https://doi.org/10.48009/4_iis_2020_285-294

Issues in Information Systems
Volume 21, Issue 4, pp. 285-294, 2020

INDIVIDUAL PERCEPTIONS OF THE INTERNET OF THINGS

Kyle Ebersold, The Hartford, kyle.ebersold@gmail.com
Richard Glass, Bryant University, rglass@bryant.edu
Suhong Li, Bryant University, sli@bryant.edu

ABSTRACT

Organizations have embraced The Internet of Things (IoT) for the benefits that they derive. Acceptance among individual consumers has been slower. An understanding of individuals' perceptions of the IoT will help promote acceptance of the technology. This paper investigates individual perceptions of IoT regarding privacy, security, trust, and convenience by providing subjects with typical IoT scenarios and having them respond to questions regarding their perceptions. For less personal scenarios, convenience was most important and privacy least important. For more personal scenarios the opposite was true; privacy was most important and convenience least important.

Keywords: The Internet of Things, Privacy, Security, Trust, Convenience

INTRODUCTION

The internet of things (IoT) can be broadly defined as a global network infrastructure, linking uniquely identified physical and virtual objects, things, and devices through the exploitation of data capture (sensing), communication and actuation capabilities. A primary goal of interconnecting devices is to create situation awareness and enable applications, machines, and human users to better understand their surrounding environments and to make intelligent decisions and to respond to the dynamics of their environments [6,9].

There has been significant growth in IoT installed devices within the last few years. It is estimated that the number of IoT devices will reach 31 billion in 2020, an increase of 24 billion installed devices since 2017. The implementation of 5G technology will further boost growth to more than 75 billion devices by 2025. Global spending on IoT should reach 1.29 trillion dollars in 2020 and by 2026 the market for IoT devices alone will reach 1.1 trillion dollars [1].

A Microsoft survey of enterprise IoT decision makers found that 85% say they have at least one IoT project in either the learning, proof of concept, purchase, or use phase, with many reporting they have one or more projects currently in use. It is expected that this number will grow to 94% by the end of 2021. Responders to the survey report that compared to traditional methods, the IoT helps them streamline processes and work more efficiently. The top benefits for their organizations included: operations optimization (56%), improvement of employee productivity (47%) and safety and security (44%). In addition, 30% to 40% of enterprise companies adopt IoT to manage supply chain, assure quality, track assets, and enable sales. [2]

IoT also provides several advantages for individuals over non IoT methods [3,4]. Key advantages include:

1. Connectivity: IoT provides the ability to operate multiple things from one device.
2. Efficiency: Increased connectivity leads to a decrease in the amount of time normally spent performing tasks.
3. Convenience: IoT makes it easier and less time consuming to perform actions such as ordering items.
4. Wellness: IoT enables you to monitor your health in real time through wearable devices.
5. Conservation: Smart cities include ways to use IoT to monitor city conditions such as traffic, air quality, electric/water usage, and environmental factors.
6. Transportation: IoT will be able to provide real time updates on travel schedules, delays bookings etc. Smart cars will drive and navigate for you, protect you from harm and recommend maintenance when needed.
7. Personalization: IoT devices gather substantial amounts of information about individuals and can then make recommendations and tailor their services to your preferences.

Despite the widespread adoption of IoT by industry there remain barriers to the adoption of IoT by individual consumers. Four key issues that impact the adoption of IoT are privacy, security, trust, and convenience. The purpose of this exploratory research project is to provide individuals with scenarios that reflect issues of privacy, security, trust, and convenience and analyze their perceptions regarding IoT as is relates to the four issues.

KEY ISSUES IMPACTING USER ADOPTION OF IoT

Privacy has been identified a key factor in the adoption of new technology [8,9,10,11,19]. Privacy issues arise from the nature of the technology itself. To protect privacy, individuals should be able to provide informed consent regarding the information shared by IoT devices and the actions that these devices originate. However, the design of the IoT is predicated on the ability to use "smart" technology to make autonomous decisions and execute them in microseconds [6]. A related privacy issue is the potential for an individual to develop a feeling of loss of control over one's life that arises from the IoT's ability to transfer decisions that impact an individual's life to devices and algorithms and take action on those decision without the awareness of the individual while at the same time creating data that is largely invisible to the public. When the intentionality of delegated actions is not fully controllable by the user, this may lead to a compromise in a person's integrity and eventually that person's freedom [16]. Perceptions of security may impact a user's adoption of IOT [10,11,17]. IoT devices are wireless and are often located in public places. Current levels of encryption are inadequate given the fact that many of the IoT devices are not powerful enough to support robust encryption [18]. Hacking into physical devices and taking control of the device may lead to disastrous consequences such as taking away control of a motor vehicle [17]. Trust has been studied extensively as a precedent for new technology adoption including the adoption of IoT [5,12,13,15]. Given that the IoT is an intangible, trust in the process and outcome may allay concerns over adoption. Convenience has received significant attention in the adoption of new technology literature [10,11,13] Discussions of the IoT assume that convenience is always beneficial. There is an implicit idea that allowing things to people and things to be connected at all times will serve us better by providing greater convenience. However, convenience may not always be perceived as desirable. In the extreme, having machines make all our decisions for us may negative impact human's perceptions of self-worth [14].

METHODOLOGY

An electronic survey powered by QuestionPro was distributed to university students enrolled in an undergraduate business program at a private university in the Northeast United States. The survey instrument had been previously presented to three students as a test for ease of use and ambiguity. The questions were revised to facilitate better understanding of the questions and the time to complete the survey was reduced by approximately five minutes. The survey instrument in its distributed form is included in the Appendix.

A total of 192 usable responses were received. The profile of the respondents is summarized in Table 1. Of the sample, 63.5% were male. The majority of the respondents were between 19 and 21 years old (81.2%). About half (53.6%) were sophomores at the university. Most respondents were also domestic U.S. students (89.1%). About half of the respondents indicated a moderate level of technical expertise with computer technology (51.3%) with an additional one-third (32.3%) reporting a higher level of expertise.

Table 1: Demographic profile of the respondents

		Respondents	Percentage
Gender	Male	122	63.5%
	Female	70	36.5%
Age	18/19	79	41.1%
	20	56	29.2%
	>=21	57	29.7%
Academic Status	Freshmen	17	8.9%
	Sophomores	103	53.6%
	Juniors	31	16.1%
	Seniors	41	21.4%
Student Type	Domestic	171	89.1%
	International	21	10.9%
Level of Technical Expertise	Low	31	16.1%
	Moderate	99	51.6%
	High	62	32.3%

DATA ANALYSIS AND RESULTS

The survey administered contained six vignettes selected to represent important application of the IoT. The vignette scenarios included applications of the following:

1. A remote home management and security system accessed remotely via mobile device
2. A placed order and remote notification by a smart refrigerator performing automatic shopping for its owner
3. Remote smart grid technology coupled with a home energy management system
4. A smart car interacting in real-time with its traffic-related surroundings while on the road
5. Automated issuance and notification of a speeding ticket by a freeway speed sensor
6. Targeted contextual advertising via smartphone based on the TV show currently being watched

Respondents were asked to rank on a scale of one (1) to seven (7) their agreement with five questions corresponding to one of the four constructs: privacy, security, trust, and convenience.

Figure 1 displays the averages of the four key constructs across all six vignettes. The results indicate that the average of the respondents rating on each of the four constructs hovered around a response of four (Neither Agree Nor Disagree) on the seven-point scale. This suggests that on average respondents tended not to have extreme positions among the four constructs.

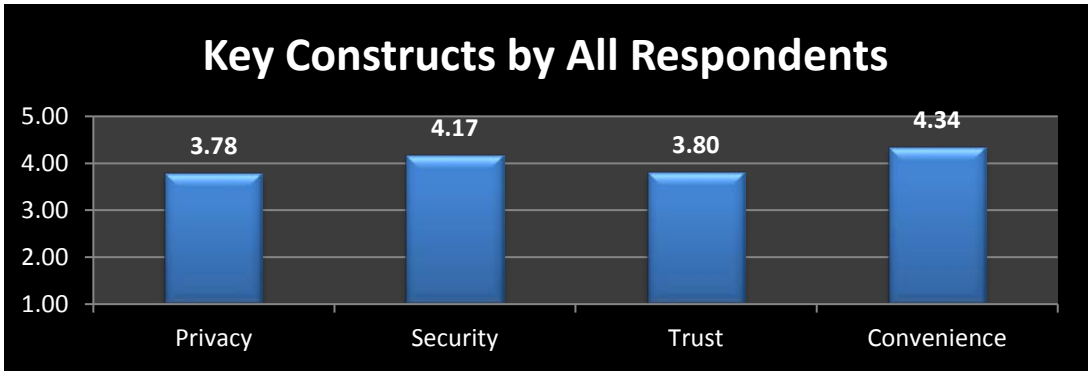

Figure 1. Key Constructs by All Respondents

When taking into consideration the individual demographic factors of gender (Figure 2), age, (Figure 3), academic status (Figure 4), student type (Figure 5), and computer technology expertise (Figure 6) the comparative means suggest that there were no observable differences within a demographic factor for each the four constructs of privacy, security, trust and convenience.

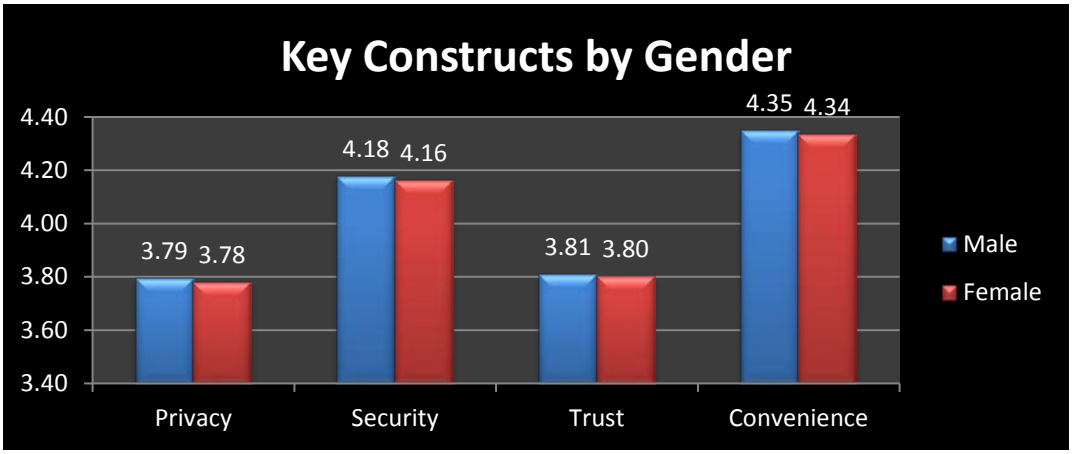

Figure 2. Key Constructs by Gender

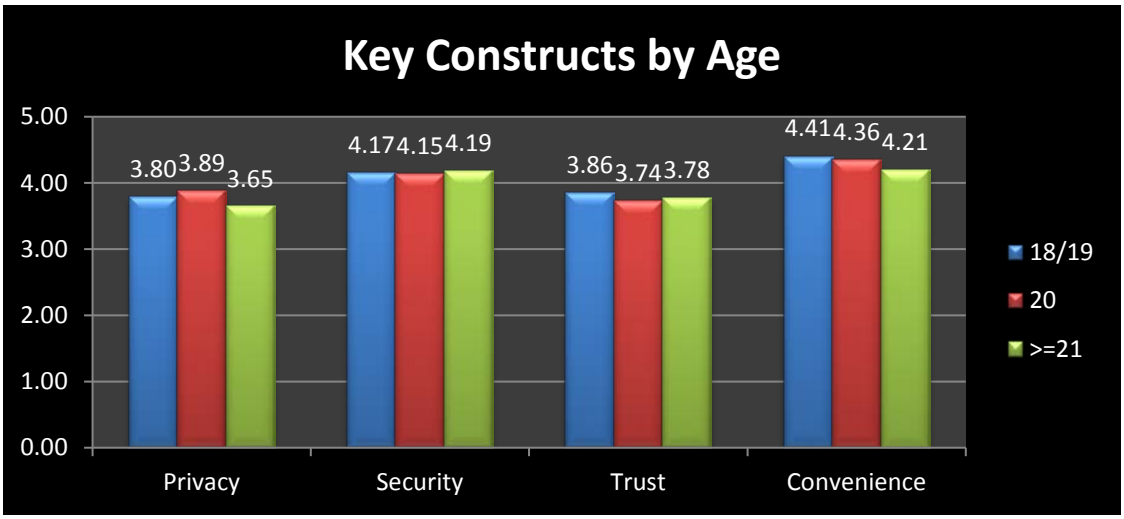

Figure 3. Key Constructs by Age

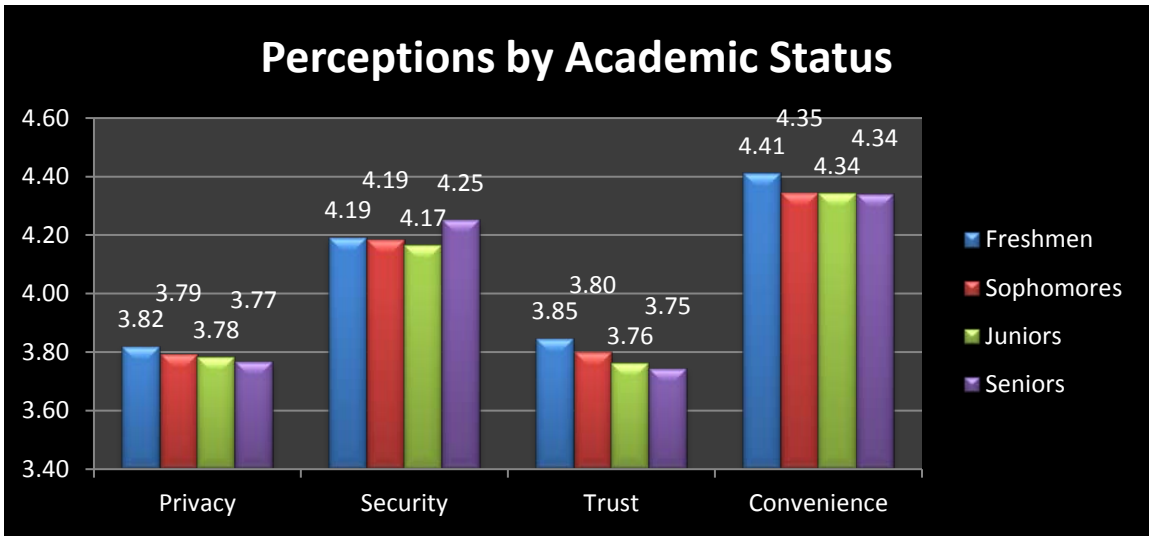

Figure 4. Perceptions by Academic Status

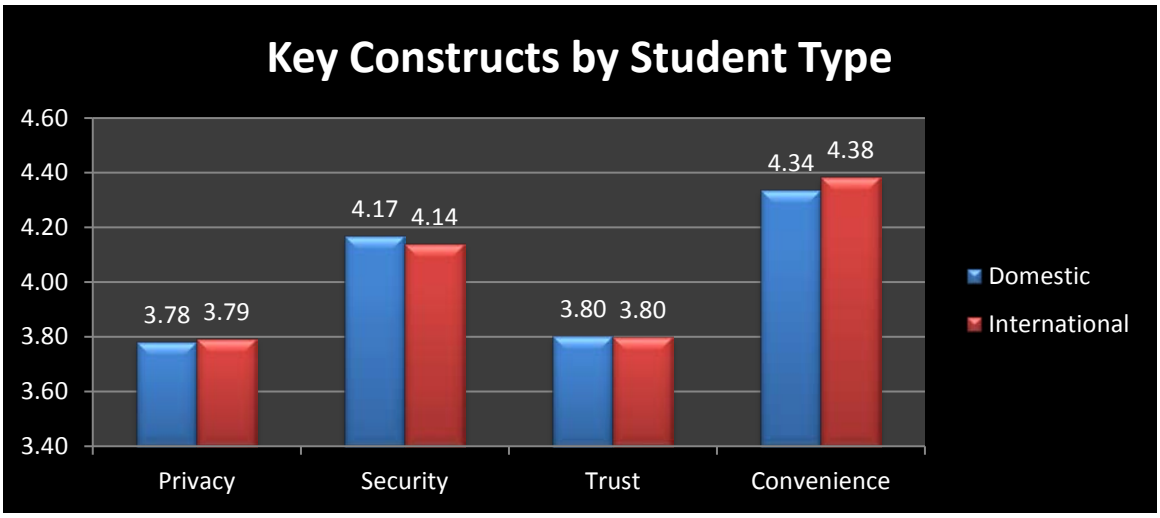

Figure 5. Key Constructs by Student Type

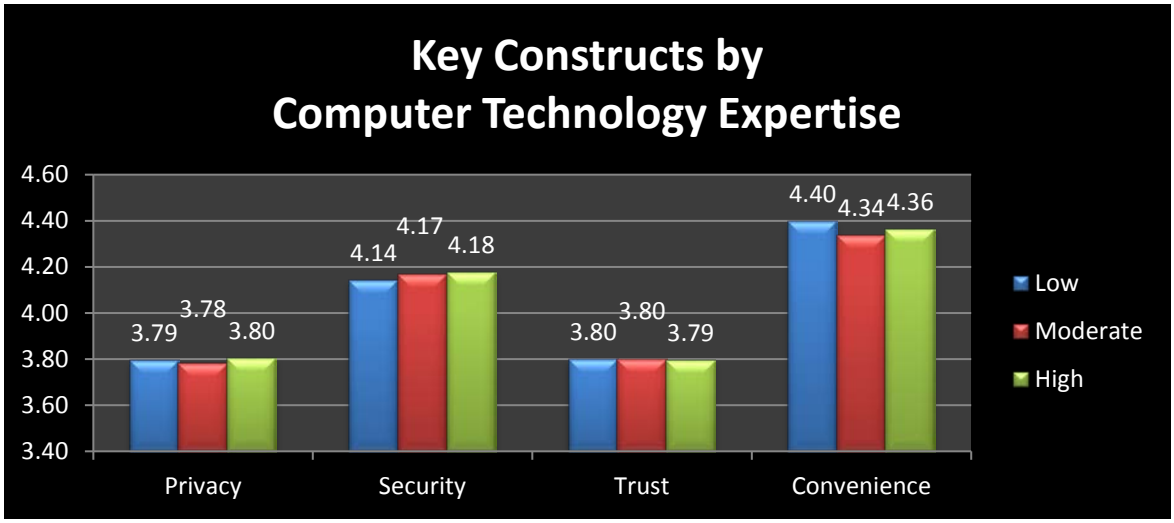

Figure 6. Key Constructs by Computer Technology Expertise

In analyzing the means across the four constructs by vignette scenario, the results indicated an inverse relationship between privacy and convenience. Furthermore, the inverse relationship changes direction dramatically for scenarios five and six compared to the first four scenarios. Privacy concerns were markedly lower compared to convenience for the first four vignettes, while the latter two scenarios saw a dynamic switch where privacy was remarkably high while convenience was relatively low. Figure 7 shows these results graphically while Table 2 displays them numerically.

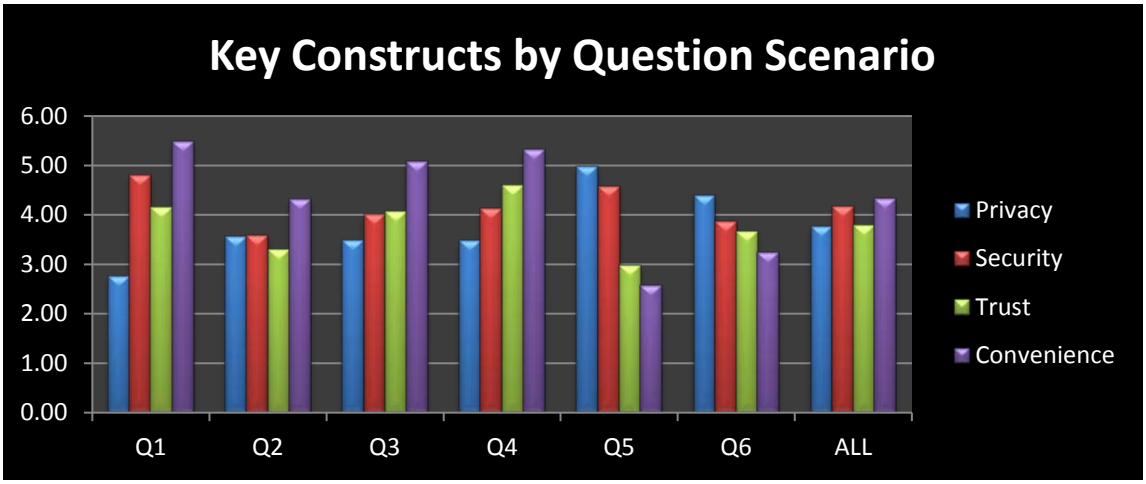

Figure 7. Key Constructs by Question Scenario

Table 2: Comparison of Means

	Privacy	Security	Trust	Convenience
Q1	2.77	4.81	4.16	5.49
Q2	3.56	3.60	3.31	4.32
Q3	3.49	4.02	4.07	5.08
Q4	3.48	4.13	4.60	5.32
Q5	4.98	4.58	2.99	2.57
Q6	4.41	3.86	3.68	3.23
ALL	3.78	4.17	3.80	4.34

Additionally, Table 3 shows the results of one-way ANOVA between each scenario by construct. As expected, due to the different kinds of constructs investigated in the differing types of vignettes posed, the large majority of the questions asked were found to be significant.

Table 3: Results of One-Way ANOVA between Individual Question Items

	Privacy	Security	Trust	Convenience
Q1 - Q2	0.000	0.000	0.000	0.000
Q1 - Q3	0.000	0.000	0.462	0.002
Q1 - Q4	0.000	0.000	0.001	0.195
Q1 - Q5	0.000	0.123	0.000	0.000
Q1 - Q7	0.000	0.000	0.002	0.000
Q2 - Q3	0.590	0.001	0.000	0.000
Q2 - Q4	0.610	0.000	0.000	0.000
Q2 - Q5	0.000	0.000	0.060	0.060
Q2 - Q7	0.010	0.089	0.018	0.018
Q3 - Q4	0.967	0.391	0.000	0.000
Q3 - Q5	0.000	0.000	0.000	0.000
Q3 - Q7	0.000	0.250	0.007	0.007
Q4 - Q5	0.000	0.001	0.000	0.000
Q4 - Q7	0.000	0.053	0.000	0.000
Q5 - Q7	0.000	0.000	0.000	0.000

(Highlighted results are significant at the .05 level)

DISCUSSION AND IMPLICATIONS

An exploratory study was conducted to investigate university students' perceptions of the IoT. Four constructs were considered including privacy, security, trust and convenience. Previous research has identified these four constructs as major issues for the effective adoption of the IoT. College students were selected for the survey because they will be entering the workforce just as applications of the IoT become more readily available. Student perceptions of IoT after graduation will be important for successful adoption.

Students were most concerned about convenience of the technology (m=4.34) followed by security issues (m=4.17), trust (m=3.80) and privacy (m=3.78). In general, the mean responses of all students varied between 3.78 and 4.34 with standard deviations for each individual question that did not exceed 1.8. This suggests that student perceptions on average were not extreme. The fact that students do not have strong opinions about the IoT with respect to privacy, security, trust and convenience may be the result of their being unfamiliar with the IoT and the likelihood that they do not have personal experience using the technology due to its relative immaturity.

The largest difference was between privacy and convenience. Convenience would appear to be a more important factor for students than privacy concerns. At face value, this result may be expected for this age group; however, there was a very interesting and notable relationship between these two constructs. Privacy concerns have the lowest means and convenience concerns have the highest means for the first four scenarios. However, for the last two scenarios the two constructs reverse the relationship with privacy having the highest mean and convenience having the lowest for the last two scenarios. This is a striking reversal in student perceptions. This result appears to be related to the type of scenarios that the students were presented with. The first four scenarios deal with situations that appear to be less personal than the last two. These four scenarios have the IoT perform a service that efficiently manages familiar functions and reduces the effort of the individual to manage these functions. For example, scenario one describes how an IoT application can automatically manage a home security system and control heating; scenario two automatically checks your groceries and reorders them; scenario three monitors your energy expenditures at home and efficiently controls them; and scenario four has the IoT reduce your time stuck in traffic. The last two scenarios are of a much more personal nature. In scenario five, the IoT monitors your individual driving patterns and automatically issues you a ticket for speeding. This scenario is perceived to be more of a privacy concern than all others. The last scenario has the IoT monitoring your individual television viewing patterns and sending ads for new products to your smartphone that are specifically targeted to your profile.

The fact that students perceive these scenarios differently with respect to privacy has strong implications for the potential adoption of the IoT. While other applications of such technology may prove more convenient and offer less overall concern for privacy, IoT applications on a highly personal level of contact may not be as well-received by people. This is an important finding for IoT architects, businesses, and government especially as it demands a need for limitation in the degrees of invasiveness and informed consent required by the public. Vendors will have to focus their marketing of IoT applications differently depending on how directly the IoT application is perceived by the individual to affect them at a personal level. The scenario with the IoT application issuing a ticket has many similarities to the video systems installed at traffic lights that capture video of automobiles going through red lights and issuing tickets. While it may be argued that these systems improve safety and earn money for cash strapped cities, many cities have removed these systems based on widespread complaints by the public.

Another interesting finding of this research was that there appears to be very little difference among student perceptions across different demographic characteristics. Mean responses for each of the 4 constructs did not vary by academic status (freshman, sophomore, junior, senior), student type (domestic, international) or by the degree of expertise with computer technology. This may be because students are not aware of the IoT or may be related to the fact that the sample was fairly homogeneous. This finding warrants future research to determine whether the results may be replicated. If, in fact, perceptions across demographics are similar, then this may facilitate the acceptance of the IoT among this group by enabling vendors to create a campaign with a uniform message.

One finding that did demonstrate a difference was the fact that concerns for privacy differed by the age of the respondent. Students in the 21 or older group tended to view privacy as less of an issue. Given that there was little difference by age for security, trust, and convenience this result may be an aberration of the data. Further research may explore whether this finding is significant. If so, it may imply that as students reach the age of graduation and entry into the workforce, privacy issues may decline in importance for adoption of the IoT.

LIMITATIONS AND FUTURE RESEARCH

One of the limitations of this research relates to the sample selected. Survey respondents were undergraduate students enrolled in a private college in the northeast United States. While students of several majors were represented, the bulk of the students were business majors with most students between the ages of 18 and 21. Further variation in the population demographics and inclusion of non-students should be undertaken to determine whether these results are generalizable to a wider population.

The development of additional question scenarios relating to IoT technology may also improve the quality of results generated. This study did not include more scenarios as the survey was distributed during limited class time by professors, and it also strived to maintain a high rate of completion by respondents who may have been less apt to complete the instrument in its entirety if it were longer.

A study that compares perceptions of convenience and privacy relating to the IoT may provide important findings for the introduction of IoT technology given the relationships between these two constructs described above. It would also be interesting to study what characteristics of the IoT are perceived by individuals to be more invasive with respect to privacy and whether these factors vary by demographic.

This research project did not consider other factors that may influence perceptions of privacy, security, trust, and convenience for the IoT. For example, how do personality factors play into the perceptions of the four constructs for different types of scenarios? How does social influence play a role? These questions also indicate areas for future research.

REFERENCES

AlHogail, A. Improving IoT Technology Adoption through Improving Consumer Trust. *Technologies* **2018**, *6*, 64.

Baldini, G., Botterman, M., Neisse, R. et al. *Sci Eng Ethics* **2016**. doi:10.1007/s11948-016-9754-5

Barnaghi, P., Wang, W., Henson, C. and Taylor, K. Semantics for the Internet of Things: early progress and back to the future. *International Journal on Semantic Web & Information Systems*, **2012** *8* (1), 1-21

Brown, S.A. Household technology adoption, use, and impacts: Past, present, and future. *Inf Syst Front* **2008** n**10,** 397.

Ebersold, Kyle and Glass, Richard. The Internet of Things: A cause for Ethical Concern, *Issues in Information Systems*, **2016** Volume 17, Issue IV, p.145-151, 2016.

Hsu, C., & Lin, J.C., An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Comput. Hum. Behav.*, **2016** 62, 516-527.

Hsu, Chin-Lung and Chuan-Chuan Lin, Judy. Exploring Factors Affecting the Adoption of Internet of Things Services, *Journal of Computer Information Systems*, **2018** 58:1, 49-57,

Khan W. Z. et. al., "Data and Privacy: Getting Consumers to Trust Products Enabled by the Internet of Things," in *IEEE Consumer Electronics Magazine*, **2019** vol. 8, no. 2, pp. 35-38.

Mobark Q. Aldossari & Anna Sidorova. Consumer Acceptance of Internet of Things (IoT): Smart Home Context, *Journal of Computer Information Systems*, **2018** DOI: 10.1080/08874417.2018.1543000

Nolin, J. and Olson, N. "The Internet of Things and convenience", *Internet Research*, **2016** Vol. 26 No. 2, pp. 360-376.

Nysveen, H., Pedersen, P.E. Consumer adoption of RFID-enabled services. Applying an extended UTAUT model. *Inf Syst Front* **2016** 18**,** 293–314.

Van Den Hoven, J. Fact Sheet - Ethics Subgroup IoT - Version 4.0. *European Commission. Delft University of Technology, n.d.* **2014**.

Weinberg, Bruce D., Milne, George R., Andonova, Yana G. and Hajjat, Fatima M., Internet of Things: Convenience vs. privacy and secrecy, *Business Horizons*, **2015** 58, issue 6, p. 615-624.

Whitmore, Andrew, Agarwal, Anurag and Xu, Li, (2015), The Internet of Things—A survey of topics and trends, *Information Systems Frontiers*, **2015** 17, issue 2, p. 261-274.

Zhou, T. The impact of privacy concern on user adoption of location-based services, *Industrial Management & Data Systems*, **2011** Vol. 111 No. 2, pp. 212-226.

APPENDIX

Example scenario

Please rate your level of agreement with each of the statements following the scenarios described below.

You arrive at work, and your GPS location is automatically transmitted by your smartphone to your home management system. Your home security system recognizes that you have arrived at work and sends you a notification on your smartphone that your home's security system has automatically armed itself, your house doors have automatically been locked, and the heat in the house has been turned off and will turn on again at exactly 4:45pm.

	Disagree strongly			**Neither agree nor disagree**			**Agree strongly**
This automated home security system is an invasion of privacy.	1	2	3	4	5	6	7
I would be concerned that a hacker could potentially break into my home management system.	1	2	3	4	5	6	7
I would trust an Internet-capable electronic door lock and security system to effectively secure my home.	1	2	3	4	5	6	7
I would find it convenient for my home security system to lock/unlock doors and set my alarm system and heat automatically via my smartphone or other mobile device.	1	2	3	4	5	6	7
I would not be worried about an Internet-generated breach into my home via the home security system.	1	2	3	4	5	6	7

Other scenarios

While at work, your smartphone buzzes with a notification that your smart refrigerator has automatically placed an order for milk, bread, and deli meat. The system determined that you were running low on these items and would need them for the next day according to your recent dietary choices. The notification also informs you that these items have been paid for automatically by debiting your checking account and that the items will be available after 4pm for you to pick up at the supermarket closest to your usual route home from work.

In the early afternoon of a blisteringly hot summer day, your home energy management system sends you a message on your smartphone that the electric company has remotely shut off your air conditioning, hot water heating tank, and a home light that you left on by accident this morning because your neighborhood is experiencing a peak grid period which would increase your electric bill. A few hours later, you receive another notification that the peak period has ended and power has been restored to these electrical devices.

On your way back from work, you hop in your "smart car" equipped with a state-of-the-art on-board computer. After easing through several green stoplights on your way to the freeway, you recall a time just a few years ago, where you used to get stuck in long car lines at those intersections before smart vehicles like yours began to "talk" with intersection stoplights to ease traffic patterns in real-time.

While on the freeway, your car's on-board computer notifies you that you have been issued a speeding ticket by the local police authority based on a highway sensor that flagged your car traveling over the freeway's speed limit.

While watching TV, an ad pops up on your smartphone about a new product/service specifically targeted for people in the demographic that usually watch this show.