standards should be put into place [5], there are instances where increased privacy benefits neither the individual nor society and that there is a benefit to the social welfare of privacy differentiation in the IoT [31]. As previously noted, increased privacy results in increased costs [12]. These costs have to be weighed against benefits to the individual and society in securing personal information.

From the perspective of the individual, providing access to their personal information can allow for targeted and relevant marketing, thereby increasing their access to relevant information and saving them time and money [54]. Disclosing private information may also provide more convenience in daily transactional activities and increase individual health by allowing healthcare providers to use private information to make accurate and proactive diagnoses [55].

From a societal perspective, there are several reasons why increased privacy is not necessarily preferable. The first involves security. With global terrorism, the ability for security agencies to skim the public's personal data and proactively identify potential threats is becoming of increasing importance. Second, there are economic reasons couched in information asymmetries due to increased privacy, which may lead to an inefficient redistribution of wealth [56]. For example, health insurance companies that are not aware of preexisting medical conditions, might provide a lower rate to one individual but increased rates overall to cover the distributed risk. Another example is vendors that sell an individual something on credit not realizing that the person is in imminent risk of bankruptcy and therefore losing their money. Other authors have argued that the free flow of individual credit data allows the efficient allocation of credit among borrowers [57].

In sum, the privacy calculus that an individual will undertake to determine a privacy preference will be highly contextual [20, 30] as their privacy concerns are influenced by increased perceived benefits (both societal and personal) of providing personal information in specific contexts [58]. This was recognized in earlier models of privacy concern, such as Internet users' information privacy concerns, IUIPC [28]. We extend on this analysis by not only taking into account the type of private information in our research design, but by also considering the context of the IoT use cases in a combination of scenarios constructed so that in some cases more personal benefit is generated from the disclosure of private information provided.

Previous attempts at Privacy Valuation and their impact on future Privacy Research Design

As we aim to understand various influences that lead to a different *Privacy Valuation,* it is important to consider previous studies that have attempted to assign a monetary value to privacy. If a value is to be placed on privacy, some unit of measure is required to quantify that value. In general terms, we wish to derive a marginal rate of substitution (MRS), which will indicate the extent to which some intrusion on privacy can be compensated by some other outcome. The most commonly used form of MRS in the privacy literature is WTP, which is the amount of money that an individual would pay to acquire a certain privacy state. Some authors [59] have suggested that monetary valuations of privacy are of interest because they inform businesses about whether to invest in privacy features, inform the legal profession about the extent to which individuals value privacy, and help policy makers make decisions about the trade-off between privacy and other goals. Furthermore, monetary valuations provide a standardized measure of privacy that can be compared between studies, in a way that other privacy measures cannot.

Any quantitative analysis of IoT privacy preference requires a methodology to elicit and measure those preferences. The diversity of measurements that have been used by researchers poses a challenge to the interpretation of results across various studies [51]. One approach has been to elicit privacy-related attitudes and beliefs. For example, it has been shown that attitudes, values, and beliefs around privacy vary by the type of organization a person works for [60]. A limitation of this approach is that attitudes may not translate to actions. Another stream of privacy research focuses on privacy-related behaviors. For example, one group of researchers [51] investigated if survey participants would disclose personal information in the context of a credit check by a bank. They captured two types of disclosure choice: stated preferences and actual choices. By comparing counts of the number of pieces of information revealed, they concluded that peoples' actual preference was to provide more personal information than their stated preference. While this study usefully demonstrates the privacy paradox, the methodology used is not informative about how people value the privacy of specific types of information, or about the intensity with which they value keeping this information private. This highlights the benefits of using monetary valuations of privacy based on transactions.

Often, individuals do not make choices about specific pieces of information in isolation, but instead choose products or offerings that contain a mix of features, some of which may be privacy related. Some authors [59] have noted that decisions about privacy are mostly made as part of larger economic transactions. In their study, privacy preference is inferred through the choice of gift cards, which differ in the value of the card, and the requirement to provide a name to redeem the card. The choice is made about which gift card to accept – the cheaper card that may be perceived to compromise privacy, or the more expensive card that can be used anonymously. From the choices of individuals who are performing a privacy calculus, the analyst can infer the extent to which they value privacy. In this case, this study shows that the monetary value attached to privacy depends on the context of the transaction.

Previous research [58] has utilized an experimental approach called CA to calculate people's WTP for certain privacy features in relation to websites. In the study, subjects were presented with a set of alternatives, each described by attributes, where each attribute can assume a certain level, which generates a certain amount of (dis)utility. The website alternatives were categorized by three privacy related attributes: secondary use of data, improper access to data, and the ability to review personal information for mistakes. Two further attributes represented compensating positive features: a monetary reward and time savings. Test subjects were asked to rank 18 alternatives, with these rankings being used as the dependent variable in an ANOVA analysis to estimate the utility coefficients. Participants assigned a *Privacy Valuation* of between $7.98 USD and $16.58 USD to improve each of the three privacy attributes. This study demonstrated a more complex privacy calculus than previous research [59], with multiple privacy and benefit dimensions typical of a real world privacy choice context. While CA is similar to the DCE methods employed in this research, there are certain advantages of DCE over CA, which we will explore in the Methodology section of this paper.

Some authors [59] have highlighted the importance of distinguishing between WTP and WTA. The WTP/WTA distinction requires the presence of a status quo. In the context of privacy, the status quo may be if privacy has already been compromised, WTP is the amount of money that an individual is prepared to pay to reduce an existing privacy violation, and WTA is the amount of monetary compensation that an individual requires to allow some intrusion on their privacy. These researchers [59] endowed study participants with one of the two gift card types and found that WTP to improve privacy from a more compromised privacy state was less than the amount of money subjects were prepared to accept to allow privacy to deteriorate from a more private state. Therefore, it is important to be cognizant of the WTP/WTA distinction in our analysis.

Proposed Contributions to the Existing Literature

In summarizing the preceding literature review, we identify several potential contributions to existing research on IoT privacy that our study will make, a number of which is derived from the use of DCE techniques. These are:

1) The use of analysis techniques (DCE) that are grounded in theory and have sound econometric properties;
2) The ability to assign a monetary valuation (WTP/WTA) to IoT privacy preference; and

3) The establishment of privacy preference through consequential choices of products as opposed to relying on declared preference, which is more rigorous and addresses issues related to the Privacy Paradox.

In addition to these contributions we also:

4) Explore further the contexts under which perceived benefits may influence privacy preference in the IoT;
5) Explore further the degree to which information type affects privacy preference in the IoT; and
6) Explore further the degree to which personal characteristics or covariates affect IoT Privacy Preference.

Research Design

Our previous discussion indicated that the need for privacy is challenged within an IoT environment. This is because of the increased amount of data that connected devices generate, and the fact that these devices do not inherently provide the same security and privacy as traditional IT or the Internet has. To study this, we designed a realistic DCE, utilizing the scenario of the purchase of a fitness tracker, to test people's willingness to use IoT services and products even when their privacy was knowingly compromised by the providers of those services and products. The structure of the experiment offers a way to quantify people's willingness to disclose various types of private information. The DCE further allows us to examine what contributes to *Privacy Concern* and therefore *Privacy Valuation,* specifically related to concern over privacy of the body, personal behavior, and personal data.

In designing our experiment, we developed a series of *Privacy Preference* hypothesis for the IoT, which are based on our consideration of the literature and the perceived differences between traditional Internet and the new IoT. We posit how these differences may impact *Privacy Preference* and therefore *Privacy Valuation,* and we categorize our hypothesis into a number of specific areas of investigation, specifically:

1. The Valuation of Privacy in an IoT context,
2. The impact of specific contexts and how private data is used on *Privacy Preference and Privacy Valuation* in IoT,
3. The types of private information and how this impacts *Privacy Preference* and *Privacy Valuation* in IoT, and finally
4. Who is providing the Private Data and how this affects their *Privacy Preference* and *Privacy Valuation* in the IoT?

These categories of investigation are illustrated in our conceptual model of privacy concern and privacy valuation in an IoT-based Consumer Privacy Choice Process shown in Figure 2. They represent influences on the *Privacy Concerns* described in the previously presented model in Figure 1, which would impact the *Privacy Calculus* and therefore *Privacy Preference,* and result in specific *Privacy Valuations* for the different types of information given the specific contexts presented. These Privacy Valuations are demonstrated through the choice of IoT device that the survey respondent makes. We construct a number of hypotheses related to these influences, which we present in subsequent sections:

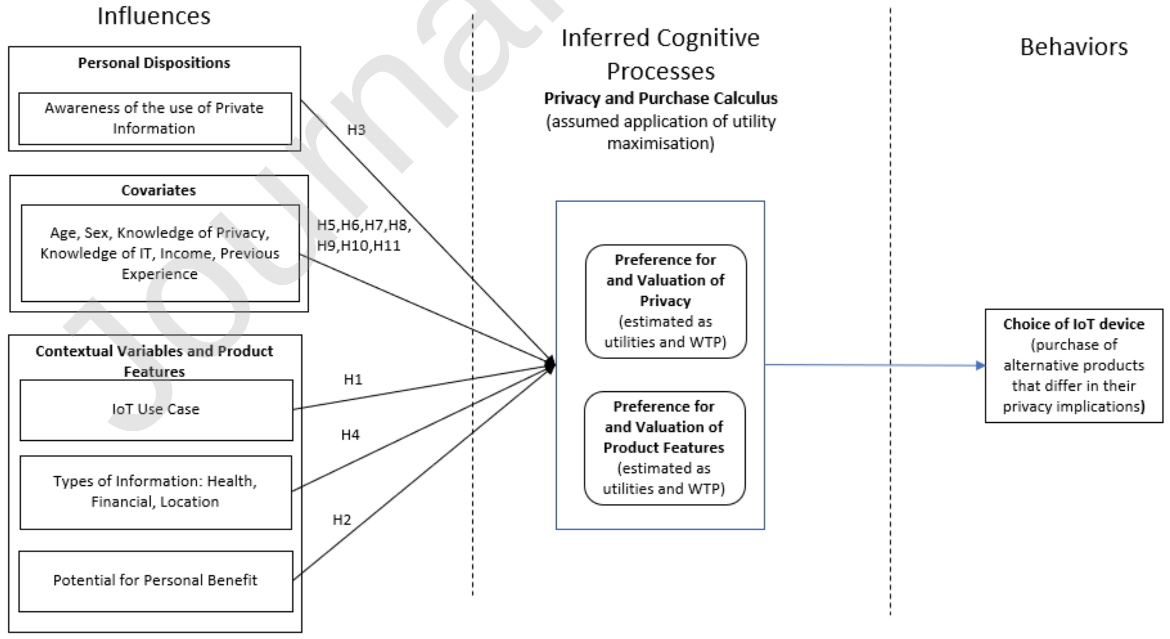

Influences
Personal Dispositions
Awareness of the use of Private Information
Covariates
Age, Sex, Knowledge of Privacy, Knowledge of IT, Income, Previous Experience
Contextual Variables and Product Features
IoT Use Case
Types of Information: Health, Financial, Location
Potential for Personal Benefit
H3
H5,H6,H7,H8, H9,H10,H11
H1
H4
H2
Inferred Cognitive Processes
Privacy and Purchase Calculus
(assumed application of utility maximisation)
Preference for and Valuation of Privacy (estimated as utilities and WTP)
Preference for and Valuation of Product Features (estimated as utilities and WTP)
Behaviors
Choice of IoT device (purchase of alternative products that differ in their privacy implications)

Figure 2: The Relationship between Influences and Behaviors in an IoT-based Consumer Privacy Choice Process including our Hypothesis about those Influences and Behaviors.

The Value of Privacy in an IoT context

The first hypothesis we put forth involves an assessment of the monetary value people assign to privacy in an IoT environment. This is the amount of money they were willing to accept for providing basic private information. Recent privacy studies have demonstrated valuations for private information as low as $2 [59] and $7 [61]. Recent studies on IoT privacy preference have struggled to demonstrate a statistically significant effect of privacy on the purchase decision for an IoT product [18]. This leads to the following hypotheses:

> *Hypothesis 1: That the monetary valuation people place on privacy in the IoT will not be statistically different to zero.*

The impact of specific contexts and how private data is used on Privacy Preference and Privacy Valuation in the IoT

A number of studies have established that privacy is contextual [51, 53, 62]. When asked to reveal a specific set of information, people's response will depend on the context in which the question is asked, who is receiving the information, and the person's understanding of how data will be used and for what purpose. When people are uncertain about their preferences, they often search for cues in their environment to provide guidance and inform their behavior. Previous research has also shown that the reasoning as to why IoT data are being solicited will impact IoT privacy preference [61]. If providing data generate benefit for the individual, they will value their privacy less than if it is being used by other parties or society as a whole. We therefore posit that context and how data will be used will impact privacy preference and valuation in the IoT.

> *Hypothesis 2: The monetary value people place on privacy in an IoT context depends on their determination of the personal benefit they will gain from disclosing private information. Increased personal benefit will reduce the preference for more privacy preference, and thus its monetary valuation in the IoT.*

In addition, consistent with previous literature on IoT privacy preference, which "underlines the need for technology to support the awareness of data collection" [19], we posit that awareness of the use of private information will have a significant impact on privacy preference and the monetary value one assigns to privacy:

> *Hypothesis 3: The ability to monitor how one's private information is being used will reduce privacy preference and decrease the monetary value one assigns to their privacy within an IoT context.*

Information Type and how this impacts Privacy Preference and Privacy Valuation in the IoT

It has been demonstrated that different types of information have different perceptions in terms of sensitivity and that sensitivity of the information has an impact on privacy preference and willing to disclose the information [28]. As the IoT may impact the availability of different types of private information differently, and that these types of information have different sensitivities, we posit that there will be different privacy preferences and privacy valuations for the different types of private information:

> *Hypothesis 4: The monetary value people place on privacy within an IoT context will vary depending on the type of private information being considered.*

Who is providing Private Data and how this affects their Privacy Preference and Privacy Valuation in the IoT?

As privacy preference can be impacted by various individual factors, we consider a number of these factors that previous studies have indicated impact privacy preference and examine whether they will have the same impact under the IoT.

First, previous research has demonstrated that those respondents that have been exposed to a recent privacy breach will have differing *Privacy Preference* from the general population [63]. We posit that this effect will continue under the IoT:

> *Hypothesis 5: Exposure to a recent personal privacy breach negatively impacts a person's willingness to accept the disclosure of private data and increases their monetary valuation of privacy within an IoT context.*

Our second hypothesis related to personal factors is driven by research, [4] which indicated that exposure to media regarding privacy breaches may impact a person's privacy preference. We therefore posit that exposure to recent news articles on privacy may also have an impact on privacy preference under the IoT:

> *Hypothesis 6: Exposure to recent news about high profile privacy breaches will negatively impact a person's willingness to accept the disclosure of their private data and increase their monetary valuation of privacy in an IoT context.*

The next set of hypotheses considers the impact of age on privacy preference and valuation. Some authors [64] have suggested that age has an impact on privacy behavior and that the younger people will have lower privacy preference and valuation than older people. In their study, they found that there was no statistically significant difference in the stated privacy preference of people from different age categories. They therefore posited that "a gap in privacy knowledge provides one explanation for the apparent license with which the young behave online" [64]. Conversely others [65] have argued that younger people have a higher privacy preference based on their more frequent manipulation of their privacy settings on social network sites. The question to ask is does more frequent adjustment of one's privacy settings equate to a preference for more privacy in general or simply a preference for a more tailored approach to privacy based on context. This would be consistent with the findings of the IoT literature on privacy [19, 20]. Consistent with this view that privacy preference and valuation is contextual not age-based, we posit that age will not have an impact on privacy preference in an IoT context:

> *Hypothesis 7: Age does not have an impact on a person's privacy preference or the monetary valuation of privacy in an IoT context.*

Also consistent with previous literature [64] on privacy preference we believe that the knowledge of privacy regulations does have an impact on privacy preference and valuation:

> *Hypothesis 8: Knowledge of privacy laws and regulation does have an impact on a person's privacy preference increasing the monetary valuation of privacy in an IoT context.*

Previous research has also identified a positive relationship between income and privacy preference with increasing income and wealth leading to more preference for privacy [22, 61]. We posit that income and wealth may have an impact on respondents' privacy preference, with those that have more money (and therefore more to lose) having a stronger preference for privacy:

> *Hypothesis 9: Increasing income and personal wealth have a positive impact on a person's privacy preference and the valuation of privacy in an IoT context.*

Some researchers have proposed that the knowledge of IT may have a positive impact on *Privacy Preference* [66], and have claimed that the knowledge of technical issues may make people more sensitive to the potential for hacking and misuse of data. This leads us to our next hypothesis:

> *Hypothesis 10: Knowledge of information technology has the impact of increasing a person's privacy preference and their monetary valuation of privacy under the IoT.*

Previous studies have also demonstrated an impact of gender on privacy preference with women typically preferring more privacy [61, 67, 68] because of the fact that they have a greater fear of being the victims of aggression of crime [67]. Implicit in these discussions is a linkage between physical security and privacy. We expect privacy preference and privacy valuation for women will increase under the IoT as the IoT provide more information particularly around physical location. This leads us to our last hypothesis:

Hypothesis 11: A person's gender has an impact on a person's privacy preference and the monetary valuation of privacy under the IoT with women having higher privacy preference.

Methodology

In this section, we outline the various components of the methodology we used for our study. We begin by detailing the DCE method, comparing it to the closest methodology, CA, and noting its econometric and behavioral advantages. We then outline the design of our survey, and explain how it addresses our hypotheses. This is followed by an outline of our data collection techniques.

The use of Discrete Choice Experimental Techniques

In this paper, we measure *Privacy Valuation* using a DCE, which is underpinned by the estimation of discrete choice models. DCEs have been used to investigate choice behavior in a wide range of literatures, including an extensive history in transportation [69] environmental and resource economics [70], health economics [71], and tourism [72].

DCE differs from methods outlined in our literature review on *Privacy Valuation*, but bears the most similarity to CA. In practice, there is often ambiguity about the differences between DCEs and CA [73]. A common element is the recognition that the utility of an alternative is the sum of the utilities associated with the attributes that describe the alternative [44]. Both approaches are experimental in nature, use stated preference data, and present subjects with a set of alternatives for consideration, although the discrete choice models used with DCEs can also be used with revealed preference data.

What differs is the response mechanism, and the models estimated, with CA using rankings or ratings, and DCEs using choices. With CA, the rank of alternative i is generated as a direct function of the utility expression, as

$Ranking_i = \alpha + \beta' X_i + \varepsilon_i,$

where α is a constant, β' is a vector of estimated utility coefficients, and X is a vector of variables including attribute levels. There is no reason why the utility expression should consistently generate integer rankings, and so an error term ε is used to handle this disparity.

With DCEs by contrast, the utility U of alternative i for individual n on choice occasion t is not measured directly, but treated as a latent construct, expressed as

$$U_{nit} = \alpha_i + \beta' X_{nit} + \varepsilon_{nit},$$

where α_i is an alternative specific constant, β' is a vector of estimated utility coefficients, and X_{nit} is a vector of attribute levels and potentially also interactions between attribute levels and individual characteristics, allowing individual differences in utility based on observed characteristics to be directly tested. DCEs typically present each respondent with multiple 'choice tasks,' hence subscript t. Collectively, $\beta' X_{nit}$ is referred to as the systematic component of utility. The random component of utility, ε_{it}, captures unidentified influences on choice, as well as differences across individuals that cannot be explained by the systematic component of utility. If we assume that ε_{it} is distributed Extreme Value Type 1, it can be shown that the probability P_{nit} of individual n choosing alternative i in a choice set of J alternatives is

$$P_{nit} = \frac{e^{\alpha_i + \beta' X_{nit}}}{\sum_{j=1}^{J} e^{\alpha_j + \beta' X_{njt}}}.$$

The random component of utility plays an important behavioral role in the model, as when the magnitudes of the utility coefficients increase relative to the variance of ε_{ni}, the choices will become more deterministically explained by the utility coefficients, and behavior will be less random. Indeed, DCEs are consistent with an underlying behavioral theory, Random Utility Theory (RUT), in a way that CA is not [74]. The underlying models are thus informed by a coherent theory, rather than being driven by model fit. Ordered logit and probit models are also based on RUT, and thus have a sound behavioral underpinning [75]; however, ranking has a heavy cognitive burden, which can result in inconsistencies in the ranking task and excess noise in the resulting models. Thus, the DCE literature has generally advocated obtaining multiple best choices instead of rankings of a single set of alternatives [74]. For these reasons, we advocate the use of DCEs for the elicitation of privacy preference when dealing with complex privacy calculi, such as choosing IoT devices. The choice response naturally aligns with the purchase of an IoT device, which is the point at which the individual starts to bear the privacy consequences of their decision. Furthermore, the representation of the IoT device as a bundle of privacy-related and other features allows privacy to be measured as a tradeoff with other features.

As with CA, the DCE approach can readily calculate MRS between the attributes investigated, including WTP and WTA measures. Consider the WTA attribute k, through compensation in cost attribute c:

$$WTA_k = \frac{\frac{\partial}{\partial_k}\beta_k x_k}{\frac{\partial}{\partial_c}\beta_c x_c} = \frac{\beta_k}{\beta_c}.$$

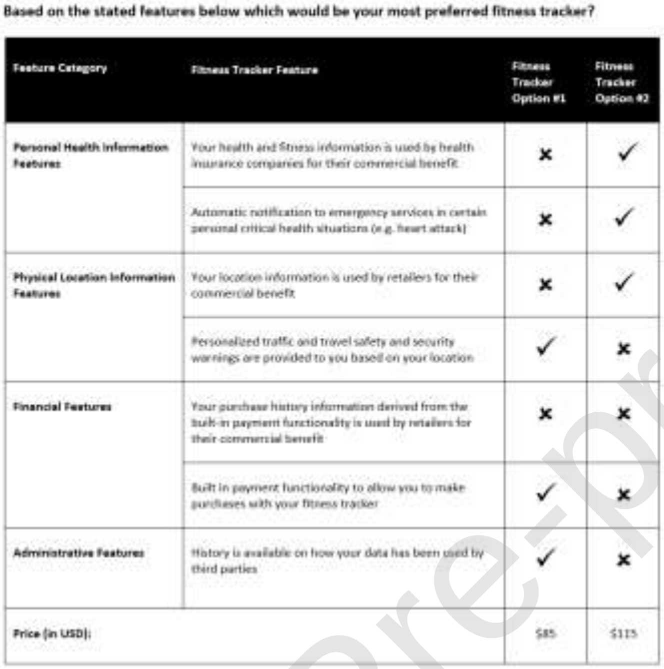
Standard errors can be calculated for this WTA function using the Delta method. In this paper, we will report the significance of both the utility coefficients, and the WTA/WTP measures.

A Discrete Choice Experiment for IoT privacy

As mentioned previously, we measure *IoT Privacy Preference* and *IoT Privacy Valuation* by asking survey respondents to participate in a realistic IoT privacy scenario, which was the choice between two different options in terms of the purchase of a fitness tracker with each option having a different combination of features. In these scenarios the dependent variable is the choice of IoT device, and from this we use the choice model to infer the WTA or WTP. It is then the WTA that we test for statistical significance. The independent variables are the features of the fitness tracker, each chosen for their perceived privacy impact.

Our survey participants were screened to only include respondents who indicated an interest to purchase a fitness tracker in the near future helping to ensure that they had some understanding of what a fitness tracker was. To set a common baseline for all hypothetical fitness trackers presented to respondents, all trackers were described as a small wrist band, which can track heart rate, number of steps taken, body temperature, and physical location through a built-in global positioning system. The trackers also fully integrate with smart phones through Bluetooth to sync with calendars and contacts. A sequence of choice tasks then described those attributes that varied across devices and asked respondents to make a choice between the two fitness trackers.

Figure 3 shows an example choice task. Respondents had to choose their most preferred of the two alternatives, which were referred to as fitness tracker options. Each alternative was described by seven features (excluding the price).



Based on the stated features below which would be your most preferred fitness tracker?

Feature Category	**Fitness Tracker Feature**	**Fitness Tracker Option #1**	**Fitness Tracker Option #2**
Personal Health Information Features	Your health and fitness information is used by health insurance companies for their commercial benefit	✗	✓
	Automatic notification to emergency services in certain personal critical health situations (e.g. heart attack)	✗	✓
Physical Location Information Features	Your location information is used by retailers for their commercial benefit	✗	✓
	Personalized traffic and travel safety and security warnings are provided to you based on your location	✓	✗
Financial Features	Your purchase history information derived from the built-in payment functionality is used by retailers for their commercial benefit	✗	✗
	Built in payment functionality to allow you to make purchases with your fitness tracker	✓	✗
Administrative Features	History is available on how your data has been used by third parties	✓	✗
Price (in USD):		$85	$115

Figure 3: Example Choice Task

The first seven features were grouped into four categories: ‘personal health information,’ ‘physical location information,’ ‘financial,’ and ‘administrative.’ Each of the first three categories has two features, each of which is either present or absent. The first feature per category, which we will call “commercial benefit features,” involves the sharing of information with businesses for their commercial benefit. None of the categories indicate whether respondents would obtain a personal benefit from their information being shared. The second feature in each category (“personal benefit features”) may generate personal benefit, but requires sharing private information gathered by the fitness tracker. This allowed for the analysis of the role that personal benefit would play in the privacy calculus the individual undertook.

To facilitate the monetary valuation of the privacy-related attributes, an eighth feature was included, the price that the respondents would need to pay for the fitness tracker with the remaining seven features. The possible price levels were $85, $100, $115, $130, and $145. Whether the monetary valuations are WTA or WTP measures will depend on the status quo for the consumer seeking to purchase an IoT device. Given the respondent is purchasing the device, we assume that the health, physical location, and financial information is not currently being shared with businesses. Consequently, the sharing of this information will represent a loss of privacy for the respondent, who will need to be compensated for this loss through a reduced price. Thus, we report WTA for the commercial benefit features. We further assume that the respondent does not currently have access to the personal benefit features, and so the associated monetary valuations are measures of their WTP for this product feature[1]. However, as the personal benefit features also require the sharing of information, privacy concerns may reduce the WTP.

The significance of the commercial benefit features informs us about H1. The significance of the personal benefit features would suggest that personal benefit can offset any associated privacy concerns, in support of H2. To ascertain whether privacy preference varies across the types of privacy (H4), we created features that directly affect privacy of the person's body (first category), behavior (second category), and personal data (third category).

A single-feature administrative category provides history on how data have been used by third parties. This is used to test if the potential secondary use of the data has an impact on privacy preference and valuation (H3). In this scenario, visibility of secondary use is equated to awareness and control over that secondary use by the respondent as they can choose not to use the fitness tracker.

We tested hypotheses 5 through 11 by relying on additional questions in the survey, which were presented after the choice tasks, listed in Table 1 below. Responses were in some cases recoded, based on a model specification search. For example, the recency of the privacy breach was found to be insignificant, and this was entered into the model as a binary variable representing whether there was any prior breach, regardless of when that breach occurred. Responses were analyzed for interaction with the commercial benefit attributes, allowing the WTA to be decomposed based on characteristics of respondents, or on their experience.

[1] We acknowledge that the endowment effect can influence monetary valuations [76] and argue that the appropriate measure is based on each individual's privacy and purchase circumstance.

Those hypotheses that directly related to privacy knowledge or experience (H5, H6, H8, and H10) were also analyzed to see the effect on WTP for personal benefit features. It was not possible to evaluate the interaction of the sociodemographic responses (H7, H9, and H11) with personal benefit features, as it would not be possible to determine if differences in utility are due to differing preferences for the personal gain of the features, or differing degrees of privacy concern.

Hypotheses 5-11 were also tested for each of health, location, and financial privacy, to determine if the hypotheses can only be accepted for certain types of privacy. Only significant interactions were retained in the reported models.

In total the complete experimental design contained 20 unique choice tasks, split into two blocks of 10. To obtain more information per respondent, each respondent was assigned to a block and completed 10 choice tasks. They were then asked the supplementary questions listed in Table 1. An efficient design was generated in the Ngene software package [76] to maximize the information gain, with Bayesian priors used to account for uncertainty [77]. Some 400 respondents were targeted to ensure adequate variation in sociodemographic characteristics, with 411 respondents recruited. Two multinomial logit (MNL) models were then estimated. The first only included the attributes as explanatory variables and was used to test hypotheses from 1 to 4. The second model additionally included various interactions between attributes and the supplementary questions, and tested hypotheses from 5 to 11. All models were estimated with the Nlogit software package, which is a commercially available software package used for this type of analysis.

Data collection

Participants were crowd sourced from Mechanical Turk an online panel. The viability of using Mechanical Turk as a tool for crowdsourcing respondents for social science research has been demonstrated in the academic literature [78]. There has also been specific research on the efficacy of Mechanical Turk for privacy studies [66]. This research has demonstrated that compared to other sample providers, the MTurkers' "greater knowledge of technical issues may make them more sensitive to the potential for hacking and misuse of online data," and therefore generate a more conservative result when calculating disutility over lost privacy and the WTA for privacy loss [66]. Mechanical Turk has other advantages as a tool for social science research. Given the large pool of *MTurkers,* it is easy to source survey respondents quickly from a broad base. The tool also allows responses to be collected anonymously, while preventing the same anonymous respondent from completing the same survey twice.

To ensure data quality, we applied several filters prior to completing the survey. These included a CAPTCHA question to guarantee the survey was not being completed by a Robot. The design of the Mechanical Turk survey also prevented a person with the same login ID from answering the same survey twice. Also, respondents were restricted to those workers who had greater than a 90% approval rate for tasks they had previously completed on MTurk, which helped to ensure that the respondents participating would provide a quality response. Respondents who had not completed the last question in our survey, where they needed to enter a five-digit number were also excluded from our analysis.

A number of filters were also applied, such as postsurvey completion and preanalysis, to ensure the quality of the results. Participants were asked a simple logical question: "Whilst watching the television, have you ever suffered a fatal heart attack?" Respondents that provided a response other than "Never" were excluded from analysis. Also, respondents that took less than two minutes to complete the survey were filtered from the survey results assessing that they had not taken sufficient time to read and understand the questions asked. As a prerequisite to taking the survey was that respondents had to have the intention to purchase a fitness tracker in the near future (and therefore have a basic understanding of the technology), anyone who answered that they had no intention of purchasing a fitness tracker were filtered out. After applying those filters, 352 respondents (sufficient to obtain statistically significant results) were remaining upon whom we based our analysis.

Previous studies have shown that Mechanical Turk Workers demographically are generally representative of the population as a whole [79]. The demographics of our Mechanical Turk sample set were consistent with that view in that both respondent age and income were well-distributed; geographically the respondents were drawn from across the greater United States of America and were 48.86% male and 50.85% female.

Results

MNL Model without Interactions

The first MNL model, used to test Hypotheses 1-4, does not include any interactions, and is reported in Table 2. In addition to absolute values, WTA and WTP measures are reported as a percentage of the average cost of the fitness trackers in the experiment, to provide some context for these figures. All utility coefficients bar one are significant at a 99% confidence level. All three personal benefit features have significant, positive utility coefficients. The WTP measures for these features are also significant, ranging from $33.53 for built-in payment functionality, to $44.62 for personalized location-based personalized traffic, and travel safety and security warnings, to $99.78 for automatic notification to emergency services. The utility coefficients for the commercial benefit features are negative and significant in two feature categories. The two associated WTA measures are also significant, with the use of health information by insurance companies requiring $38.66 in compensation, and the use of location information by retailers requiring $30.79 in compensation. By comparison, the utility of commercial use of financial information by retailers is not statistically significantly different from zero, and a significant monetary valuation cannot be generated, demonstrating a degree of indifference as to how one's personal financial information is being used.

In these results, we observe a pattern across feature categories, with personal health information category having the greatest monetary valuations for both personal and commercial benefit features, the financial category having the lowest monetary valuations for both (including indifference to commercial use of financial information), and the physical location category lying in between. The personal health and physical location categories are both contingent on the IoT, whereas the financial category is not. We posit that the higher valuation for the former two categories is due in part to the novelty of these factors. While financial information has been transmitted frequently over the Internet for years, the idea that someone can be physically tracked at all times and that their health information may be collected and used by service providers is relatively new. Our conclusion is that those forms of privacy more negatively impacted by the IoT generate higher levels of privacy concern, but that the overall level of privacy concern in the IoT is statistically significant.

> ***Reject*** *Hypothesis 1: That the monetary valuation people place on privacy in the IoT will not be statistically different to zero.*

Personal benefit also appears to bear an influence on the privacy calculus. All personal benefit features generated positive utility, and thus individuals are prepared to pay a premium for the features, despite the privacy compromises they entail. Thus we

> ***Failed to Reject*** *Hypothesis 2: The monetary value people place on privacy in an IoT context depends on their determination of the personal benefit they will gain from disclosing private information. Increased personal benefit will reduce the preference for more privacy preference and thus its monetary valuation in the IoT.*

The utility coefficient for "History is available to you on how your data have been used by third parties" was positive and significant to the 99% level. The valuation of this information was $21.15 USD and significant to the 95% level. In this context, we interpret awareness of how private IoT information is being used as a form of control over their data, and therefore an important factor in the individuals IoT privacy calculus:

> ***Failed to Reject*** *Hypothesis 3: The ability to monitor how ones private information is being used will reduce privacy preference and decrease the monetary value one assigns to their privacy within an IoT context.*

The differences in sensitivity to aggregate commercial benefit features across the feature categories are supportive of H4. Personal health and physical location have WTA measures of $38.66 and $30.79 respectively, and both measures are significantly different from WTA the financial features (p=0.013 and p=0.027). Conversely, personal health and physical location WTA measures are not significantly different to each other (p=0.377). However, once we disaggregate the monetary valuations using interactions in our second model reported below, we will see that differences between personal health and physical location privacy will exist for people of certain age, gender, and privacy breach history. It could be argued that the sensitivity of individuals to their data being used for commercial benefit might vary depending on the commercial entity receiving the data. In the choice experiment, health information was shared with insurance companies, while physical location and financial information was shared with retailers. That the WTA differed between physical location and financial information, despite this information being shared with the same commercial entity, suggests that the differences are due to different types of privacy, not just different recipients of the data. Overall, we

> ***Failed to Reject*** *Hypothesis 4: The monetary value people place on privacy within an IoT context will vary depending on the type of private information being considered.*

Extended MNL Model with Interactions

The second MNL model, reported in Table 3, is the consequence of the model specification search process described earlier, which tested all the individual factors listed in Table 1. Table 3 reports the utility coefficients for both the main effects for each product feature, and all significant interactions. For any given feature, a unique WTA or WTP can be generated for each combination of significant interaction responses[2], and these values are reported in Table 4. When testing the hypotheses that rely on the interactions, we will report two p–values. The first reports the significance of the utility coefficient. The second reports the significance of the marginal contribution of the interaction term to the WTA/WTP, and is more conservative as it includes the variance associated with the cost parameter. We retain all interactions for which p<0.1 for the utility coefficients.

[2] Consider the WTP for the administrative feature. For individuals without privacy knowledge, WTP = -1*(0.3537+0x-0.2558)/-0.0061 = $57.88, and for individuals with privacy knowledge, WTP = -1*(0.3537+1x-0.2558)/-0.0061 = $16.02. The values reported here are rounded, with the WTP values calculated from the precise estimated coefficients.

First we consider the personal factors related to previous exposure to privacy issues. Exposure to recent media on privacy breach had no statistically significant impact on privacy preference. In contrast, personal exposure to privacy breach has a significant impact across all of the health and location features. Respondents with a privacy breach history were more sensitive to commercial use of health, with an additional WTA of $51.41 (p=0.000; p=0.016). For example, 55- to 64-year-old male respondents without a privacy breach history need to be compensated $39.85 for the health commercial benefit feature, but this increases to $91.26 for the same demographic who has had a privacy breach at some point in the past. Likewise, those with a privacy breach history are more sensitive to commercial use of their location, with an additional WTA of $30.17 (p=0.009; p=0.051). For example, male respondents without a history are not sensitive at all to this use (with an insignificant WTP of $1.53), but those with a history have a WTA of $28.63. Health personal gain (notification to emergency services) is reduced by $23.14 (although only with marginal significance: p=0.059; 0.110), from $110.48 to $87.34 for all respondents, and location personal gain is reduced by $29.17, from $60.06 to $30.89 for all respondents (p=0.015; p=0.061). This strongly suggests that these individuals are more concerned about the privacy implications of these features that otherwise bring personal gain. No statistically significant impact on financial information privacy preference was found because of personal privacy breach or exposure to privacy media. What becomes clear from this analysis is that for there to be an impact on privacy preference, the experience with privacy issues needs to be personal with the individual having had their own privacy breach and that simple media exposure is not sufficient. In summary:

> ***Failed to Reject*** *Hypothesis 5: Exposure to a recent personal privacy breach negatively impacts a person's willingness to accept the disclosure of private data and increases their monetary valuation of privacy within an IoT context*
>
> *… and …*
>
> ***Reject*** *Hypothesis 6: Exposure to recent news about high-profile privacy breaches will negatively impact a person's willingness to accept the disclosure*

> *of their private data and increase their monetary valuation of privacy in an IoT context.*

The next series of personal factors we consider are self-reported knowledge of IT and privacy regulation. The question here being would knowledge and education impact a person's privacy preference and WTA the disclosure of private IoT-based information. Our analysis here indicates limited impact on privacy preference. We find the only effect being self-reported knowledge of privacy law and regulation moderating a person's desire to understand how their private information is being used, with WTP reduced for the history feature, from $57.88 to $16.02 (p=0.019; p=0.065). The specific causal factors for this are unclear but perhaps may be due to respondents experienced in privacy regulation considering these controls either ineffective or unnecessary. In summary, it is concluded that there is no clear relationship between IT and privacy regulation knowledge and privacy preference in general. We therefore:

> ***Failed to Reject (Partially)*** *Hypothesis 8: Knowledge of privacy laws and regulation does have an impact on a person's privacy preference increasing the monetary valuation of privacy in an IoT context.*
>
> *… and …*
>
> ***Reject*** *Hypothesis 10: Knowledge of information technology has the impact of increasing a person's privacy preference and their monetary valuation of privacy under the IoT.*

The final series of personal factors that we consider as part of the Extended MNL Model are demographic factors such as age, sex, and personal income and health. Contrary to previous research there appears to be no relationship between income, wealth, and personal privacy preference in this fitness tracker IoT context. As predicted by the literature [64], in terms of age the only relationship that was significant was related to health information, with WTA for the health commercial benefit feature increasing by $1.92 for each additional year of age (p=0.000; p=0.022). For example, for female respondents with no privacy breach history, WTA increases from $45.79 for 21 year old to $139.62 for 70 year old respondents. We posit that the effect here is due to a personal benefits calculus in the most elderly of respondents, which considers the disclosure of private health information related to their bodies as potentially damaging financially (i.e., higher health insurance premiums).

As also predicted by the literature [61, 67, 68], there is a linkage between privacy preference and gender, with men having a lower WTA in all categories as compared to women. This is particularly true for those two factors, such as health and location information, which are more directly linked to the IoT. Men clearly have lower privacy preference for commercial use of health and location information. The health commercial benefit feature WTA is $29.21 lower for male than female respondents (p=0.011; p=0.049), with, for example, 70 year old respondents with a privacy breach history having a WTA of $110.41 if they are male, versus $139.62 if they are female respondents. The location commercial benefit feature WTA is $27.65 lower for male than female (p=0.015; p=0.056) respondents. For those with a privacy breach history, the WTA is $28.63 if they are male and $56.28 if they are female. In conclusion we:

> ***Reject (Partially)*** *Hypothesis 7: Age does not have an impact on a person's privacy preference or the monetary valuation of privacy in an IoT context.*
>
> *…and…*
>
> ***Reject*** *Hypothesis 9: Increasing income and personal wealth have a positive impact on a person's privacy preference and monetary valuation of privacy in an IoT context.*
>
> *…and…*

Failed to Reject *Hypothesis 11: A person's gender has an impact on a person's privacy preference and the monetary valuation of privacy under the IoT with women having higher privacy preference.*

Discussion

Implications for Theory

Having presented and discussed our results, we now consider their implications for Privacy Theory in the IoT. Our analysis shows that context plays a heavy role in an individual's privacy calculus, privacy preference, and privacy valuation. This is consistent with the previous theory on IoT Privacy [19, 20].

What our research also indicates is that the type of privacy concern and personal factors play a significant part in a person's privacy calculus, privacy preference, and privacy valuation. This suggests that other studies that do not vary on the type of privacy information or investigate differences based on sociodemographic, experience, and knowledge may average out a much more nuanced distribution of privacy valuation.

There is also a clear difference in those types of private information, which are more significantly impacted by newer technologies like the IoT; whereas those types of private information which are not novel to the IoT are less impacted. We posit then that as those forms of technology become more broadly used and gain some form of cognitive legitimacy that privacy concern and the resultant privacy preference will likely decrease [80, 81]. However, any decrease in concern might be offset by high levels of privacy breaches, which we have shown increases privacy valuation.

Implications for Practice

There are three main implications for practice that could be concluded from our study. First is that the WTA a reduction in privacy for the various IoT scenarios ranged in value from as low as $30.79 USD per person for individuals to provide their location data to as high as $139.62 USD per person for individuals in certain demographics to provide their health information. This indicates that process, procedures, and technology, which cost an organization more than these amounts, may be inappropriate and need to be reconsidered. In this context, there is a "right amount of privacy" depending on the type of information, the context, and the individual in question. Treating everyone equally in terms of privacy is not necessarily the best strategy.

The second conclusion is that because the WTA varies significantly based on the type of private information, practitioners are well advised to adjust the level of process, procedures, and technology used to ensure privacy based on the type of private information being captured. Otherwise, they may either be offering too much or too little privacy. In other words, a "one solution fits all" approach does not apply to privacy concern. Just how much effort should be expended to ensure privacy will depend on the type of information, and so it may be advisable to conduct studies such as the one herein to determine sensitivity to specific information types before the deployment of an IoT-based solution.

The third implication from this research is that the degree to which individuals are aware of how their private information is being used will impact their privacy preference and associated privacy valuation. This means that organizations may optimize their privacy processes, procedures, and technologies by ensuring full and complete disclosure of how the private information they collect may be used.

Limitations

The use of DCE methods, realistic choice scenarios, and a broader data set means that the statistical results are robust and nuanced. However, this study has relied on the standard DCE assumption that the choice process is compensatory. This implies that the privacy calculus is itself compensatory, and trade-offs can and will be made between privacy and other features. Other possibilities that could be modeled with appropriate extensions to the choice models are the elimination of devices from consideration that have certain levels of privacy intrusion [82] and complete indifference to privacy by segments of the population [83]. There is also the question of the generalizability of the study findings outside of the consumer products vertical in IoT.

Future Research Opportunities

We posited that as these technologies are more broadly used that they gain some form of cognitive legitimacy and that privacy preference decreases. It would be useful therefore to prove out this notion by conducting research into the legitimation process of adopting the IoT and how this impacts privacy preference. One way would be to conduct a longitudinal study over time of how individuals value the various types of privacy concern in various contexts understanding whether privacy concern decreases over time as these technologies gain cognitive legitimacy [80].

Further cross-sectional studies across a number of different IoT scenarios in different industries within the different types of privacy concern would also be useful. This would prove out the generalizability of the initial findings in our study to other IoT verticals.

Modeling alternative privacy calculi would provide insight into the extent to which privacy can be traded away.

Finally, we identified a focus on individual factors that may influence privacy concern and therefore privacy valuation. It would be of interest to attempt a study, which looked to understand institutional factors which affect privacy. These institutional factors could include (but are not necessarily limited to) the medium of communication used as indicated in the Social Presence Theory [84] or the degree of information disclosure reciprocity as indicated in the Social Response Theory [85].

Conclusions

The IoT now enables certain forms of private information (e.g., location and health) to be more readily collected than before. As a result, these new forms of information collection experience a higher sensitivity to privacy concern on the part of the individual. In part, this is due to the novelty of the data collection process and in part due to a perceived lack of cognitive legitimacy about that same process. Therefore, individuals will exhibit a higher preference for privacy in these cases, and will be willing to pay more to address their privacy concerns in these contexts. We also conclude that the degree to which individuals have awareness of how their private information is used will moderate that privacy preference and valuation within the IoT but that the perceived benefits from control are in turn moderated by the knowledge of privacy regulations.

What is important to consider through all of this is that the valuations that people assign to privacy are low and heavily affected by the personal benefit that disclosing this private information provides. This reinforces the view that more privacy is not always better and that in some cases the costs of additional regulation regarding privacy outweigh the benefits and the actual desire on the part of the individual to "pay" for that regulation. The overall conclusion is that privacy legislation to enforce more privacy does need to be judicious and specific to the use cases for the private information in question and the types of private information involved.

Author Statement

David Goad: Conceptualization, Methodology, Investigation, Formal Analysis, Data Curation, Writing – Original Draft, Visualization. **Andrew Collins:** Methodology, Software, Formal Analysis, Validation, Writing – Review and Editing, Visualization. **Uri Gal:** Writing – Review and Editing

References

1. Tully, F., Lheureux, Geschlickter, Hung, *Internet of Things Primer.* Gartner Research, 2016.
2. Solove, D.J., *Conceptualizing privacy.* Cal. L. Rev., 2002. **90**: p. 1087.
3. Westin, A.F. and O.M. Ruebhausen, *Privacy and freedom*. Vol. 1. 1967: Atheneum New York.
4. Madden, M. and R. Lee, *American's Attitudes about Privacy, Security and Surveillance*, in *Pew Research Centre*, M. Dugan, Editor. 2015.
5. EMC, *The EMC Privacy Index: Global and In-Depth Country Results*. 2014.
6. BBVA, *Internet of Things: Connected Home*, Leer, Editor. 2015.
7. McIntyre, A., B. Blau, and M. Reitz, *Forecast: Wearable Electronic Devices Worldwide*, in *Gartner Research*. 2016.
8. Zuboff, S., *Big other: surveillance capitalism and the prospects of an information civilization.* Journal of Information Technology, 2015. **30**(1): p. 75-89.

9. Heudecker, N.H., Jim, *Survey Analysis: Big Data Investments Begin Tapering in 2016.* Gartner Research, 2016.

10. Pache, C. and B. Taney. *Complaince with Notifiable Data Breaches Scheme* 2018; Available from: https://www.australasianlawyer.com.au/sections/features/compliance-with-the-notifiable-data-breaches-scheme-246600.aspx.

11. Goodman, B. and S. Flaxman, *European Union regulations on algorithmic decision-making and a" right to explanation".* arXiv preprint arXiv:1606.08813, 2016.

12. Willemsem, B., S. Matthew, and T. Ayol, *Predicts 2017: Privacy Becomes a Necessity with Opportunity.* Gartner Research, 2016.

13. Ponemon, *The True Cost of Compliance: A Benchmark Study of Multinational Organizations*, in *Ponemon Institute*, P. Institute, Editor. 2011.

14. Christensen, L.R. and F. Etro, *European data protection: Impact of the EU data-protection regulation*, in *Vox EU*. 2013.

15. Hung, M., A. Singh, and D. Mahdi, *Hardware Security and its Impact on IoT Projects.* Gartner Research, 2016.

16. Hung, M., A. Singh, and D.A. Mahdi, *Hardware Security and Its Impact on IoT Projects.* Gartner Research, 2016.

17. Acquisti, A., C.R. Taylor, and L. Wagman, *The economics of privacy.* Available at SSRN 2580411, 2016.

18. Hsu, C.-L. and J.C.-C. Lin, *An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives.* Computers in Human Behavior, 2016. **62**: p. 516-527.

19. Naeini, P.E., et al. *Privacy expectations and preferences in an IoT world*. in *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 2017.

20. Lee, H. and A. Kobsa. *Understanding user privacy in Internet of Things environments*. in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. 2016. IEEE.

21. Kim, D., et al., *Willingness to provide personal information: Perspective of privacy calculus in IoT services.* Computers in Human Behavior, 2019. **92**: p. 273-281.

22. Acquisti, A. and J. Grossklags, *Privacy and rationality in individual decision making.* IEEE security & privacy, 2005. **3**(1): p. 26-33.

23. Jensen, C., C. Potts, and C. Jensen, *Privacy practices of Internet users: self-reports versus observed behavior.* International Journal of Human-Computer Studies, 2005. **63**(1-2): p. 203-227.

24. Connelly, K., A. Khalil, and Y. Liu. *Do I do what I say?: Observed versus stated privacy preferences*. in *IFIP Conference on Human-Computer Interaction*. 2007. Springer.

25. Louviere, J.J., D.A. Hensher, and J.D. Swait, *Stated choice methods: analysis and applications*. 2000: Cambridge University Press.

26. Street, D.J. and L. Burgess, *The construction of optimal stated choice experiments: Theory and methods*. Vol. 647. 2007: John Wiley & Sons.

27. Smith, H.J., S.J. Milberg, and S.J. Burke, *Information privacy: measuring individuals' concerns about organizational practices.* MIS quarterly, 1996: p. 167-196.

28. Malhotra, N.K., S.S. Kim, and J. Agarwal, *Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model.* Information systems research, 2004. **15**(4): p. 336-355.

29. Train, K.E., *Discrete choice methods with simulation*. 2009: Cambridge university press.

30. Chow, R., et al. *HCI in Business: A collaboration with academia in IoT privacy*. in *International Conference on HCI in Business*. 2015. Springer.

31. Zhou, W. and S. Piramuthu, *Information relevance model of customized privacy for IoT.* Journal of business ethics, 2015. **131**(1): p. 19-30.

32. Lau, J., B. Zimmerman, and F. Schaub, *Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers.* Proceedings of the ACM on Human-Computer Interaction, 2018. **2**(CSCW): p. 102.

33. Apthorpe, N., et al., *Discovering smart home internet of things privacy norms using contextual integrity.* Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2018. **2**(2): p. 59.

34. Zheng, S., et al., *User perceptions of smart home IoT privacy.* Proceedings of the ACM on Human-Computer Interaction, 2018. **2**(CSCW): p. 200.

35. Kisekka, V. and J.S. Giboney, *The effectiveness of health care information technologies: evaluation of trust, security beliefs, and privacy as determinants of health care outcomes.* Journal of medical Internet research, 2018. **20**(4): p. e107.

36. Emami Naeini, P., et al., *The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios.* Proceedings of the ACM on Human-Computer Interaction, 2018. **2**(CSCW): p. 48.

37. Katz, M.L. and C. Shapiro, *Network externalities, competition, and compatibility.* American economic review, 1985. **75**(3): p. 424-440.

38. Yang, Y., et al., *A survey on security and privacy issues in Internet-of-Things.* IEEE Internet of Things Journal, 2017. **4**(5): p. 1250-1258.

39. Zhou, W. and S. Piramuthu. *Security/privacy of wearable fitness tracking IoT devices*. in *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*. 2014. IEEE.

40. Bahirat, P., et al. *A data-driven approach to developing iot privacy-setting interfaces*. in *23rd International Conference on Intelligent User Interfaces*. 2018. ACM.

41. Caron, X., et al., *The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective.* Computer Law & Security Review, 2016. **32**(1): p. 4-15.

42. Li, Y., *Theories in online information privacy research: A critical review and an integrated framework.* Decision Support Systems, 2012. **54**(1): p. 471-481.

43. Lichtenstein, S. and P. Slovic, *The construction of preference*. 2006: Cambridge University Press.

44. Lancaster, K.J., *A new approach to consumer theory.* Journal of political economy, 1966. **74**(2): p. 132-157.

45. Rosen, S., *Hedonic prices and implicit markets: product differentiation in pure competition.* Journal of political economy, 1974. **82**(1): p. 34-55.

46. McFadden, D., *Conditional logit analysis of qualitative choice behavior.* Frontiers in Econometrics, 1973.

47. Rogers, R.W., *A protection motivation theory of fear appeals and attitude change1.* The journal of psychology, 1975. **91**(1): p. 93-114.

48. Petronio, S., *Communication boundary management: A theoretical model of managing disclosure of private information between marital couples.* Communication Theory, 1991. **1**(4): p. 311-335.

49. Bandura, A., *Social cognitive theory: An agentic perspective.* Annual review of psychology, 2001. **52**(1): p. 1-26.

50. Junglas, I.A., N.A. Johnson, and C. Spitzmüller, *Personality traits and concern for privacy: an empirical study in the context of location-based services.* European Journal of Information Systems, 2008. **17**(4): p. 387-402.

51. Norberg, P.A., D.R. Horne, and D.A. Horne, *The privacy paradox: Personal information disclosure intentions versus behaviors.* Journal of Consumer Affairs, 2007. **41**(1): p. 100-126.

52. Pötzsch, S. *Privacy awareness: A means to solve the privacy paradox?* in *IFIP Summer School on the Future of Identity in the Information Society*. 2008. Springer.

53. Kokolakis, S., *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon.* Computers & Security, 2017. **64**: p. 122-134.

54. Deighton, J.A. and R.C. Blattberg, *Interactive marketing: Exploiting the age of addressability.* Sloan management review, 1991. **33**(1): p. 5-14.

55. Page, R. *Your Health E-Wallet.* Choice 2017 [cited 2018 15 Oct 2018]; Available from: https://www.choice.com.au/electronics-and-technology/internet/using-online-services/articles/ehealth-records-online.

56. Posner, R.A., *The economics of privacy.* The American economic review, 1981. **71**(2): p. 405-409.

57. Rubin, P.H. and T.M. Lenard, *Privacy and the commercial use of personal information*. 2002: Springer Science & Business Media.

58. Hann, I.-H., et al., *Overcoming online information privacy concerns: An information-processing theory approach.* Journal of Management Information Systems, 2007. **24**(2): p. 13-42.

59. Acquisti, A., L.K. John, and G. Loewenstein, *What is privacy worth?* The Journal of Legal Studies, 2013. **42**(2): p. 249-274.

60. Stone, E.F., et al., *A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations.* Journal of applied psychology, 1983. **68**(3): p. 459.

61. Carrascal, J.P., et al. *Your browsing behavior for a big mac: Economics of personal information online*. in *Proceedings of the 22nd international conference on World Wide Web*. 2013. ACM.

62. Acquisti, A., L. Brandimarte, and G. Loewenstein, *Privacy and human behavior in the age of information.* Science, 2015. **347**(6221): p. 509-514.

63. Cho, H., J.-S. Lee, and S. Chung, *Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience.* Computers in Human Behavior, 2010. **26**(5): p. 987-995.

64. Hoofnagle, C.J., et al., *How different are young adults from older adults when it comes to information privacy attitudes and policies?* 2010.

65. Blank, G., G. Bolsover, and E. Dubois, *A New Privacy Paradox.* 2014.

66. Schnorf, S., et al. *A comparison of six sample providers regarding online privacy benchmarks*. in *SOUPS Workshop on Privacy Personas and Segmentation*. 2014.

67. Moscardelli, D.M. and R. Divine, *Adolescents' concern for privacy when using the Internet: An empirical analysis of predictors and relationships with privacy‐ protecting behaviors.* Family and Consumer Sciences Research Journal, 2007. **35**(3): p. 232-252.

68. Fogel, J. and E. Nehmad, *Internet social network communities: Risk taking, trust, and privacy concerns.* Computers in human behavior, 2009. **25**(1): p. 153-160.

69. Hensher, D.A., *Stated preference analysis of travel choices: the state of practice.* Transportation, 1994. **21**(2): p. 107-133.

70. Hoyos, D., *The state of the art of environmental valuation with discrete choice experiments.* Ecological economics, 2010. **69**(8): p. 1595-1603.

71. de Bekker‐ Grob, E.W., M. Ryan, and K. Gerard, *Discrete choice experiments in health economics: a review of the literature.* Health economics, 2012. **21**(2): p. 145-172.

72. Huybers, T., *Domestic tourism destination choices—a choice modelling analysis.* International Journal of Tourism Research, 2003. **5**(6): p. 445-459.

73. Carson, R.T. and J.J. Louviere, *A common nomenclature for stated preference elicitation approaches.* Environmental and Resource Economics, 2011. **49**(4): p. 539-559.

74. Louviere, J.J., T.N. Flynn, and R.T. Carson, *Discrete choice experiments are not conjoint analysis.* Journal of Choice Modelling, 2010. **3**(3): p. 57-72.

75. Greene, W.H. and D.A. Hensher, *Modeling ordered choices: A primer*. 2010: Cambridge University Press.

76. ChoiceMetrics, *Ngene 1.2 User Manual & Reference Guide.* 2018.

77. Sandor, Z. and M. Wedel, *Designing conjoint choice experiments using managers' prior beliefs.* Journal of Marketing Research, 2001. **38**(4): p. 430-444.

78. Mason, W. and S. Suri, *Conducting behavioral research on Amazon's Mechanical Turk.* Behavior research methods, 2012. **44**(1): p. 1-23.

79. Stewart, N., C. UngeMach, and A. Harris, *The Average Population of Mechanical Turn Workers.* 2015.

80. Binz, C., et al., *The Thorny Road to Technology Legitimation—Institutional Work for Potable Water Reuse in California.* Technological Forecasting & Social Change, 2016. **103**: p. 249.

81. Johnson, C., T.J. Dowd, and C.L. Ridgeway, *Legitimacy as a social process.* Annu. Rev. Sociol., 2006. **32**: p. 53-78.

82. Koo, T.T., et al., *How Safety Risk Information and Alternative Forms of Presenting It Affect Traveler Decision Rules in International Flight Choice.* Journal of Travel Research, 2018: p. 0047287518759228.

83. Campbell, D., W.G. Hutchinson, and R. Scarpa, *Incorporating discontinuous preferences into the analysis of discrete choice experiments.* Environmental and resource economics, 2008. **41**(3): p. 401-417.

84. Rice, R.E., *Media appropriateness: Using social presence theory to compare traditional and new organizational media.* Human communication research, 1993. **19**(4): p. 451-484.

85. Moon, Y., *Intimate exchanges: Using computers to elicit self-disclosure from consumers.* Journal of consumer research, 2000. **26**(4): p. 323-339.

Primary Author

David Goad, Postgraduate Fellow, Business Information Systems, Sydney University

David is a Postgraduate Fellow at the University of Sydney where he researches the Internet of Things and Artificial Intelligence. He teaches Digital Business Management, Technology and Innovation Management at the University of Sydney and the University of New South Wales. David has degrees in Engineering and Business and has over 20 years of industry and academic experience. He actively advises large enterprises on their IT, AI and IoT strategies.

David has a number of previously published academic articles including articles on the Internet of Things and Algorithmic Decision Making/ Artificial Intelligence.

Second Author:

Andrew Collins, Senior Lecturer, Logistics and Supply Chain Management, Sydney University

Andrew studied computer science and philosophy at the University of NSW, obtaining a Bachelor of Science/Bachelor of Arts with first class honours in 2003. He was awarded a PhD in 2012, for a thesis which proposed and evaluated new techniques for handling attribute non-attendance in discrete choice models. For this research Andrew was awarded the prestigious Eric Pas Dissertation Prize by the International Association for Travel Behaviour Research.

Andrew has broad research interests, with a particular focus on the behavioural influences of decision makers in the fields of logistics, supply chain management, and transport. He also has methodological research interests, in the areas of discrete choice modelling, choice heuristics, and stated choice experimental design. His publication record includes top tier journals such as Transportation Research Parts B and E, and Transportation. He has published over 30 Journal articles including several articles on the topic of Discrete Choice Experiments.

Andrew enjoys teaching discrete choice methods to a diverse audience. He teaches these techniques to PhD students in BUSS7904 Advanced Quantitative Methods. Additionally, each July, he runs a Discrete Choice Analysis five day course, attracting academics, PhD students, consultants and government employees from a wide range of disciplines, including marketing, health economics, environmental economics, and transportation.

Third Author:

Uri Gal, Associate Professor, Director of Doctoral Studies, Business Information Systems, Sydney University

Uri is the Director of Doctoral Studies for the University of Sydney Business School. Uri joined the University of Sydney in July 2010 from Copenhagen Business School in Denmark, where he had been Assistant Professor at the Centre for Applied Information and Communication Technology. He received his Ph.D. in Information Systems from Case Western Reserve University, USA.

Uri's research takes a social view of organisational processes in the context of the implementation and use of information systems. He is particularly interested in the relationships between people and technology in organisations, and the changes in the nature of work practices, organisational identities, and interactions associated with the introduction of new information systems.

Uri has published a number of academic articles including articles on the Internet of Things, Algorithmic Decision Making/ Artificial Intelligence and People Analytics and Big Data.

Table 1: Supplementary questions used to test hypotheses 5 – 11

Hypothesis	**Question**	**Responses**
5	Have you yourself ever experienced a breach of your own personal privacy?	Never, within the last 5 years, 2 years, 1 year, 6 months, and 1 month
6	How recently have you seen or heard an article in the news that talked about a breach of privacy?	Never, within the last 5 years, 2 years, 1 year, 6 months, and 1 month
7	To what age group do you belong?	18-24, 25-29, 30-34, 35-39, 40-44, 45-49, 50-54, 55-64, and 65+
8	How do you rate your knowledge of Privacy Law and the rules and regulations governing the use of your personal information?	None at all, some, knowledgeable, very knowledgeable, and expert
9	What is your current personal annual income in USD?	$0, $1 to $15,000, $15,001 to $31,000, $31,001 to $52,000, $52,001 to $78,000, $78,001 to $130,000, $130,001 or greater
10	How do you rate your knowledge of Information Technology?	None at all, some, knowledgeable, very knowledgeable, and expert
11	Please select your gender	Male, female, or other

Table 2: Base MNL model with no interactions

Feature category	Fitness tracker feature	Feature Benefit Type	Utility coefficient	Willingness to Accept Value (and % of average cost)	Willingness to Pay Value (and % of average cost)
Personal health information features	Your health and fitness information is used by insurance companies for their commercial benefit	Commercial	-0.2260***	$38.66** (33.6%)	
	Automatic notification to emergency services in certain personal critical health situations (e.g., heart attack)	Personal	0.5833***		$99.78*** (86.7%)
Physical location information features	Your location information is used by retailers for their commercial benefit	Commercial	-0.1780***	$30.79** (26.8%)	
	Personalized traffic and travel safety and security warnings are provided to you based on your location	Personal	0.2608***		$44.62*** (38.8%)
Financial features	Your purchase history information derived from the built-in payment functionality is used by retailers for their commercial benefit	Commercial	0.0677		$11.58 (10%)
	Built-in payment functionality to allow you to make purchases with your fitness tracker	Personal	0.1960***		$33.53** (29%)

Feature category	**Fitness tracker feature**	**Feature Benefit Type**	**Utility coefficient**	**Willingness to Accept Value (and % of average cost)**	**Willingness to Pay Value (and % of average cost)**
Administrative features	History is available to you on how your data have been used by third parties		0.1236***		$21.15** (18.4%)
Price			-0.0059***		

Note: Confidence levels: *** 99%, ** 95%, and *90%. The average attribute cost = $115

Table 3: MNL model with interactions

Feature category	Fitness Tracker Feature	Parameter	Utility coefficient	Related hypotheses
Personal health information features	Your health and fitness information is used by insurance companies for their commercial benefit	Main effect	0.2801**	
		x Any privacy breach history	-0.3142***	H5
		x Age in years	-0.0117***	H7
		x Male	0.1785**	H11
	Automatic notification to emergency services in certain personal critical health situations (e.g., heart attack)	Main effect	0.6751***	
		x Any privacy breach history	-0.1414*	H5
Physical location information features	Your location information is used by retailers for their commercial benefit	Main effect	-0.1596**	
		x Any privacy breach history	-0.1844***	H5
		x Male	0.1690**	H11
	Personalized traffic and travel safety and security warnings are provided based on your location	Main effect	0.3670***	
		x Any privacy breach history	-0.1783**	H5
Financial features	Your purchase history information derived from the built-in payment functionality is used by retailers for their commercial benefit	Main effect	0.0681	
	Built-in payment functionality to allow you to make purchases with your fitness tracker	Main effect	0.1993***	
Administrative features	History is available to you on how your data have been used by third parties	Main effect	0.3537***	
		x Any privacy knowledge	-0.2558**	H8
Price		Main effect	-0.0061***	

Note: Confidence levels: *** 99%, ** 95%, *90% .

Table 4: WTA/WTP decomposed by privacy breach, privacy knowledge, gender and age

Feature category	Fitness Tracker Feature	Privacy breach history (H5)	Age (H7)	Privacy knowledge (H8)	Gender (H11)	% sample	WTA (and % of Average Cost)	WTP (and % of Average Cost)
Personal health information features	Your health and fitness information is used by insurance companies for their commercial benefit	No	18-24	-	Female	4.1%		$5.62 (4.9%)
		Yes	18-24	-	Female	1.9%	$45.79** (39.8%)	
		No	18-24	-	Male	3.3%		$34.83** (30.3%)
		Yes	18-24	-	Male	3.0%	$16.58 (14.4%)	
		No	55-64	-	Female	1.4%	$69.06** (60%)	
		Yes	55-64	-	Female	1.9%	$120.47*** (105%)	
		No	55-64	-	Male	1.1%	$39.85* (34.6%)	
		Yes	55-64	-	Male	2.4%	$91.26*** (79.3%)	
	Automatic notification to emergency services in certain personal critical health situations (e.g., heart attack)	No	-	-	-	56.6%		$110.48*** (96%)
		Yes	-	-	-	43.4%		$87.34*** (75.9%)
Physical location information features	Your location information is used by retailers for their commercial benefit	No	-	-	Female	22.0%	$26.11* (22.7%)	
		Yes	-	-	Female	28.7%	$56.28** (48.9%)	
		No	-	-	Male	21.4%		$1.53 (1.3%)

Feature category	Fitness Tracker Feature	Privacy breach history (H5)	Age (H7)	Privacy knowledge (H8)	Gender (H11)	% sample	WTA (and % of Average Cost)	WTP (and % of Average Cost)
		Yes	-	-	Male	27.9%	$28.63** (24.9%)	
	Personalized traffic and travel safety and security warnings are provided to you based on your location	No	-	-	-	56.6%		$60.06*** (52.7%)
		Yes	-	-	-	43.4%		$30.89** (26.9%)
Financial features	Your purchase history information derived from the built-in payment functionality is used by retailers for their commercial benefit	-	-	-	-	100%		$11.14 (9.7%)
	Built-in payment functionality to allow you to make purchases with your fitness tracker	-	-	-	-	100%		$32.62** (28.4%)
Administrative features	History is available to you on how your data have been used by third parties	-	-	No	-	11.7%		$57.88** (50.3%)
		-	-	Yes	-	88.3%		$16.02** (13.8%)

Note: Confidence levels: *** 99%, ** 95%, *90%. The average attribute cost = $115