Spring 2019

Data Disparity: Tiered Pricing as an Alternative to Consumer IoT Data Privacy Regulations

Matthew LoStocco
University of New Hampshire, Durham

Data Disparity: Tiered Pricing as an Alternative to Consumer IoT Data Privacy Regulations

By

Matthew LoStocco

Thesis Advisor: Jeffrey Sohl

Honors Thesis submitted to the Peter T. Paul College of Business and Economics

University of New Hampshire

May 2019

Table of Contents

Abstract

In recent years, Internet of Things (IoT) devices have exploded on the consumer scene. These emerging products bring new technological capabilities into our everyday lives. IoT is projected to contribute anywhere from $4-11 trillion to the global economy and companies are investing billions of dollars into the technology. However, with the vast amount of data that IoT devices collect, consumers are burdening the risk of having their personal data breached or sold to third parties. This paper first identifies why consumers may be weary or willing towards providing their personal data and how unconscious biases in the purchasing process cause consumers to misperceive their level of risk. Then, the impact of potential regulations that may be enacted are analyzed. Finally, a study is conducted that tests consumers' purchasing behavior around a smart speaker that is offered under a three-tier price model providing three different levels of data privacy. From this study, a two-tier price model is proposed as an effective measure towards ensuring greater equality in the personal data trade between consumers and sellers, and a proactive alternative to regulations that may create new challenges for both parties.

Data Disparity: Tiered Pricing as an Alternative to Consumer IoT Data Privacy Regulations

Emerging technologies offer exciting prospects for efficiency and optimization of our everyday lives. Rising utilization and collection rates of data provide organizations and individuals more insight into almost any aspect of our lives. To capture this data across many different mediums, there has been an emergence of the use of Internet of Things devices (IoT). These connected devices capture and analyze data from the environment around them in near-real time. As a result, anything from a watch monitoring a user's heartbeat to a thermostat automatically setting a desired temperature in a home is a result of IoT technology. Consumer IoT devices are rising steadily in popularity. Offerings such as home assist devices, smart phones, smart watches, and smart cars all leverage collected personal data and have gained traction as everyday consumer items. In addition, IoT devices are expected to be a key driver of the data production growth. Data production is predicted to rise from 33 zettabytes per year in 2018 to 175 zettabytes per year in 2025, representing a 61% compound annual growth rate. IoT is expected to account for more than 50% of all data produced in 2025. (Gantz, Reinsel, & Rydning, 2018). While there are impressive benefits to the consumer and economy from IoT devices, the use of the technology poses a risk. Data breaches are exposing the private information of organizations and individuals, resulting in financial impacts for not only consumers, but the organizations involved as well. The average cost of each personal record breached is $148, while the average data breach costs $3.86 million. ("Cost of a Data Breach Study", 2018). Globally, data breaches are estimated to cost organizations up to $445 billion every year. (Janakiraman, Lim, & Rishika, 2018). As a result of rising breaches and misuse of data, consumer concern has grown around the protection of personal data. And with data

collection rates growing, the potential risk of data breaches will continue to grow. Yet, regulations in the U.S. to protect consumers have not been put in place. And additionally, many consumers choose to continue using IoT devices even with the risk that comes with providing personal data.

The risk of consumer data being exploited may not rid the economy completely of IoT technology. It is still projected to be a crucial economic driver in the coming years. However, analysts are not certain exactly what impact this represents. According to a 2015 report published by McKinsey, the potential global impact of IoT ranges from $4 trillion to $11 trillion a year by 2025. There are several factors that contribute to a $7 trillion range. McKinsey notes that for IoT to reach its $11 trillion potential, specific conditions must be present, "notably overcoming the technical, organizational, and regulatory hurdles." (Dobbs, Manyika, & Woetzel, 2015). One is the interoperability of IoT systems. In order for the data to be effectively utilized, IoT systems must be compatible with one another without many restrictions. Another factor is the level of consumer adoption rates, which will impact technology implementation in all aspects of the economy. While business-to-business applications represent 70% of these projections, the reception of the technology on the consumer side generates attention and has a large impact on shaping the public's perception of the technology.

IoT adoption on the consumer side is crucial towards the implementation and value generation of the technology on the corporate side. It is important, then, that consumer IoT devices are perceived well by consumers to reach its economy-wide potential. In order to dispel some risks associated with the use of the technology, regulations can be put in place to garner trust in the eyes of consumers and protect their personal data from being exploited. In May 2018, the European Union passed the General Data Protection Regulation (GDPR), which is a formal

set of policies that organizations must follow to protect the personal data of customers. Other countries, such as Australia and the Philippines, have implemented similar acts. In the U.S., however, there is no federal regulation enacted that protects user data under emerging data collection technologies, but there are steps being taken. In September 2016, the House of Representatives presented HoR 847, which:

> *Expresses the sense of the House of Representatives that the United States should: (1) develop a national strategy to encourage development of the Internet of Things for connected technologies to empower consumers, foster future economic growth, and improve the nation's collective social well-being; (2) recognize the role of businesses in the future development of the Internet of Things; (3) engage in inclusive dialogue with industry and work cooperatively; and (4) determine if using the Internet of Things can improve the government's efficiency and effectiveness and cut waste, fraud, and abuse.*

But does risk mitigation through stricter security measures substantially affect consumer adoption of the technology? Do consumers actually care about data protection if the device provides value in using it? In a study conducted by Cisco in 2017 ("The IoT Value/Trust Paradox", 2017), levels of consumer sediment towards the use of IoT devices and subsequent security risks were identified. 9% of participants believed that personal data being collected by IoT devices is done so securely and 14% believed that companies had effective explanations about how personal data was being used. However, 53% believed that IoT devices made their lives more convenient and 42% believed that IoT technology is too ingrained in everyday life to disconnect even with knowing the perceived risks. Following these results, the report presents the Cisco IoT Value/Trust Paradox, recognizing that there is a gap in how companies perceive IoT compared to consumer acceptance levels, and that the value of IoT is being diminished by data protection risks. To increase this trust, Cisco suggests that companies take steps to clearly

define their data policies and create accountability measures within the devices. The Cisco report concludes that the level of security does affect the net value created by IoT devices, however the study does not address by how much.

This research aims to identify the value consumers place on IoT devices when presented with varying levels of protection over their personal data. By allowing consumers to place monetary values on their personal data, consumers will be able to better comprehend their level of risk exposure, reducing inherent risk biases and promoting more accurate privacy trades with IoT device manufacturers. Meanwhile, companies and private investors are committing billions of dollars towards the IoT market and any restrictions or hindering of forecasted data collection without proper financial benefits will result in substantial value depletion for those investments. To combat these current and potential issues, a study will be conducted that tests a tiered pricing model, which offers consumers varying levels of data privacy for a corresponding purchasing price. From the study, the effectiveness of the proposed privacy solution can be determined by looking at (1) the purchasing intent of an IoT device under each price tier and (2) the level of autonomy consumers feel over their personal data. If determined as an effective measure, the solution could serve an alternative to consumer IoT data privacy regulations by strengthening both consumer privacy trades and the future promise of IoT in the economy.

Literature Review

(De Cremer, Nguyen, & Simkin, 2017) conducted a study to better understand why consumers might be hesitant to share their personal data by discussing the motivation behind obtaining such data. Increased connectivity and data collection of user devices were analyzed to determine causes of consumer exploitation. The authors examine what they refer to as the "dark-side" of IoT, meaning the gathering of user information for deliberate, malicious intent. With the

IoT market growing rapidly and more user data being collected than ever before, much has been discussed about what benefits the technology will bring. However, this study aims to uncover and address the negative effects of continual data collection and offers forward-looking statements to combat these dark-side practices.

De Cremer et al. (2017) conducted an analysis of the industry to determine the motivations behind why IoT providers would engage in dark-side activities. The research first calls out the different use cases for IoT, such as cameras, industrial devices, and GPS systems. Next the study generates examples from companies that have engaged in dark-side activities. Banks, insurance providers, music streaming, and health clubs all have had their issues with consumers, where the organization will exploit the data and mislead its users in order to charge higher fees.

To uncover the determinants of such motivation in IoT providers, De Cremer et al. (2017) broke down dark-side behavior into four categories, each containing two subcategories. The four factors are: integrity, intelligence, transaction, and relationship. The two behaviors in each of those factors are: dishonestly and unfairness in integrity; information misuse and privacy issues in intelligence; financial penalties and confusing customers in transaction; favoritism and switching barriers in relationship. Through examination of the external environment, the study chooses these behaviors to understand the underlying causes for dark-side behavior and the resulting actions.

The development on dark-side practices and behavior were developed into a matrix that explains underlying causes for such activities. De Cremer et al. (2017) provides a framework for issues going forward as a behavioral reference for dark-sided behavior in IoT technology. They found that integrity was the hardest component of the matrix to deter, and that little research has

been done in the area, so such behaviors are enabled. From the analysis, a holistic strategy made up fives components to avoid dark practices is developed: strategy development, value creation, multi-channel integration, information management, and performance assessment. By integrating these components within an IoT use case, dark-sided behavior can be deterred.

The emerging use of connected devices and data sharing will uncover technological advances in everyday life. However, the undeveloped knowledge of its potential risk has yet to be fully uncovered. De Cremer et al. (2017) aim to provide business and organizations a framework to deter dark-sided behavior in the use of IoT products. In doing so, organizations will be able to hedge risk again data misuse and gain trust from the consumer. While more research is needed in this topic, as it is relatively undeveloped, the study provides an introductory measurement of how to better understand the reasonings behind exploitation of consumer data and why consumers may be hesitant to adopt IoT devices. According to the developed framework, tiered pricing may be a potential measure for organizations to deter these dark-side practices.

(Janakiraman, Lim, & Rishika, 2018) conducted a study to uncover the impact that a public data breach would have on consumer purchasing behavior. According to the Center for Strategic and International Studies, data breaches are estimated to cost businesses up to $445 billion and 200,000 jobs annually. When there is a data breach announcement (DBA), consumers react negatively, and customer-firm relationship is weakened. However, various attributes of a customer can determine how likely they are to change their purchasing behavior (and in result, losses for the organization) when a DBA is made public.

Janakiraman et al. (2018) aim to cover four objectives. The first is to compare customer transaction data from before and after a DBA to identify any shifts in purchasing behavior.

Second, the study looks at how consumers change their purchasing behavior at other firms in connection to the breached firm, to uncover what impact a DBA will have on firms that are part of the channel. Third, the study compares purchasing behavior between customers with high patronage levels to the firm and those that are considered low patrons. The final objective is to find the role of customer data vulnerability as a significant cause of negative shifts in consumer behavior, such as reading an email saying that your personal information was involved in a data breach.

To determine the impact that various consumer attributes has on declined purchasing, Janakiraman et al. (2018) utilize a real data set of customer payments from a company that had experienced a data breach. The unanimous company provided is a publicly traded department chain in the apparel industry and had customer payment card information compromised. The study compares the purchasing data of that before the DBA and after the DBA and analyzes the data to determine trends between altered purchasing behavior and the various customer attributes previously mentioned. As control, Janakiraman et al. (2018) segregate purchasing data from customers who had not had information compromised. They also used email data of those who were notified that their data was breached and compares the purchasing behavior difference between those who read the email and those that did not, in order to determine the impact of perceived data vulnerability.

The results showed that customers who had their personal information compromised decreased their spending amount by 32.45% after the DBA. In comparison, the customers whose personal data was not affected by the breach did not change their spending level significantly. The results also indicated that customers who are considered high-level patrons had relatively less change in their spending behavior compared to low-level patrons. For those whose personal

data was exposed, the customers that opened the notification email stating that their personal data was involved decreased their spending level more than the customers who did not read or receive a similar email, showing that negative purchasing behavior can be linked to having a greater perceived data vulnerability.

Janakiraman et al. (2018) demonstrate that when an individual believes their data has become more vulnerable, the perceived risk around that matter is increases, which contributes to a decrease in spending behavior. However, individuals who do not believe or know that their data has been accessed are unlikely to change their spending behavior significantly. Additionally, when customer-firm relationship is strong, customers will reduce their spending behavior relatively less compared to those who were not patrons. For consumer IoT device manufacturers, it is critical to establish strong customer-firm relationship, which may be strengthened by increasing levels of consumer autonomy over the use of personal data. For owners or prospective buyers of consumer IoT devices, they will be less likely to purchase or continue using a device if their perceived risk of their data being breached is greater than the risk level before a DBA.

(Bailey, 2016) conducted a study to further understand why consumers engage in risky behavior as it relates to data privacy. Bailey (2016) notes that when a data breach is made public, there is significant outcry from consumers and media, yet there is little conversation about the fact that consumers grant organizations access to their personal data on a daily basis. In addition, policymakers are pondering regulations that would restrict private data collection. Therefore, Bailey (2016) attempts to provide reasoning into why consumers subject themselves to risk in return for using IoT devices and applies these concepts to the effectiveness of potential regulations.

Bailey's (2016) study is founded on two objectives. The first to analyze the consumer psychology behind discounting risk of IoT devices in return for the advantages of the technology. Second, Bailey (2016) applies the consumer risk-reward trade-off to potential private data regulations for consumer IoT devices and discusses the effect each would have on the consumer and the manufacturers if enacted.

To analyze the effectiveness of potential regulations, Bailey (2016) first discusses consumer behavior and decision-making. Bailey (2016) notes that privacy terms can be unclear and ambiguous about how data is being used. For the sake of the study, it is assumed that consumers are fully aware of the extent to which their data is being used. The first consumer psychology trait discussed is unrealistic optimism. Bailey (2016) notes that the average person believes they are above average, and if presented with the probability of negative event occurring to them, the average person believes they are less likely to experience that event. However, this is statistically impossible because not every individual can be above average. As it relates to IoT, consumers believe they less likely to have their personal data exploited compared to another individual. This perceived risk further weakens due to the lack of public attention towards private data protection. The second consumer bias discussed is the notion of hyperbolic discounting (HD). HD is the idea that consumers are not rational when valuating future events or risks, being impatient in the present and patient about the future. Bailey (2016) applies this concept to IoT devices. Due to the bias of HD, the benefit gained from the device is instant, while the risk of having private data exposed is in the future. This results in the perceived risk of the technology being less than the actual risk during using the decision to use IoT devices. In addition, due to unrealistic optimism discounting the probability of their personal data being misused, consumers are likely to display HD bias when deciding to use IoT devices. Due to these

inherent biases, a consumer's perceived risk is lower than the actual risk, and a result, engages in irrational thinking when choosing to use IoT devices.

After discussing the biases held by consumers during the decision-making process, Bailey (2016) proposes three data protection regulations that could be enacted and analyzes the subsequent impacts of each. The first would be to require companies to provide disclosures that clearly outlines not only how a user's private data is being used, but the potential risk of doing so. This scenario intends to reduce both the lack of knowledge surrounding personal data allowance and the inherent biases consumers hold. By providing the consumer with as much information as possible, as many are unware of the risks of providing personal data, the consumer can make a more educated decision and reduce the bias that goes into risk taking. However, this does not ensure that all consumers will read or understand the message of the disclosure, thus limiting the effectiveness of a disclosure as a standalone regulation. The second would be to set a default opt-out rule under the privacy terms. Often, privacy terms are set to a default choice of "opt-in" that sees the user consenting to firms having access to their data and would have to consciously click out of the default rule to prevent data sharing. This regulation would require all devices to have a default rule that is set to "opt-out," having users' data only be shared if the user chooses to opt-in to data sharing. This regulation would help reduce biased risk perception and promote accurate decision-making by requiring users to make a conscious decision. However, a standard default rule could negatively affect users that choose not to opt-in, as companies may offer incentives that encourage users to allow access into their personal data. The third scenario proposed is strictly regulating the sale of personal data to third parties. This policy would eliminate consumer bias because users would not have to include the risk of the personal data violation in the decision-making process; the risk of a data breach would be the

only risk to account for. Bailey (2016) notes several setbacks of this last scenario. Many companies rely on the sale of personal data to third parties as a significant contributor to revenue and prohibiting this sale would disrupt the performance of the IoT market. Further, this scenario promotes greater paternalism from the government, discouraging consumers from making decisions that are in their best interest and causing harm to already rational decision makers.

Bailey (2016) suggests that consumers do not engage in rational decision making when choosing to adopt consumer IoT devices because consumer bias errors promote an inaccurate understading of perceived risk. Any regulations should work to reduce these inherent biases so a consumer's perceived risk of sharing personal data is more closely aligned with the actual risk. However, a likely reaction by firms to such regulatory scenarios would be to offer incentives that compensates consumers for grating access to their personal data, presenting the case for placing a monetary value on risk exposure in order to promote a fair privacy trade between the consumer and data collector.

Benndorf & Normann (2018) noticed that private data regulations were beginning to gain more attention from policymakers. Companies and government organizations are investing in databases that rely on a wealth of personal data to benefit from the full capabilities of the technology. At the same time, the public is becoming more concerned about how their personal data is being used and protected. Benndorf & Normann (2018) believe that policies concerning private data must strike a balance between the economic benefit of data availability and the personal welfare of consumers. To do that, Benndorf & Normann (2018) suggest that placing a monetary value on personal data to effectively balance trades between purchaser and seller. Benndorf & Normann (2018) conducted a study that tested how consumers would respond to

incentives in return for their personal data in order to assign a market price for specific pieces of data.

Benndorf & Normann (2018) had two objectives. First, to provide an effective and valuable resource to policymakers in regard to personal data regulations. Second, to discover if there is a disparity in consumer responses between a study with real incentives versus a hypothetical survey.

Benndorf & Normann (2018) used Facebook as the test platform in the study. The study tested individuals' responses to three types of personal data collected by Facebook. First, anonymous data on personal preferences such as hobbies or occupation. Second, contact information such as name and phone number. Third, detailed profile data such as unique profile posts and messages. Benndorf & Normann (2018) used a two-step incentive process. First was the Becker-DeGroot-Marschak mechanism, which asked subjects to provide an initial desired selling price, then computed a price at random, and accepted the sale if the subject price was lower than the randomly computed purchase price. Second was a take-it-or-leave-it mechanism, in which subjects were asked to provide their personal information in return for a €5 reward. A hypothetical survey with hypothetical rewards offered ran as the control.

Benndorf & Normann (2018) discovered that 5 out of 6 participants were willing to provide at least some of their Facebook data in return for a monetary reward, while 1 out of 6 were not willing to provide any personal data for any reward. The average request for contact information was €15, while the average request for full access to data on a subjects Facebook account was €19. 5 out of 6 people also accepted to provide contact information for a €5 payment. However, in the hypothetical control surveys, the respondents were much more likely to refuse to provide any personal information. 90% of respondents claimed they would not

provide their personal data for commercial use under any circumstances. The 10% that agreed to provide personal data requested unrealistic compensation a majority of the time.

Benndorf & Normann (2018) indicate that there is clear discrepancy between how consumers believe they value their personal data and how they actually value it. Benndorf & Normann (2018) believe that "people are concerned with privacy, but they are willing to compromise when being paid for the data." Due to the inconsistent responses between being presented with a hypothetical reward versus an actual reward, Benndorf & Normann (2018) suggest that hypothetical research should not be basis of which personal data privacy policies are created from because of the inherent bias present when asked to sell personal data hypothetically. At the same time, regulations that price data based off averages of actual incentives study data would harm those opted to sell their personal data, as the minority who chose not to sell will decrease the market value of specific personal data, resulting in a market demand price less than what a majority of consumers would be willing to sell. As it relates to this research, it can be inferred that a majority of users and potential customers of consumer IoT devices would be willing to exchange personal data for some level of monetary value, effectively putting a quantifiable price on personal data sacrificed to use the device, which in turn would reduce customer bias and hyperbolic discounting. However, it is worth noting that a hypothetical study may not fully represent consumer behavior.

After review of the available literature, it can be concluded that there is motivation towards exploiting consumers' personal data through either a data breach or third-party sale, creating risk for consumers to provide access to this data. It is shown that consumers will react negatively knowing their data has been violated; yet, consumers do not anticipate these risks because of inherent biases during the decision-making process. Current U.S. privacy laws do not

protect against these biases, currently resulting in an imbalanced trade of personal data between consumer and collector. Any regulations put forth would help promote more informed decisions, but at the cost of creating new challenges for the consumer and the firm. It has been demonstrated that most consumers are willing to place a monetary value on providing access to their personal data, presenting the case for using monetary valuation as a metric to measure privacy risk. Doing so may promote a consumer decision-making process that accurately reflects the risk-reward tradeoff when adopting IoT devices.

Methods

This study attempts to determine if tiered pricing models could serve as an effective alternative to data privacy regulations. As shown through the review of literature, consumers do not engage in accurate risk assessment when they trade access to personal data in return for an IoT device. Proposed regulations aim to protect consumers, but at the cost of consumer freedom and harm to profits for device producers. Prior studies have shown that consumers are willing to place monetary values of personal data trades with businesses; this study attempts to expand on that idea as it relates to providing varying levels of data privacy for different prices. Allowing consumers to select their level of privacy based on price will reduce inherent consumer behavior surrounding risk and promote more accurate privacy tradeoffs with IoT device producers. To determine if tiered pricing could serve as an effective alternative to privacy regulations, consumers should demonstrate greater receptiveness in terms of purchasing intent and control over personal data when offered a tiered pricing model compared to a single offering.

To gather this data, students at the University of New Hampshire were asked to participate in a questionnaire. In the survey, participants were asked questions related to their level of interest in purchasing a smart speaker a varying levels of data privacy and prices. Smart

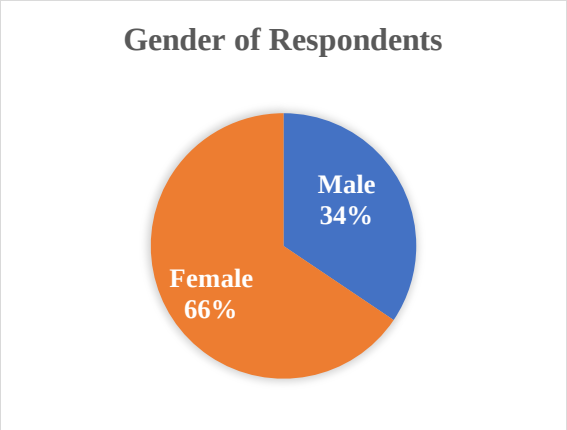
speakers are one of the most popular consumers IoT devices on the market today, so this was chosen as an example to provide a specific product. First, participants were asked if they had ever considered purchasing or had purchased a smart speaker. This provides a base for changes in consumer behavior when faced with varying levels of privacy/prices. The survey presented a three-tier pricing model as follows: standard price for standard level of data privacy, premium price to limit data collection and prevent third-party distribution, and reduced priced to allow third parties to access data directly linked to the user. The control in this study was a standard price, standard privacy offering. Deviations from the control when faced with the two other options was used the primary measure of determining changes in purchasing behavior.[1] Participants were then asked to identify the highest price premium they would be willing to pay to prevent collection of their personal data, as well as the lowest discount they would be willing to accept in return for allowing greater access to their data. Assuming the smart speaker was $100, participants were asked to choose the highest price they would be willing to pay for each condition, with four $10 price ranges to choose from. Then, an average price for each condition was calculated to determine the monetary value consumers placed on either protecting more or less of their data. The next question of the survey asks how likely the subject would be to purchase a smart speaker under a standard, premium, or reduced privacy condition. Subjects are then asked to pick the purchasing tier that they would most likely choose. A result that shows a strong favoring towards standard pricing instead of premium or reduced options would indicate that a tiered pricing model may not be effective. Finally, subjects are asked to choose the level of control they feel they have over their personal data as a result of being able to choose their level of privacy. Responses that show subjects feel more in control over their data indicates that a

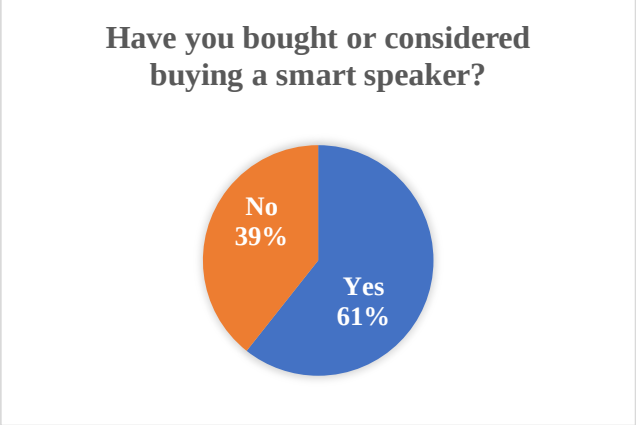
[1] For reference, standard price for standard level of data privacy refers to most current offerings, with a singular price offering encrypted or basic data to be collected by the provider and potentially sold to third parties.

tiered pricing measure may be effective at promoting consumer autonomy over personal data. Even if a subject chooses to give up additional protection to their data, the ability to choose how their data is being leveraged allows the consumer to engage in a more balance trade and be monetarily rewarded for doing so.

Results

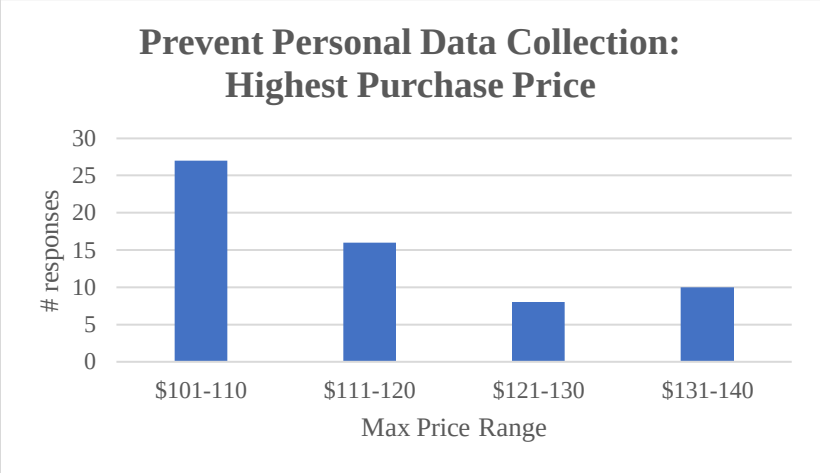
The questionnaire was built online using the Qualtrics platform and distributed through various Facebook communities made up of UNH students. The survey gathered sixty-one responses, consisting of forty females and twenty-one males (or 66% and 34%, respectively). 61% of respondents had either purchased or considered purchasing a smart speaker, while 39% did not.

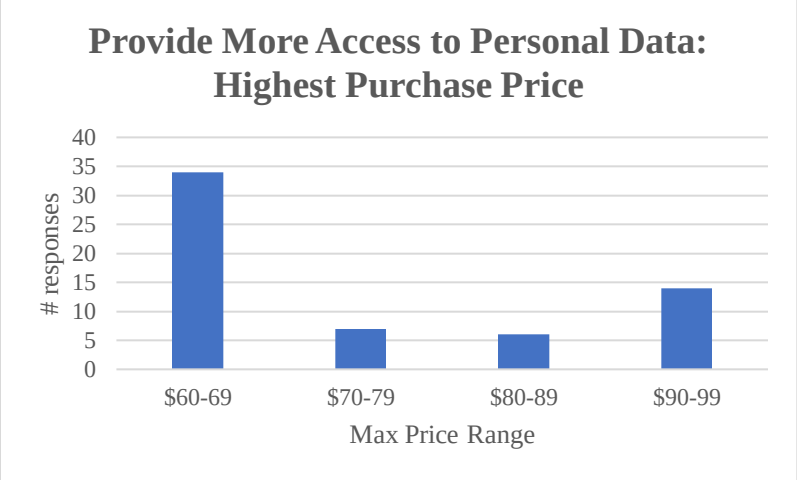




When asked to provide the highest price one would be willing to pay for a smart speaker (given that a standard offering costs $100 and price premiums/discounts reflect the provided level of clarity into personal data), respondents showed price sensitivity in both cases. More than half of respondents said that they would be willing to buy a smart speaker at a reduced privacy level under the $60-69 price range, the lowest price range provided by the question. Regarding the premium offering, 70% of respondents chose a desired price range between $101-120. The

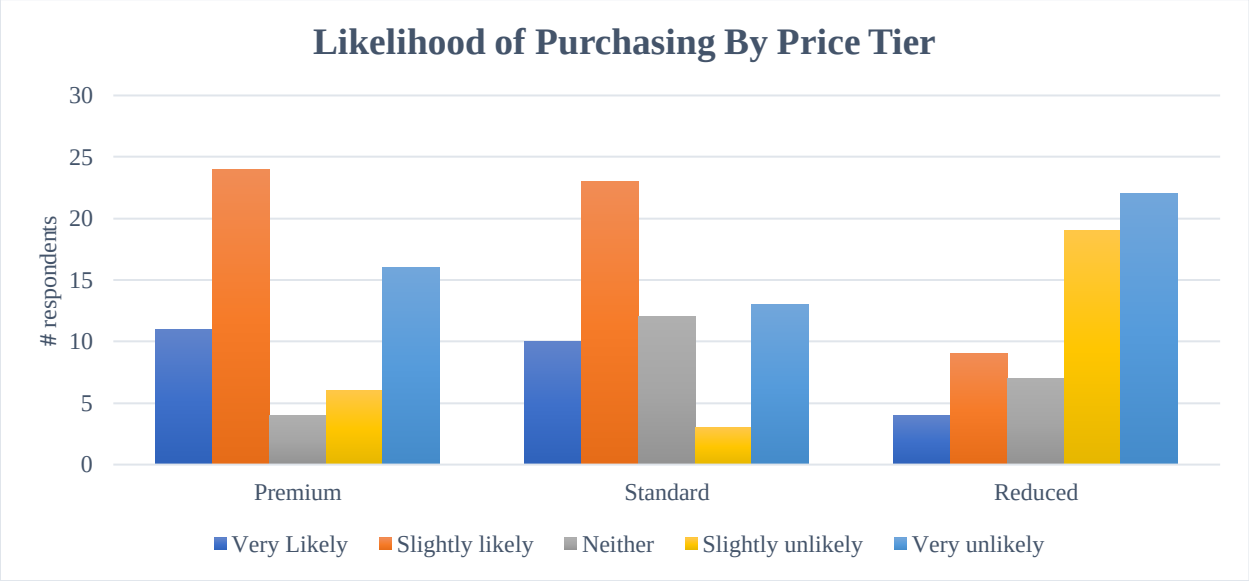
average price for each condition was $74.50 for the discounted product and $115.66 for the premium, or a 25.5% and 15.7% deviation respectively from the standard price.



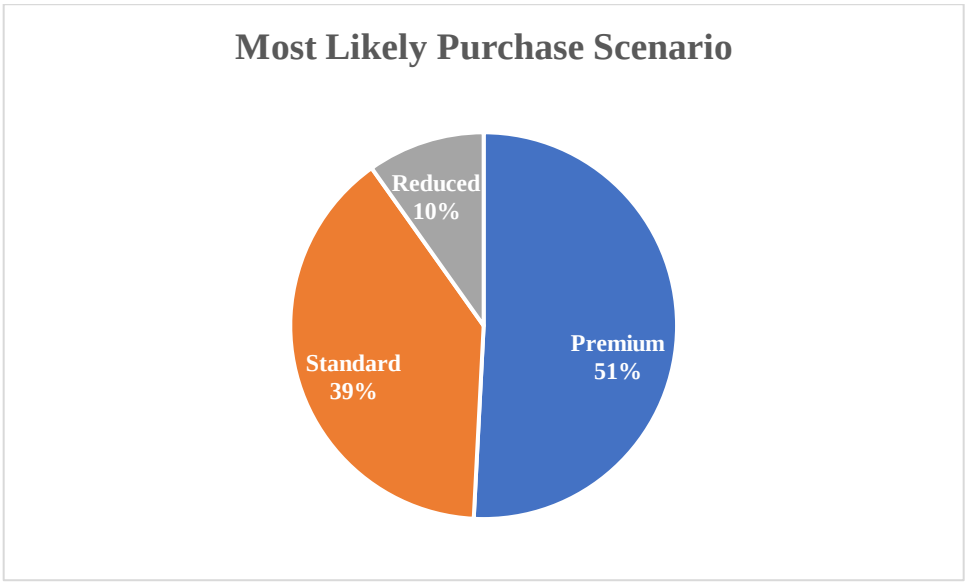


Respondents were then asked how likely they would be to purchase a smart speaker under each of the three conditions. Premium and standard offerings had nearly similar rates of consumer sediment, with 57% of respondents feeling very or slightly likely to purchase a smart speaker at a premium level of privacy and 54% responding similarly to a standard offering. However, only

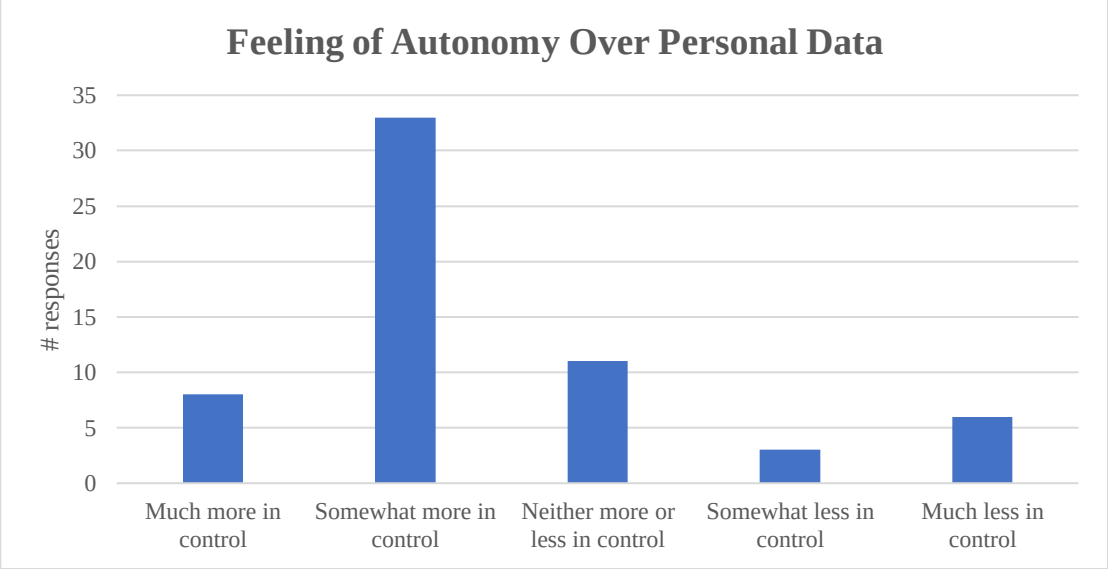
21% of respondents said that they were likely to purchase a smart speaker that was offered at a discount for lower privacy restrictions.



When asked to select one offering that the respondent would most likely choose when presented with three different privacy scenarios, 51% said they would choose to pay more to protect more of their data. The standard offering was selected as the preferred purchase by 39% of respondents and the discounted product was selected by 10% of respondents.



The final question asked respondents if they felt they had more autonomy over how their personal data was being used when presented with the option to choose their level of data privacy. Two-thirds of respondents felt that they were either much more or somewhat more in control over their personal data under a tiered pricing model.



When isolating the 39% of respondents that had not purchased or were not initially interested in purchasing a smart speaker, a change in purchasing intent can be observed. In Question 5, 17% of these respondents said they would likely purchase a speaker under the standard conditions. In comparison, 46% of these respondents said they would likely purchase a smart speaker with stronger security for a premium, a 29% increase between the two tiers.

Analysis

After analysis of the data recorded by the survey, it can be inferred that a three-tier model would not be sufficient. While premium and standard offerings were well-received by respondents, the reduced option that offered a discounted price in return for giving additional access into a user's personal data was not well-received. 67% of respondents said that they were

unlikely to purchase a smart speaker under this offering, compared to 26% unlikely for standard and 36% unlikely for premium. In addition, only 10% of respondents chose the reduced offering as the ideal purchasing scenario. Further, more than half of respondents answered that the highest price they would be willing to pay for that kind of privacy was the lowest range offered, $60-69. As this was the lowest range possible respondents could answer, the $74.50 is very likely higher than the true average respondents would be willing to pay. With strong reception to higher-than-standard security, consumers may feel that a standard offering is not sufficient for their personal needs. So, it is understandable that offering a tier below standard protection could be too risky for consumers to purchase even at a 25% price discount. This offering would also open up greater risk to IoT providers in facing financial and public image repercussions from a data breach as there would be collection of more sensitive data.

As a result of these responses, a three-tier model would not be an effective measure to improve the current trade imbalance of consumer data. However, the data shows that a two-tier model consisting of a premium and standard offering could be an effective measure. Respondents were highly receptive to the premium offering and more receptive to the premium offering than the standard offering. The average price of the premium offering was around 16% higher than the standard offering, indicating that consumers value the data collected by a smart speaker at that percentage of the purchase price. Another metric to evaluate is the change of purchasing interest when presented with a higher-privacy option. Those who answered “No” regarding if they had purchased or considered purchasing a smart speaker were more interested in the product if it offered higher privacy. This indicates that some consumers want more privacy than what is standardly offered on the market and are willing to pay a premium for it.

Discussion

With strong sediment towards premium offerings, could it be inferred that the heightened protection condition should become the standalone new standard? There would be two issues with this new standard if this were the case. The first is that the imbalanced data trade would flip from weak on the consumer side to weak on the provider side. IoT providers would face operability hurdles from not being able to leverage data collected from users to make improves to the device and financial hurdles from not being able to sell data to third parties. The second issue of this reality is the fact that not all users value their data in the same way. Some users may not want to pay a premium to protect more of their data if they feel that standard measures are sufficient. Providing two different options would appeal to a wider range of consumers and allow consumers to choose to pay for heightened data protection. In addition, IoT vendors would be compensated for the lost value that would come with some consumers opting for heightened protection in the form of an upfront premium. A two-tier model would help balance the trade of data between consumer and provider without imposing restrictive measures that would presented new challenges for each party.

The research was limited by a few factors. The first to note is that the questionnaire was built around consumer sediment towards a smart speaker. While this device represents a popular IoT product on the market today, not all consumer IoT devices collect similar data. Data collected by a smart speaker, such as vocal conversations and consumer preferences, is different data than what is collected by a fitness tracker, which might collect data on a user's personal health. Therefore, deviation from the standard price and product purchasing intent for each privacy tier may differ between the type of IoT device. This study is limited by solely demonstrating the general sediment towards tiered pricing models as relates to personal data and

consumer devices. Those choosing to deploy a tiered pricing model should conduct independent research for the specific product in order to account for the different data types being collected, as well as prior consumer sediment towards the standard offering. Another shortcoming of the research is the hypothetical nature of the study. As shown by Benndorf & Normann (2018), consumers are more likely to engage in risk-averse behavior in a hypothetical setting. But when presented with real monetary situations, consumers were more likely to give additional access to their personal data for that monetary reward. If tiered pricing were to be deployed in a real consumer setting, it could be inferred that purchasing intent for the reduced price would be greater than the hypothetical questionnaire. In addition, this study only looked at a few metrics to determine if a tiered pricing model is effective; namely, the interest in purchasing under each price tier and the level of autonomy users feel over their personal data. To further assess the "effectiveness" of tiered pricing, additional metrics should be tested. Furthermore, this study solely focuses on responses from students aged 18-22. Sediment towards a tiered model may differ between various demographics.

More research is needed to validate the effectiveness of a tiered pricing model in a real consumer setting. IoT device producers looking to implement such model should determine the tier prices and purchasing intent under each privacy level of the specific device, as data does not hold uniform value across IoT devices. While there are currently shortcomings to the model, tiered pricing could act as a solution for producers that are looking to not only protect themselves from consumer and regulatory backlash but increase their addressable customer base by providing additional offerings. For example, grocery stores may offer organic and non-organic variations for the same produce. While not all consumers are looking for organic produce, the store appeals to those that are, and is able to charge a premium on those products due to the

various benefits of organic food (less additives, better for the environment). The same logic can be applied to a premium and standard device offering. While not all customers are looking for a premium privacy offering, the IoT producer can meet the needs of those that are by providing the heightened privacy product for a higher price due to the greater benefits that come with the device (less risk of data breach or third-party exploitation).

While it is unknown how the United States will follow through on proposed regulations towards consumer data privacy, implementation of tiered pricing looks like a promising solution that could be adopted by device producers or implemented as a regulation itself. As the amount of personal data being collected grows at a rapid clip, so too is the risk of data breaches and third-party exploitation. Consumers are demanding greater autonomy and protection over their personal data, yet are unable to engage in such behavior due to current device offerings and unconscious purchasing biases. The tiered pricing model is a potential first step towards ensuring higher equality between consumers and producers engaging in a personal data trade.

References

2018 Cost of a Data Breach Study: Global Overview. (2018). IBM, Ponemon Institute.

Bailey, M. W. (2016). Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things. *Texas Law Review, 94(5)*, 1023–1054.

Benndorf, V., & Normann, H. (2018). The Willingness to Sell Personal Data. *Scandinavian Journal of Economics, 120(4)*, 1260–1278.

De Cremer, D., Nguyen, B., & Simkin, L. (2017). The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side. *Journal of Marketing Management, 33(1/2)*, 145–158.

Gantz, J., Reinsel, D., & Rydning, J. (2018). The Digitization of the World: From Edge to Core. IDC, Seagate.

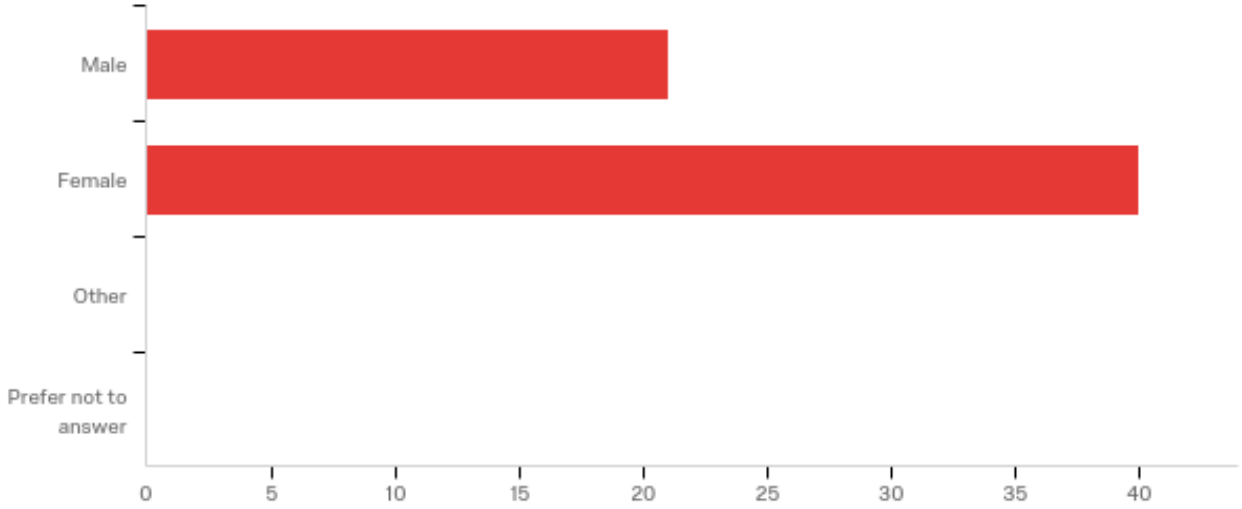
Dobbs, R., Manyika, J., & Woetzel, J. (2015). The Internet of Things: Mapping the Value Beyond the Hype. McKinsey Global Institute.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing, 82(2)*, 85–105.

The IoT Value/Trust Paradox. (2017). Cisco, Jasper.

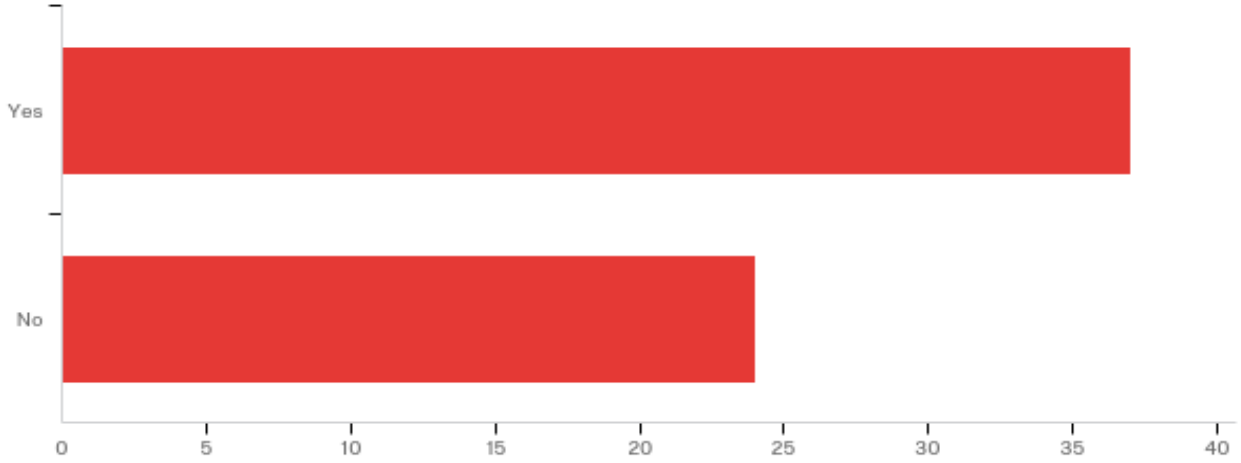
Appendix

Q1 - How do you identify yourself?



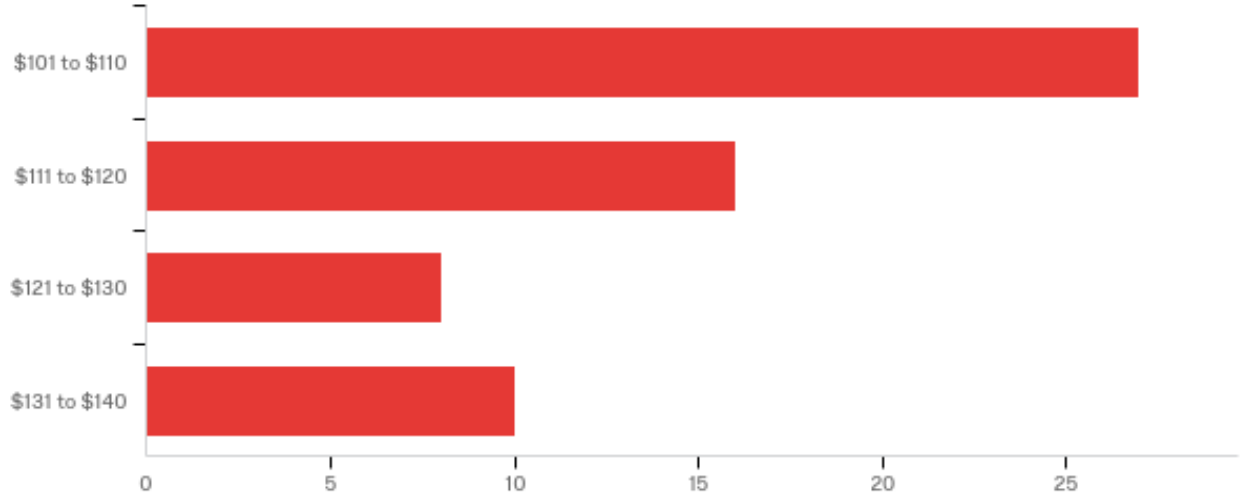
#	Answer	%	Count
1	Male	34.43%	21
2	Female	65.57%	40
4	Other	0.00%	0
5	Prefer not to answer	0.00%	0
	Total	100%	61

Q2 - Have you ever bought or considered buying a smart speaker (e.g. Amazon Alexa, Google Home, Facebook Portal)?



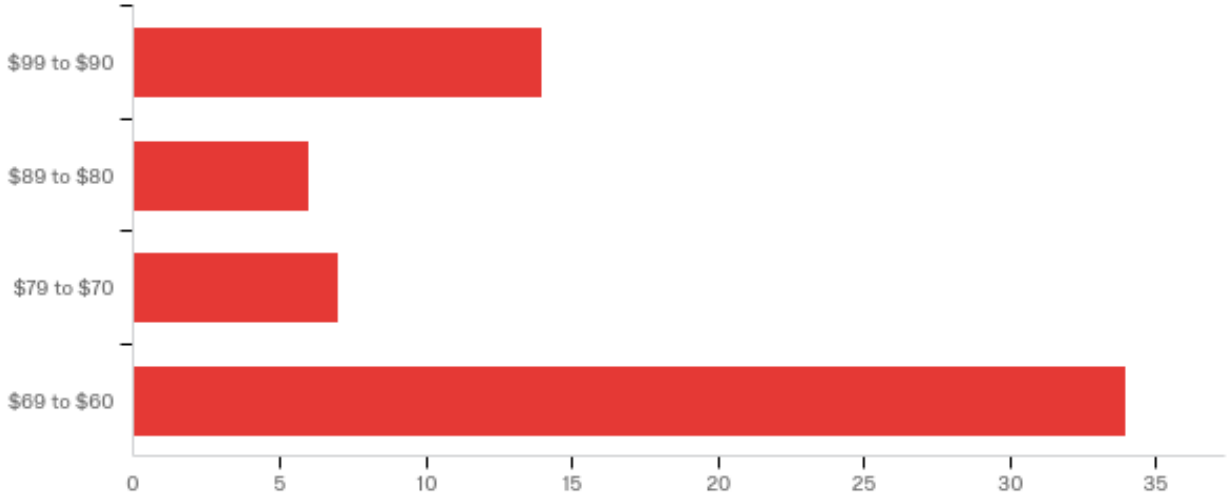
#	Answer	%	Count
1	Yes	60.66%	37
2	No	39.34%	24
	Total	100%	61

Q3 - A smart speaker sells for $100. Suppose you could pay an additional amount to prevent your personal data from being disclosed publicly or to any third parties. How much would you willing to pay for a smart speaker?



#	Answer	%	Count
1	$101 to $110	44.26%	27
2	$111 to $120	26.23%	16
3	$121 to $130	13.11%	8
4	$131 to $140	16.39%	10
	Total	100%	61

Q4 - A smart speaker sells for $100. Suppose you can agree to grant additional access to your personal data (i.e. third parties can access to data directly linked to you) in return for a lower purchase price. How much would you be willing to pay for a smart speaker?

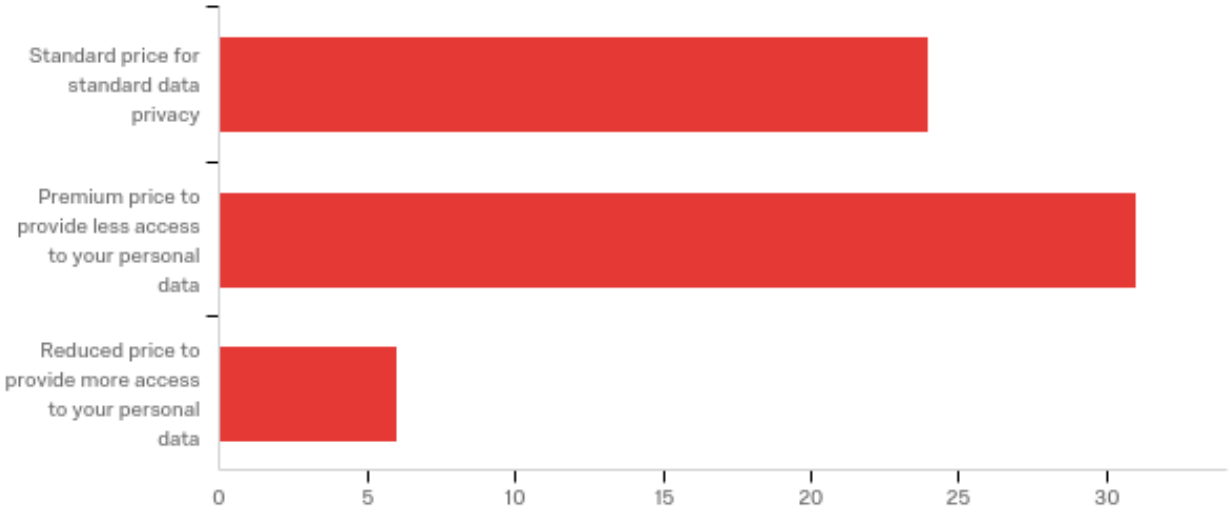


#	Answer	%	Count
1	$99 to $90	22.95%	14
2	$89 to $80	9.84%	6
3	$79 to $70	11.48%	7
4	$69 to $60	55.74%	34
	Total	100%	61

Q5 - How likely are you to purchase a smart speaker under the conditions below?

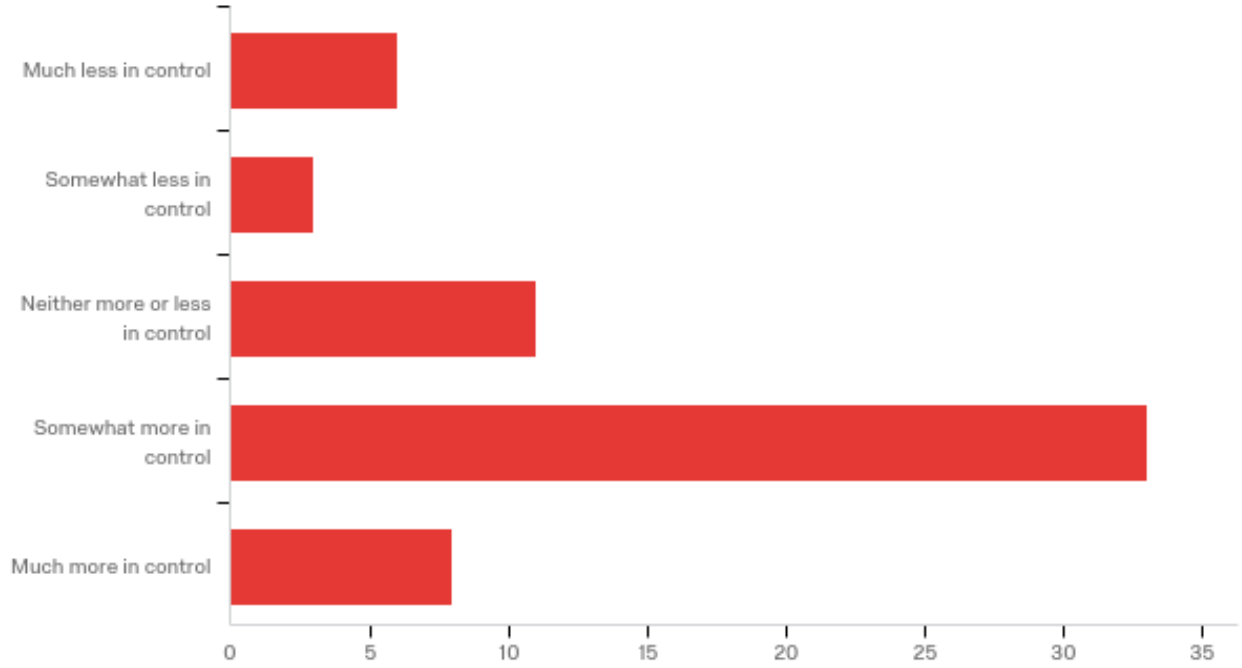
#	Question	Very likely		Slightly likely		Neither likely nor unlikely		Slightly unlikely		Very unlikely		Total
1	Standard price for standard data privacy	16.39%	10	37.70%	23	19.67%	12	4.92%	3	21.31%	13	61
2	Premium price for higher data privacy	18.03%	11	39.34%	24	6.56%	4	9.84%	6	26.23%	16	61
3	Reduced price for lower data privacy	6.56%	4	14.75%	9	11.48%	7	31.15%	19	36.07%	22	61

Q6 - Suppose you could purchase a smart speaker under one of the three conditions below. Which option are you most likely to choose?



#	Answer	%	Count
1	Standard price for standard data privacy	39.34%	24
2	Premium price to provide less access to your personal data	50.82%	31
3	Reduced price to provide more access to your personal data	9.84%	6
	Total	100%	61

Q7 - When given the option to choose a purchase price based on your level of data privacy, what extent of control do you feel over your personal data?



#	Answer	%	Count
1	Much less in control	9.84%	6
4	Somewhat less in control	4.92%	3
5	Neither more or less in control	18.03%	11
6	Somewhat more in control	54.10%	33
7	Much more in control	13.11%	8
	Total	100%	61