The Influence of Perceptions of Safety & Socioeconomic Factors on Smart Lock Adoption Rate

AP Research

May 2nd, 2022

Word Count: 5300

Contextual Information

Since the advent of the industrial revolution, humans have been inventing new technologies to help mankind and improve quality of life. More recently, smart home technology has become more prevalent and widespread. Smart home technology is technology that is used to "monitor the internal environment and the activities that are being undertaken whilst the house is occupied" (Ricquebourg et al., 2006, p. 1). This data can then be used to modify the environment to benefit the user. Many examples of smart home technology can be seen in everyday life, from Amazon's Alexa to smart bulbs and thermostats. One of the lesser known technologies in this category is the smart lock.

There are numerous applications of smart locks. A smart lock controls the deadbolt that secures one's house and can be used to automate locking and unlocking. Automatic locking can keep a home more secure by locking the door when one forgets to. Furthermore, smart locks are more convenient for the user by providing keyless entry. One smart lock customer notes that "it is easy for kids to access the house because all they need is a code and there is no risk of them losing a physical key" (2020). This functionality also makes home delivery processes efficient for all parties involved. For example, grocery stores can cut down on "last mile" and "high consumer delivery costs" as customers do not have to be at home at the time of delivery (Bijvank, 2018). A smart lock would allow a temporary key to be made which would only unlock the door at a specified time and allow items to be placed just inside the door. This is especially convenient for consumers when the item being delivered is time sensitive. The idea of a temporary key also leads to applications in Airbnb. A physical key is inefficient as it requires in-person interaction and holds privacy concerns (de Camargo Silva et al., 2019). A temporary key, held in a smartphone, allows quick transfership of access and reassures guests that only they have access to the property. Due to the numerous benefits that smart locks provide, demand for this technology is increasing.

This technology is predicted to be prevalent in the future with Grand View Research finding that "global smart lock market demand is expected to reach 41.9 million units by 2028" (2021). Furthermore, this demand grows in parallel with the demand of smart home technology, in general, which expands at an annual rate of 17.2% (Park et al., 2017). However, the demand for smart locks may not be as stable as expected. This is primarily due to the nature of home security systems and its unique importance. People are more anxious to adopt a technology that

controls safety compared to a smart home technology which controls lighting, for example. With the potential of smart locks being limitless, it is important to identify the factors which cause lower adoption rates in smart locks, compared to other smart home technologies. Research in this area could be used to better market smart locks and create an upward trend in smart lock acceptance.

As demand for smart lock technology fluctuates, research must be conducted on what factors influence the rate of its adoption. Although much research has not been done in regard to smart locks, several factors have been identified as influential in smart home technology adoption. Further research must aim to identify if the same factors are influential in smart lock adoption. Therefore, an initial research question arises: what characteristics make one likely to adopt (to use) smart locks? Furthermore, this question brings up three main subquestions. How significant of a factor is security in one's decision to use a smart lock? Does access to information about smart locks affect perceptions of security? How does location or current environment affect willingness to use smart lock technology?

Literature Review

Three main factors have been identified as influential in smart home technology adoption: perception of security, socio-economic qualities, and personality.

Perceptions of Security

For the smart lock, specifically, the biggest potential factor is perception of security. Currently, many consumers see smart locks as a threat to their security and a privacy concern. Blythe et al. finds that 90% of consumers distrust the IoT technology behind smart locks (2020). The Internet of Things (IoT) is a network of devices composed of smart locks and other smart devices connected by the internet and servers. Khan and Salah also recognize that the IoT is "easy to hack and compromise" and "pose[s] a threat to privacy, integrity and confidentiality of data" (2018). Alongside IoT concerns, smart locks are also made vulnerable by bluetooth low energy. Bluetooth Low Energy (BLE) is the technology that makes smart locks function. Smart Locks use BLE to communicate with one's smartphone. This process determines when the device locks and unlocks. Prada-Delgado et al. explains that this process includes five features: pairing, bonding, device authentication, encryption, and message integrity (2016). Furthermore, the authors show in their analysis of a smart lock how this process can be tricked and how

unauthorized access can be gained, confirming the general consensus that smart locks are susceptible to attacks and untrustworthy currently.

While there are many concerns about security of the smart lock, Blythe et al. notes that 42% of consumers are willing to disregard security concerns due to the "value afforded by it" (2020). This directly contradicts the previous finding that 90% of consumers distrust smart lock technology, leading to questions about how much consumers are willing to sacrifice in security for potential benefit. This is also known as the privacy paradox (Blythe et al., 2020). Schneier confirms this paradox by explaining that security is a trade-off. He continues by stating that "security costs money, but it also costs in time, convenience, capabilities, and liberties" (2008). Consumers must determine at what point they are willing to "draw the line" and stop sacrificing security for the benefits. The privacy paradox may be important in the research being done and provides clues as to how adoption rates may be increased. If public perception of the security of smart locks is increased, customers will be more willing to accept the devices as they move farther from the metaphorical "line".

Public perception of safety may increase in the near future with the introduction of block-chain technology and other fixes. As previously mentioned, smart locks are vulnerable to various attacks. Blockchain technology, the same technology behind cryptocurrency, might be the solution to the many security concerns as it will "decentralize the system" by compartmentalizing the process bluetooth low energy (BLE) uses to communicate to the smart lock (de Camargo Silva et al., 2019). Han et al. explains that blockchain technology works in four steps. First, nodes will interact with the blockchain network via a pair of private/public keys. Next, the transaction is verified by all nodes in the blockchain network. Then, each node collects records of previous transactions. Lastly, all nodes select a block that is being broadcasted for the first time and verify that the block "contains valid transactions" (Han et al., 2017). By having nodes across many servers verify each other, the system becomes extremely secure and hard for an attacker to corrupt. This technology provides hope that the perception of safety will greatly increase in the future, leading to higher adoption rates.

The current perception of safety is largely based on the information that the average customer has access to. Vivint, a major manufacturer of smart locks, provides little security information on their website. Only a basic explanation of how a smart lock works is given and the information focuses only on its benefits. Drawbacks or security concerns/improvements are

not mentioned. This is important as Shuhaiber and Mashal find in their study that the more information people have about smart homes and how they work, the better their attitude was towards them (2019), implying that the adoption of smart locks may be affected in a similar way.

Socio-economic Factors

While perception of security plays an important role in adoption rates, socio-economic factors are also expected to influence rates. Age is one such factor. Shin et al. finds that "older people are more likely to purchase smart home products within six months or one year", whereas the purchase time for younger demographics was delayed (2018). However, it is important to note that purchase intention was never affected by age (Shin et al., 2018). The authors of the study expected this result because the priorities someone has vary a great degree with age. Additionally, adoption rates vary with gender. Shin et al. notes that perceived usefulness of a smart home device was greater in older and male groups, while compatibility was "more important in the higher education and female groups" (2018). Surprisingly, income does not have a great effect on the adoption rate of smart home devices. It had a great effect on purchase timing, but not purchase intention (Shin et al., 2018). This is crucial as it becomes plausible that the current price of smart locks is not too high for the average consumer.

Personality

Lastly, personality traits of a consumer may have an effect on adoption rates. In their study, Parag and Butbul found that "gender, income, openness to experience, and positive and negative attitudes toward SHT explained 64.4% of the variance in interest in smart Homes" (2018). More importantly, the authors found that willingness to try smart home technology led to greater rates of permanent adoption, agreeing with the Technology Acceptance Model (TAM) which explains that rates of adoption are directly correlated to openness to experience (King & He, 2006). This supports the theory of Ajzen, who explains that past behavior has a significant impact on behavior in the future (1991). His "Theory of Planned Behavior" can be applied to the prediction of smart lock adoption rates. If the customer has a history of buying smart home products or safety products, in general, the Theory of Planned Behavior explains that they are likely to buy the smart lock. This provides a deeper insight on the kind of person who might buy a smart lock.

Gaps in Understanding

While it is generally understood how personality traits and socioeconomic rates affect smart lock adoption rates, it is less understood how changes in perceptions of security regarding smart locks does. The current perception of safety is known and well-defined but the effect of changes in these perceptions is not well documented. This provides opportunities to discover what can change perceptions of security over time. Several causal factors may be media, homeowner experiences, a bandwagon effect, or the advent of new technologies. In specific, there has been little public research done on how the amount of smart lock information available (media) to the average consumer affects perception of security, and therefore, adoption rates. Furthermore, there is not much research on factors that affect adoption rates of smart locks. The current research is more general and focuses on factors that affect adoption rates of smart home technology rather than specifically smart locks. Research must be done to confirm if the three factors: perceptions of security, socio-economic traits, and personality, affect the adoption of smart locks in a similar way. Specifically, the question must be answered: How do socioeconomic factors and perceptions of security, aided by the current information available, affect the adoption rate of smart locks?

Research Design and Methodology

Previous Methods

This study attempted to find the relationship between the adoption of smart locks and three variables: participants' perception of security, their access to known information, and various socioeconomic factors such as age and income. Past methods were used to guide the methodology of the researcher and to inform important decisions.

The first key aspect of the researcher's design was the use of an online survey. A study conducted by Shin et al. analyzed factors affecting consumer adoption and diffusion of smart home services. The authors of this study utilized a two-part survey method: one survey to clarify adoption intentions and another to investigate usage behavior. Shin et al. (2018) acknowledges that the smart home market is relatively new, making it hard to access consumer data on smart home technology, justifying the use of a survey. An online survey allows for authors to collect preference data easily. The particular survey was sent to 310 South Korean smart home users, controlling for location and granting access to the general homeowner population. Homeowners were chosen to be the target population as they have the most stake in the market. Homeowners

are more likely to have opinions on smart locks as it is a technology designed to, specifically, make their life better.

Furthermore, it was decided that a quantitative approach to collecting data would be used. A study conducted by Williams et al. aimed to "investigate the influence of a number of individual difference characteristics on the adoption of secure use of smart home technology" (2020). The authors of this study used a quantitative survey methodology to examine how differences in personality, such as risk-taking propensity and impulsivity, and the extent to which socio-demographic characteristics influenced adoption of smart home technologies and use behaviors. Not only did using a quantitative survey methodology allowed for numerical data to be collected, making statistical analysis easier, but the authors of this study, similar to Shin et al., implemented their survey online. In doing so, the authors were able to gather a large amount of responses (633) over a relatively short time. This is vital, as it looks for opinions of a vast homeowner population. Therefore, a large, representative sample was needed. By implementing their survey online, Williams et al. were able to gather a large amount of responses over a relatively short time.

When studying the correlation between various variables and the adoption of smart home technologies (like the smart lock), the survey method seems to be the best option for most researchers. While this method is certainly effective, it is primarily a form of quantitative data collection, only allowing for descriptive claims to be made about the population. Rather than solely analyzing the opinions of the sample, the researcher wanted to analyze changes in opinion. As the aim was to find the relationship between smart lock knowledge, how perceptions of security changed and adoption rate, a more experimental approach was more appropriate. Therefore, the survey design that Shin et al. and Williams et al. used was modified to meet the needs of this study.

Design

While the aim of the study was to identify how socio-economic factors and perception of security affect adoption rates of smart locks, the researcher also wanted to identify how the change in the amount of information available to consumers about smart locks affects adoption intention. Therefore, a mixed-method design was used. The design utilized elements of a survey, but also introduced a change and attempted to measure a response from the participants. This was done by having the participants take a pre-test, read an article, and then take a post-test. The

goal was to analyze how the independent variables (perceptions of safety, information about smart locks available, and socio-economic factors) affected the adoption rate (the dependent variable) before and after reading the article.

An initial survey (see questions 1-11 in Appendix B) was used to determine the participants' initial perceptions of safety, socioeconomic traits, and initial adoption rates. The pre-survey asked about the participants' age, gender, location, and household income, allowing for a baseline analysis of the participant and isolated the effect of perceptions of safety and the socioeconomic factors on adoption intention. Furthermore, participants were asked how safe they feel in their home (question 4 in Appendix B) from "I do not feel safe in my home" to "I always feel safe in my home". This was done in order to determine how safe someone felt impacted adoption rates. Participants were also asked on a similar scale used for the previous question how much they know about smart locks (question 6 in Appendix B), how much they trust the security of smart locks (question 8 in Appendix B), how much they trust technology in general (question 9 in Appendix B), likeliness of using a smart lock in the present (question 10 in Appendix B), and likeliness of using a smart lock in 10 years (question 11 in Appendix B).

Then, the participants were then exposed to a change in the independent variable to see how responses to the questions changed; in this case, the participant was asked to read a short article on smart locks (see Appendix A), how they function, and potential security risks and fixes. The article was adapted from "What is a Smart Lock and How Does it Work?" written by ADT. It discussed the benefits and uses of smart locks such as: keyless entry, mobile access, custom user access codes, and smart keys. Specific components were added to the article which discussed security concerns of smart locks such as the use of Bluetooth Low Energy and the use of IoT technology. Furthermore, future solutions to these security concerns such as the implementation of blockchain technology were discussed.

A post-survey (questions 13-17 in Appendix B) analyzed the effect of the article on participants' responses; the participants were asked once again how much they know about smart locks (question 13 in Appendix B), how much they trust the security of smart locks (question 14 in Appendix B), how much they trust technology in general (question 15 in Appendix B), likeliness of using a smart lock in the present (question 16 in Appendix B), and likeliness of using a smart lock in 10 years (question 17 in Appendix B). By including a post-survey, the effects of the article and access to new information were isolated and analyzed separately.

Participants and Instruments

The study was conducted on homeowners in the suburban Nashville area. This was to minimize the effects of location on smart lock adoption rate and isolate the independent variables as the only influencers. The survey was posted on a social media platform and participants could choose whether or not to take the survey. While voluntary response sampling is generally less effective in generating good data, it was necessary in this case to gather a large amount of responses in a short time. 36 data points were collected throughout the course of the survey. The sample consisted of people aged 17 to 62, with 25 females and 11 males. All of the participants were located in the suburban Nashville area, with 68% of the sample being located in the zip code 37027.

For this study, a computer was used to create the survey and administered online (included the pre-survey, article, and post-survey). The survey was distributed on various social media sites such as Facebook, Instagram, and Nextdoor. The data was analyzed using Python. The Python libraries pandas, seaborn, matplotlib, and statsmodels were used for data analysis and plotting.

The resulting data was imported from a csv file and made into a Pandas Dataframe. This dataframe was manipulated and analyzed to draw connections between the relationships between different variables and formulate conclusions. Data was converted into a numerical form with each answer choice being assigned a number. A contingency table (table of counts) was created for the responses to the questions. The contingency table made it easy to visualize how the data changed before and after the article. Initial analysis included descriptive statistics gathered by Pandas.describe() and bar graphs created by using seaborn and matplotlib. In order to determine if changes in responses were statistically significant, a Stuart-Maxwell test was conducted. The Stuart-Maxwell test is a statistical test used to determine if two variables are homogeneous (Stuart-Maxwell Test). In other words, it determines if the distribution of the occurrences of two categorical variables are the same. This was beneficial as it allowed for a conclusion as to whether or not the article had an effect on the response of the participants or if the results simply occurred by chance. The contingency tables created were fed into the homogeneity function from the statsmodels python package to run the Stuart-Maxwell test.

Results and Analysis

The first variable that was analyzed was the amount of information known about smart locks by each participant before and after reading the article. This variable was referred to as the "Level of Expertise". Bar graphs of the responses were plotted with the y-axis representing the number of responses in each category.

Figure 1

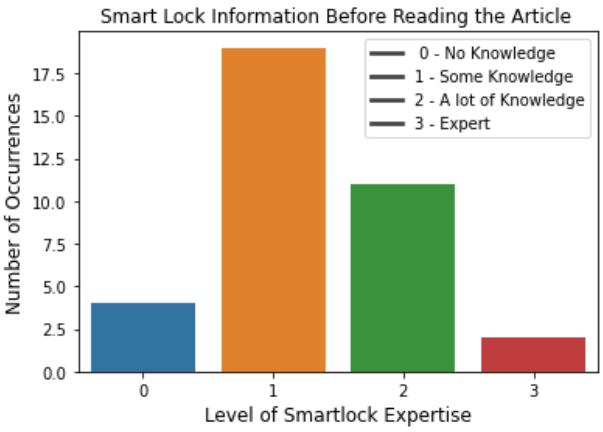
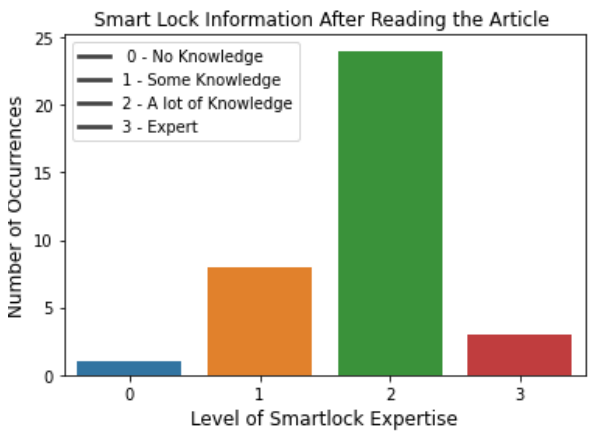


Figure 2



While there are still responses in every category in the 2nd bar graph, comparison of the two plots (Figure 1 and Figure 2) shows that Level of Expertise generally increased after reading the article. This was confirmed with a Stuart-Maxwell test.

The hypotheses for the test were the following,

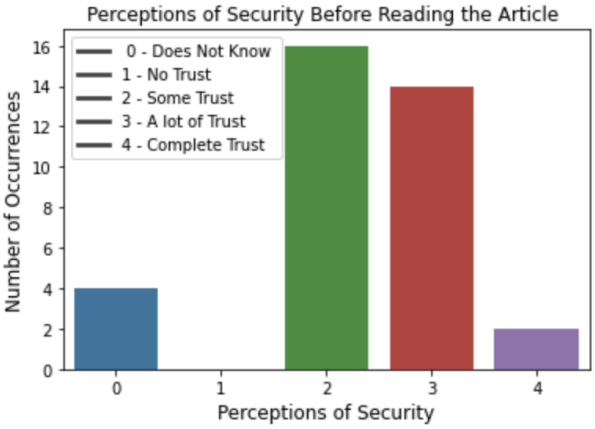
H_0: The marginal distribution of counts of the level of expertise before reading the article does not differ from the distribution after reading the article.

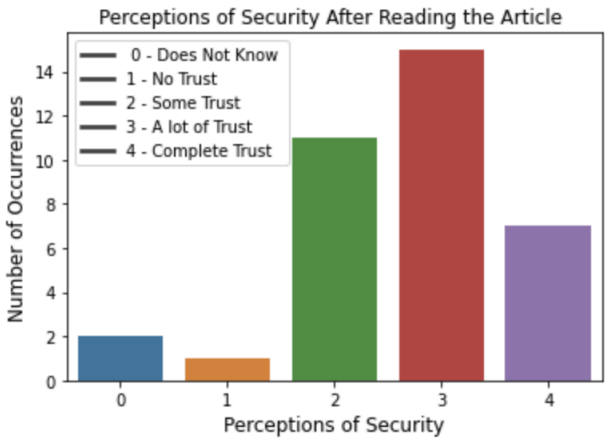
H_A: The marginal distribution of counts of the level of expertise before reading the article does differ from the distribution after reading the article.

The result was a p-value of .0131 and a test statistic of 10.770 (df = 3). As the p-value was less than $\alpha = .05$, the researcher rejected the null hypothesis and conclude that the article did have a significant effect on the amount of information the participant knew about smart locks before reading the article and after reading the article. The results of the test showed that the article was a good medium of conveying information about smart locks. Now that it is known the article led to an increase in information, we can analyze how this increase in information affected the other variables being analyzed.

Figure 3

Figure 4

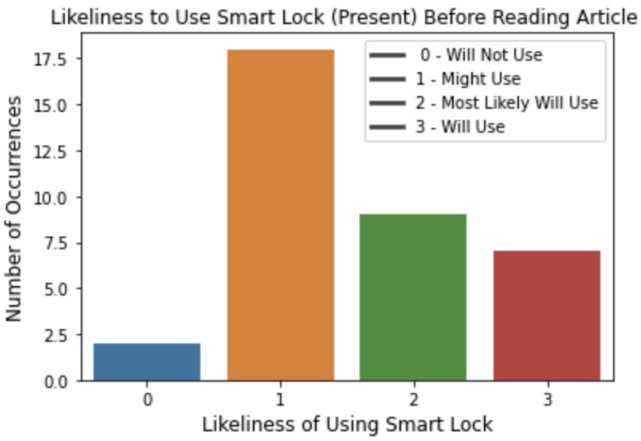


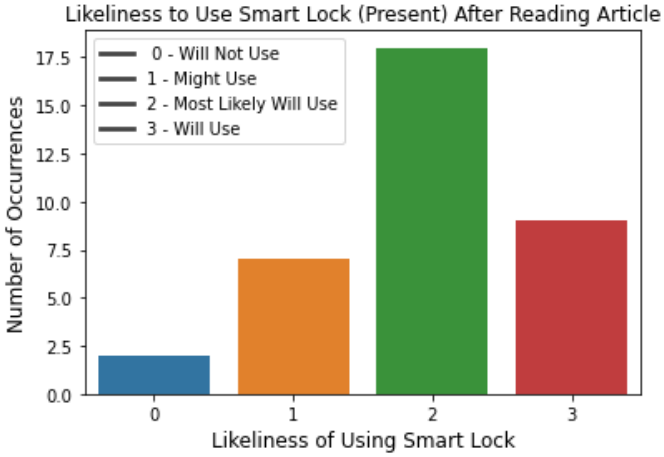


Note: 1 - No People Completely Distrusted Smart Locks Before Reading the Article

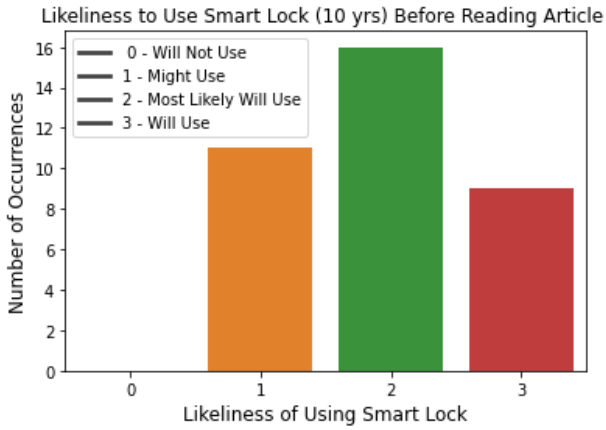
Similar to Level of Expertise, the perceptions of safety before and after reading the article were analyzed (Appendix C1). After reading the article, the trend slightly shifts to the right (See Figures 3 and 4), meaning that perceptions of security increased. However, a Stuart-Maxwell test (p-value = .49) shows that the shift is not statistically significant.

Next, the relationship between trust in technology and adoption rate (in the present) was analyzed. Both the contingency table of counts (Appendix C2) and a Stuart-Maxwell test (p-value = .0005) showed that these two variables were dependent on each other. This meant that participants who trusted technology were more likely to use a smart lock (in the present). Furthermore, it was found that gender and adoption rate (in the present)(Appendix D) were independent (p-value = .46), meaning that males and females were just as likely to buy smart locks.



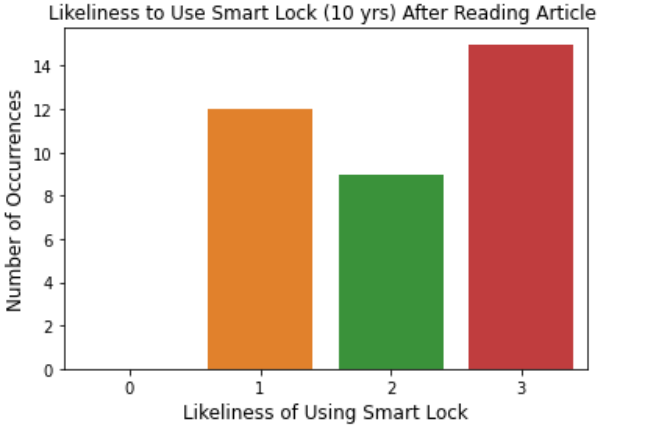


Additionally, participants' likelihood to buy a smart lock in the near future before reading the article and after reading the article was measured. Figure 5 showed that most participants said they might use a smart lock in the near future before reading the article. After reading the article, however, people were more likely to use a smart lock, as shown by figure 6. A Stuart-Maxwell test (p-value = .0499) confirmed this, meaning that the two variables were dependent and smart lock adoption rate was increased in the short term.



Note: 0 - No people said they would not use a smart lock before reading the article

Figure 7



Note: 0 - No people said they would not use a smart lock after reading the article

Figure 8

Lasty, participants' likelihood to buy a smart lock in 10 years before reading the article and after reading the article was measured. Most people before reading the article said they would most likely use a smart lock in 10 years (Figure 7). After reading the article, the trend slightly shifts to the right and most people said that they will definitely use a smart lock in 10 years (Figure 8). A Stuart-Maxwell test (p-value = .21), however, showed that the two variables were independent and the trend was not statistically significant. This means that reading the article did not change the long term adoption rate of smart locks.

Limitations

There were several limitations to my method such as sample size, sampling methods, and the nature of some questions in the survey. The sample size was 36 participants, lower than the

recommended value of 50 for chi-squared tests (PASSEL). This may explain why trends in the barplots of gender vs smart lock adoption (Appendix D) and smart lock adoption in 10 years (Figure 7 and 8) were present upon analysis, but not statistically significant. In order to determine that there is definitively not a relationship between these variables, a bigger sample size would be ideal.

Furthermore, most of the 36 people who took the survey lived near each other and were not a representative sample of the population of the Nashville area. This may have been because the survey was distributed on local platforms. Not only did this lead to a sample of similar economic background, but participants' perceptions of safety of their own homes were all similar. For example, in lower-income populations who have higher crime rates, home security is arguably more important, and participants may have been more concerned by the security risks presented, implying that perceptions of safety are more likely to be varied based on income. As the sample was mostly from the zip code 37027 in which the median income is $133,254 and 83.3% of the sample indicated that they always felt safe in their home, the results of this study cannot be applied to lower-income populations and those who feel unsafe in their homes. This could be accounted for by using stratified random sampling instead of voluntary sampling, which would have ensured that data from all ranges of income was represented.

Even in higher-income populations, differences between income could not be analyzed due to the nature of some of the questions. For example, 55.5% of the participants chose not to disclose their annual family income. As a result, not enough data was available to draw conclusions about how income affects adoption rate. This may be accounted for in future studies with an increase in sample size. To elaborate, if 50 is the ideal sample size for a chi-square test, then a sample size of 90 would be required if 55.5% of people chose not to respond to the question. Overall, an increase in sample size and implementation of stratified random sampling is necessary in future research.

Discussion

Based on the results of the test, the article did increase the amount of information the participant knew about smart locks. While participants knew more about smart locks, how they work, and security concerns, the participants' perception of security of the smart lock did not change (p-value = .49). This indicates that the security risks did not cause the sample to trust smart locks more or less. Although perceptions of security did not change, short-term adoption

rates increased (p-value = .049), supporting the privacy paradox for smart locks which explains that customers are willing to sacrifice security for potential benefit (Schneier, 2008), meaning that the benefits presented were greater than potential loss. Even though participants were informed of the security and privacy concerns, perceptions of security did not change and many chose to still use a smart lock in the near future.

Importantly, however, smart lock adoption rates were not changed by the article in the long term (p-value = .21), showing that the article did not change purchase intention in 10 years. This was interesting as it indicated that marketing and advertising is effective in the short term, but not necessarily crucial to long-term adoption rates. As previously mentioned, Shin et al. found that younger and lower-income groups are more likely to buy later than older and higher-income groups, known as purchase timing. Since adoption rates are not changed in the long term, younger and lower-income populations are likely to be less influenced by the increased access to information.

Additionally, it was found that trust in technology and short-term adoption rates were dependent (p-value = .0005), meaning that people who trusted technology were more likely to use a smart lock. This support's Ajzen's Theory of Planned Behavior which explains that past behavior has a significant impact on behavior in the future (1991). In this case, it was confirmed that past trust indicates future trust in technology, suggesting that increased information will not affect adoption rates in those with past histories of buying similar products. This agrees with the Technology Acceptance Model (King & He, 2006), which posits that rates of adoption in smart home technologies are directly correlated to openness to experience (created by trust in technology).

Conclusion

With smart home technology becoming more relevant, analysis of data like this becomes only more important with time. Key results from the data analysis show that smart lock advertising is effective if it focuses on the benefits of smart locks due to the Privacy Paradox. This can be used by smart lock companies to market their products and connect to consumers in the most efficient way. Another implication would be focusing short-term advertising on older and higher income populations due to purchase timing.

However, it is important to note that these results can only be generalized to high-income populations. Future research should focus more on smart lock adoption rates are affected in

lower-income populations. Furthermore, research could analyze how the information presented affects intention to buy smart locks. For example, presenting security concerns and fixes before the benefits may affect adoption rates differently. This could be done by separating the sample into multiple groups and giving a different article to each group. Lastly, future studies could analyze how the use of different mediums to convey information affects smart lock adoption rate. The medium used in this study was an article; however, advertisements on social media or platforms like Youtube may be more effective as it targets younger populations. This may lead to different conclusions related to purchase timing.

Overall, the conclusions drawn from this data were significant and can impact how companies advertise products and services related to home security in the future.

References

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-t

Bijvank, J. E. (2018, January 1). Adoption of smart Lock delivery in THE E-grocery market in the Netherlands. Adoption of smart lock delivery in the E-grocery market in the Netherlands. Retrieved September 10, 2021, from http://essay.utwente.nl/76689/.

Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure internet of things devices. Crime Science, 9(1). https://doi.org/10.1186/s40163-019-0110-3

Courtney K. L. (2008). Privacy and senior willingness to adopt smart home information technology in residential care facilities. Methods of information in medicine, 47(1), 76–81. https://doi.org/10.3414/me9104

de Camargo Silva, L., Samaniego, M., & Deters, R. (2019). IoT and blockchain for smart locks. 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). https://doi.org/10.1109/iemcon.2019.8936140

Han, D., Kim, H., & Jang, J. (2017). Blockchain-based smart door lock system. 2017 International Conference on Information and Communication Technology Convergence (ICTC). https://doi.org/10.1109/ictc.2017.8190886

How do smart locks work? Vivint. (2021, May 26). Retrieved September 9, 2021, from https://www.vivint.com/resources/article/how-do-smart-locks-work.

Khan, M. A., & Salah, K. (2018). Iot security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

King, W. R., & He, J. (2006). A meta-analysis of the technology acceptance model. Information & Management, 43(6), 740–755. https://doi.org/10.1016/j.im.2006.05.003

Parag, Y., & Butbul, G. (2018). Flexiwatts and seamless technology: Public perceptions of demand flexibility through smart home technology. Energy Research & Social Science, 39, 177–191. https://doi.org/10.1016/j.erss.2017.10.012

Park, E., Kim, S., Kim, Y. S., & Kwon, S. J. (2017). Smart home services as the next mainstream of the ict Industry: Determinants of the adoption of smart home services. Universal Access in the Information Society, 17(1), 175–190. https://doi.org/10.1007/s10209-017-0533-0

Prada-Delgado, M. A., Vazquez-Reyes, A., & Baturone, I. (2016). Physical unclonable keys for smart lock systems using Bluetooth low energy. *IECON 2016 - 42nd*

Annual Conference of the IEEE Industrial Electronics Society. https://doi.org/10.1109/iecon.2016.7792955

Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., & Loge, C. (2006). The Smart Home Concept : Our immediate future. 2006 1ST IEEE International Conference on E-Learning in Industrial Electronics. https://doi.org/10.1109/icelie.2006.347206

Schneier, B. (2008). The psychology of security. Progress in Cryptology – AFRICACRYPT 2008, 50–79. https://doi.org/10.1007/978-3-540-68164-9_5

Shin, J., Park, Y., & Lee, D. (2018). Who will be smart home users? An analysis of adoption and diffusion of smart homes. Technological Forecasting and Social Change, 134, 246–253. https://doi.org/10.1016/j.techfore.2018.06.029

Shuhaiber, A., & Mashal, I. (2019). Understanding users' acceptance of smart homes. Technology in Society, 58, 101110. https://doi.org/10.1016/j.techsoc.2019.01.003

Smart lock market demand to reach 41.9 million units by 2028. Market Research Reports & Consulting. (n.d.). Retrieved September 10, 2021, from https://www.grandviewresearch.com/press-release/global-smart-lock-market.

Stuart–Maxwell Test. Oxford Reference. (n.d.). Retrieved April 3, 2022, from https://www.oxfordreference.com/view/10.1093/oi/authority.20110810105946716.

SUNNY. (2020). One of a kind Smart lock...Love this. Amazon. Retrieved September 9, 2021, from https://www.amazon.com/gp/customer-reviews/R373EI62H928RA/ref=cm_cr_dp_d_rvw_ttl?ie=UTF8&ASIN=B08FR31H3M.

What is a smart lock and how does it work? ADT Security Systems. (n.d.). Retrieved April 30, 2022, from https://www.adt.com/resources/what-are-smart-locks

When Chi-square is appropriate - strengths/weaknesses. passel. (n.d.). Retrieved April 3, 2022, from https://passel2.unl.edu/view/lesson/9beaa382bf7e/14

Williams, E., Slade, E., Hodges, D., & Morgan, P. (2020). Individual Differences in the Adoption and Secure Use of Smart Home Technology. *British Academy of Management*

Conference.

Appendix A

Article Implemented After Pre-Survey and Before Post-Survey

Adapted From:

What is a smart lock and how does it work? ADT Security Systems. (n.d.). Retrieved April 30, 2022, from https://www.adt.com/resources/what-are-smart-locks

Article:

Considering that a traditional lock is generally an inanimate object, you might be wondering how one can be considered "smart." The adjective "smart" in this context refers to the lock's ability to connect to other technology. Just as your smartphone can connect to the internet, a smart lock can connect to your home Wi-Fi.

This connection gives you the ability to activate the lock remotely, as well as check if it is locked or unlocked. In fact, you can even check on the status of a smart lock from virtually anywhere in the world, as long as you have an internet connection.

No two smart locks are exactly alike, but many share common features. These features contribute to both the convenience and security associated with having a smart lock.

Keyless entry: Most smart locks are equipped with a number keypad allowing you to open the door by simply entering a code. You can change the key code at any time for added security.

Mobile access: Smart locks can connect to a mobile app, allowing you to lock and unlock your door from anywhere in the world with an internet connection.

Custom user access codes: Many programmable locks allow you to create custom user access codes so that each member of the family has a different pin code.

Smart key: It used to be that if you needed to prevent someone from entering your home or you lost track of spare keys, you would need to replace your door lock entirely. With a smart key, you can just reprogram the key codes in your existing lock instead.

How do they work?

Just as you can replace the standard deadbolt locking mechanism in your door with another similar lock, so too can you replace the mechanism with a smart lock device. In terms of the locking mechanism itself, all of the parts are the same, it's just that it is controlled electronically instead of manually when you lock and unlock the door.

The smart lock itself, being an electronic device, requires a power supply in the form of a battery. So the lock will include a small, hidden battery compartment.

Your smart lock will contain electronic components allowing it to connect to your home internet either via Bluetooth, Wi-Fi, or Z-Wave. This is what gives you remote access to the lock via an internet-enabled smart device.

Safety Concerns

IoT devices, like smart locks, are recognized by experts to be easily hacked and compromised. They can pose a threat to privacy, integrity and confidentiality of data.

Smart locks are also made vulnerable by bluetooth low energy, the technology that makes smart locks function. Criminals can take advantage of how smart locks use bluetooth low energy and gain unauthorized access.

Fixes in the Future

Blockchain technology and other fixes may soon improve the security of smart locks. Block-chain technology, the same technology behind cryptocurrency, might be the solution to the many security concerns as it will “decentralize the system” by compartmentalizing the process Bluetooth Low Energy uses to communicate to the smart lock. By having nodes across many servers verify each other (Blockchain technology), the system becomes extremely secure and hard for an attacker to corrupt.

Appendix B

Pre-Survey and Post-Survey

Survey

Hello! Today you will be taking a survey about smart locks and perceptions of security. This survey is anonymous and the content of your responses will not be shared. This should take about 5 minutes. Thank you!

1.

What is your age?

2.

What gender do you identify as?

Mark only one oval.

- Male
- Female
- Prefer not to say
- Other:

3.

What is your household income (in dollars)?

Mark only one oval.

- 0 - 30,000
- 30,000 - 50,000
- 50,000 - 100,000
- 100,000 - 150,000
- 150,000 - 200,000
- 200,000 - 250,000

- 250,000+
- Prefer Not to say

4.

Which of the following statements do you most closely identify with? *Mark only one oval.*

- I do not feel safe in my home
- I feel safe in my home sometimes
- I feel safe in my home most of the time
- I feel safe in my home always

5.

What is your zip code/neighborhood?

6.

Which of the following statements do you most closely identify with? *Mark only one oval.*

- I do not know what a smart lock is
- I know a little about smart locks
- I know a lot about smart locks
- I am an expert in smart locks

7.

Please explain what a smart lock is. (Optional)

8.

Which of the following statements do you most closely identify with? *Mark only one oval.*

- I do not trust the security of smart locks
- I somewhat trust the security of smart locks
- I trust the security of smart locks most of the time
- I trust the security of smart locks always
- I do not know what a smart lock is

9.

Which of the following statements do you most closely agree with? *Mark only one oval.*

- I do not trust technology
- I trust technology sometimes
- I trust technology most of the time
- I trust technology always

10.

Which of the following statements do you most closely agree with? *Mark only one oval.*

- I will not use a smart lock in the foreseeable future
- I might use a smart lock in the foreseeable future
- I will most likely use a smart lock in the foreseeable future
- I will use a smart lock in the foreseeable future

11.

Which of the following statements do you most closely agree with? *Mark only one oval.*

- I will not use a smart lock in ten years time
- I might use a smart lock in ten years time
- I will most likely use a smart lock ten years time
- I will use a smart lock in ten years time

12.

Please Read This Article:

https://docs.google.com/document/d/1kOT6J5oq6FbnSqZIOdfiAbs_MYVxFQM7456uVrLohvw/e dit?usp=sharing

Mark only one oval.

- I have read the article

13.

Which of the following statements do you most closely identify with? *Mark only one oval.*

- I do not know what a smart lock is
- I know a little about smart locks
- I know a lot about smart locks
- I am an expert in smart locks

14.

Which of the following statements do you most closely

identify with? *Mark only one oval.*

- I do not trust the security of smart locks
- I somewhat trust the security of smart locks
- I trust the security of smart locks most of the time
- I trust the security of smart locks always
- I do not know what a smart lock is

15.

Which of the following statements do you most closely agree with? *Mark only one oval.*

- I do not trust technology
- I trust technology sometimes
- I trust technology most of the time
- I trust technology always

16.

Which of the following statements do you most closely agree with? *Mark only one oval.*

- I will not use a smart lock in the foreseeable future
- I might use a smart lock in the foreseeable future
- I will most likely use a smart lock in the foreseeable future
- I will use a smart lock in the foreseeable future

17.

Which of the following statements do you most closely agree with? *Mark only one oval.*

- I will not use a smart lock in ten years time
- I might use a smart lock in ten years time
- I will most likely use a smart lock ten years time
- I will use a smart lock in ten years time

Appendix C

Contingency Tables

Which of the following statements do you most closely identify with? .4 / Which of the following statements do you most closely identify with? .2	I do not know what a smart lock is	I do not trust the security of smart locks	I somewhat trust the security of smart locks	I trust the security of smart locks always	I trust the security of smart locks most of the time
I do not know what a smart lock is	1	0	1	0	2
I somewhat trust the security of smart locks	0	1	10	2	3
I trust the security of smart locks always	1	0	0	1	0

Figure C1. The above is a table of counts which shows the relationship between perceptions of security before and after reading the article.

Figure C2. The above is a table of counts which shows the relationship between trust in technology and smart lock adoption rate.

Which of the following statements do you most closely agree with? .1 Which of the following statements do you most closely agree with?	I might use a smart lock in the foreseeable future	I will most likely use a smart lock in the foreseeable future	I will not use a smart lock in the foreseeable future	I will use a smart lock in the foreseeable future
I trust technology always	1	0	0	2
I trust technology most of the time	12	8	1	4
I trust technology sometimes	5	1	1	1

Appendix D

Graph of Gender vs Adoption Rate (present)